No. _____

IN THE

Supreme Court of the United States

NAICOM CORPORATION; D&V IP HOLDINGS, LLC; PAYLINK, LLC; and KIARAS, LLC,
Petitioners,
v.
DISH NETWORK CORPORATION; DISH NETWORK L.L.C.; NAGRASTAR LLC; UNITED STATES ATTORNEY FOR THE DISTRICT OF PUERTO RICO; ROSA EMILIA RODRÍGUEZ-VÉLEZ; JOSÉ CAPÓ-IRIARTE; NICHOLAS W. CANNON; FEDERAL BUREAU OF INVESTIGATION; DOUGLAS A. LEFF; BRADLEY REX; LANCE LANGE; CLAY REHRIG; JUAN GALARZA; JASON LOPEZ; KEVIN PEARSON; TOLTEC INVESTIGATIONS, L.L.C., et al.,
Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the First Circuit

---

APPENDIX TO PETITION FOR WRIT OF CERTIORARI

EDWIN PRADO-GALARZA
Counsel of Record
PRADO, NÚÑEZ & ASSOCIATES, P.S.C.
403 Del Parque Street, 8th Floor
San Juan, Puerto Rico 00912
Telephone: (787) 977-1411
pradolaw10@gmail.com

APPENDIX INDEX

App. 1a Judgment of the United States Court of Appeals for the First Circuit entered December 2, 2025. 1a

App. 4a Order of the United States Court of Appeals for the First Circuit denying request for written opinion entered December 8, 2025. 4a

App. 6a Order of the United States Court of Appeals for the First Circuit denying rehearing and rehearing en banc entered February 24, 2026 . 6a

App. 9a Order on DISH/NagraStar Defendants' Motion to Dismiss, United States District Court for the District of Puerto Rico, entered March 29, 2024. 9a

App. 120a Order on DISH Network Corporation's Motion to Dismiss, United States District Court for the District of Puerto Rico, entered March 29, 2024. 103a

App. 239a Order on Federal Defendants' Motion to Dismiss, United States District Court for the District of Puerto Rico, entered March 29, 2024. 198a

Pages 358a–610a App. 358a Order on Toltec Investigations, LLC and Michael Thomas Jaczewski's Motion to Dismiss, United States District Court for the District of Puerto Rico, entered March 29, 2024. 291a

App. 461a Second Amended Complaint, United States District Court for the District of Puerto Rico 375a

App. 601a Rule 28(j) Letter submitted to the United States Court of Appeals for the First Circuit 496a

App. 605a Relevant Constitutional and Statutory Provisions 499a

/s/ EDWIN PRADO-GALARZA
EDWIN PRADO-GALARZA
Counsel of Record
PRADO, NÚÑEZ & ASSOCIATES,
P.S.C. 403 Del Parque Street, 8th Floor San Juan,
Puerto Rico 00912
Telephone: (787) 977-1411
pradolaw10@gmail.com

Dated May 26, 2026

12.2.2025 WL 4694553

Only the Westlaw citation is currently available. United States Court of Appeals, First Circuit.

Naicom Corporation; D&V IP Holdings, LLC; Paylink, LLC; Kiaras, LLC, Plaintiffs, Appellants,

v.

DISH NETWORK CORPORATION; Dish Network L.L.C.; NagraStar LLC.; Bert Eichhorn; Emily Rinkel; Jordan Smith; Kevin Gedeon; Michael Thomas Jaczewski, a/k/a Brian Parson; Dish Network Collaborators; United States Attorney for the District of Puerto Rico; Rosa Emilia Rodríguez-Vélez; José Capó-Iriarte; Nicholas W. Cannon; Federal Bureau of Investigation San Juan Field in Puerto Rico; Douglas A. Leff; Bradley Rex; Lance Lange; Clay Rehrig; Juan Galarza; Jason Lopez; Kevin Pearson; United States Attorney's Office; Toltec Investigations, L.L.C., Defendants, Appellees, Dish Network Collaborators, Kevin Reaves, Several Unknown Agents of Federal Bureau of Investigations, and John Does 1-20, Defendants.

No. 24-1416|

Entered: December 2, 2025

Attorneys and Law Firms

Rafael F. Castro Lang, Rafael F. Castro Lang Law Office, San Juan, PR, for Plaintiffs-Appellants.

Carolina V. Cabrera-Bou, Jose Luis Ramirez-Coll, Antonetti Montalvo & Ramirez-Coll, San Juan, PR, Timothy Frank, Chad Hagan, Kronsky Kennon Sherer, Hagan Noll & Boyle LLC, Houston, TX, for Defendants-Appellees Dish Network Corporation, Dish Network L.L.C., NagraStar L.L.C., Bert Eichhorn, Emily Rinkel, Jordan Smith, Kevin Gedeon, Michael Thomas Jaczewski, a/k/a Brian Parson.

Priscila Acevedo, Juan Carlos Reyes-Ramos, US Attorney's Office, San Juan, PR, Daniel J. Aguilar, US Dept of Justice, Civil Division, Washington, DC, Patrick B. Fenior, US Department of Justice, Civil Division, Washington, DC, for Defendants-Appellees United States Attorney for the District of Puerto Rico, Rosa Emilia Rodríguez-Vélez, José Capó-Iriarte, Nicholas W. Cannon, Federal Bureau of Investigation San Juan Field in Puerto Rico, Douglas A. Leff, Bradley Rex, Lance Lange, Clay Rehrig, Juan Galarza, Jason Lopez, Kevin Pearson, United States Attorney's Office, Toltec Investigations, L.L.C.

Before Barron, Chief Judge, Gelpí and Hamilton, * Circuit Judges.

JUDGMENT

***1** Plaintiffs-appellants appeal from the dismissal of

their claims pursuant to Fed. R. Civ. P. 12(b)(6). After de novo review of the briefs and record below, we affirm the dismissal of plaintiffs-appellants' claims for the reasons set forth in the district court's well-reasoned orders.

Footnotes

* Of the U.S. Court of Appeals for the Seventh Circuit, sitting by designation.

United States Court of Appeals
For the First Circuit
No. 24-1416

NAICOM CORPORATION; D&V IP HOLDINGS, LLC; PAYLINK, LLC; KIARAS, LLC,

Plaintiffs - Appellants,

v.

DISH NETWORK CORPORATION; DISH NETWORK L.L.C.; NAGRASTAR LLC.; BERT EICHHORN; EMILY RINKEL; JORDAN SMITH; KEVIN GEDEON; MICHAEL THOMAS JACZEWSKI, a/k/a Brian Parson; UNITED STATES ATTORNEY FOR THE DISTRICT OF PUERTO RICO; ROSA EMILIA RODRÍGUEZ-VÉLEZ; JOSÉ CAPÓ-IRIARTE; NICHOLAS W. CANNON; FEDERAL BUREAU OF INVESTIGATION SAN JUAN FIELD IN PUERTO RICO; DOUGLAS A. LEFF; BRADLEY REX; LANCE LANGE; CLAY REHRIG; JUAN GALARZA; JASON LOPEZ; KEVIN PEARSON; UNITED STATES ATTORNEY'S OFFICE; TOLTEC INVESTIGATIONS, L.L.C., DISH NETWORK COLLABORATORS, KEVIN REAVES, SEVERAL UNKNOWN AGENTS OF FEDERAL BUREAU OF INVESTIGATIONS, AND JOHN DOES 1-20,
Defendants.

Before. Barron, Chief Judge, Hamilton* and Gelpí, Circuit Judges.

ORDER OF COURT

Entered: December 8, 2025

Appellants D&V IP Holdings, LLC; Paylink, LLC; Kiaras, LLC; and Naicom Corporation's motion requesting opinion affirming judgment is denied.

* Of the U.S. Court of Appeals for the Seventh Circuit, sitting by designation.

By the Court:

Anastasia Dubrovsky, Clerk

cc:
Rafael F. Castro Lang Jose Luis Ramirez-Coll Carolina V. Cabrera-Bou Chad Hagan Kronsky Kennon Sherer Timothy Frank Priscila Acevedo Juan Carlos Reyes-Ramos Daniel J. Aguilar

United States Court of Appeals
For the First Circuit

No. 24-1416

NAICOM CORPORATION; D&V IP HOLDINGS, LLC; PAYLINK, LLC; KIARAS, LLC,

Plaintiffs - Appellants, v.

DISH NETWORK CORPORATION; DISH NETWORK L.L.C.; NAGRASTAR LLC.; BERT EICHHORN; EMILY RINKEL; JORDAN SMITH; KEVIN GEDEON; MICHAEL THOMAS JACZEWSKI, a/k/a Brian Parson; UNITED STATES ATTORNEY FOR THE DISTRICT OF PUERTO RICO; ROSA EMILIA RODRÍGUEZ-VÉLEZ; JOSÉ CAPÓ-IRIARTE; NICHOLAS W. CANNON; FEDERAL BUREAU OF INVESTIGATION SAN JUAN FIELD IN PUERTO RICO; DOUGLAS A. LEFF; BRADLEY REX; LANCE LANGE; CLAY REHRIG; JUAN GALARZA; JASON LOPEZ; KEVIN PEARSON; UNITED STATES ATTORNEY'S OFFICE; TOLTEC INVESTIGATIONS, L.L.C.,

Defendants - Appellees,

DISH NETWORK COLLABORATORS, KEVIN REAVES, SEVERAL UNKNOWN AGENTS OF FEDERAL BUREAU OF INVESTIGATIONS, AND JOHN DOES 1-20,

Defendants.

Before Barron, Chief Judge, Hamilton,* Gelpí, Montecalvo, Rikelman, Aframe, and Dunlap, Circuit Judges.

ORDER OF COURT

Entered: February 24, 2026

The petition for rehearing having been denied by the panel of judges who decided the case, and the petition for rehearing en banc having been submitted to the active judges of this court and a majority of the judges not having voted that the case be heard en banc, it is ordered that the petition for rehearing and the petition for rehearing en banc be denied.

By the Court:

Anastasia Dubrovsky, Clerk

---

* Of the U.S. Court of Appeals for the Seventh Circuit, sitting by designation.

cc:

Rafael F. Castro Lang Jose Luis Ramirez-Coll Carolina

V. Cabrera-Bou Chad Hagan Kronsky Kennon Sherer Timothy Frank Priscila Acevedo Juan Carlos Reyes-Ramos Daniel J. Aguilar

2024 WL 1363462
Only the Westlaw citation is currently available. United States District Court, D. Puerto Rico.
NAICOM CORPORATION, et al., Plaintiffs, v.
DISH NETWORK CORPORATION, et al., Defendants.

No. 3:21-cv-01405-JAW
|
Signed March 29, 2024

Attorneys and Law Firms

Rafael F. Castro-Lang, Castro & Castro Law Office, San Juan, PR, for Plaintiffs.

Chad M. Hagan, Pro Hac Vice, Timothy Frank, Pro Hac Vice, Hagan Noll & Boyle LLC, Houston, TX, Jose L. Ramirez-Coll, Antonetti Montalvo & Ramirez-Coll, San Juan, PR, Carolina V. Cabrera-Bou, AMRC, LLC, San Juan, PR, for Defendants Dish Network Corporation, DISH Network L.L.C., NagraStar LLC, Bert Eichhorn, Emily Rinkle, Jordan Smith, Kevin Gedeon, Michael Thomas Jaczewski.
Patrick B. Fenior, DOJ-Civ, Washington, DC, Priscila M. Acevedo-Roman, U.S. Attorney's Office for the District of Puerto Rico, San Juan, PR, for Defendants United States Attorney for the District of Puerto Rico, Rosa Emilia Rodriguez-Velez, Jose Capo, Nicholas W. Cannon, Federal Bureau of Investigations San Juan Field in Puerto Rico,

Douglas A. Leff, Bradely Rex, Lance Lange, Clay Rehrig, Juan Galarza, Jason Lopez, Kevin Pearson, United States Attorney's Office, Toltec Investigations, LLC.

ORDER ON THE DISH/NAGRASTAR DEFENDANTS' MOTION TO DISMISS

JOHN A. WOODCOCK, JR., UNITED STATES DISTRICT JUDGE

***1** Two limited liability companies and several of their employees file a motion to dismiss plaintiffs' seven-count complaint, arising out of a criminal investigation wherein the private parties assisted federal law enforcement. The Court grants the motion to dismiss, dismissing all seven counts. The Court dismisses plaintiffs' RICO claims because plaintiffs have not adequately pleaded the existence of an enterprise, a pattern of racketeering activity, or a conspiracy. The Court dismisses plaintiffs' Computer Fraud and Abuse Act claim, Stored Communications Act claim, Digital Millennium Copyright Act claim, and Defend Trade Secrets Act claim because, taking plaintiffs' allegations as true, the private entities' assistance to law enforcement fell within statutory exceptions for authorized law enforcement activity. Finally, the Court dismisses the Puerto Rico Uniform Trade Secrets Act claim because plaintiffs have not adequately alleged that the defendants misappropriated their trade secrets.

I. PROCEDURAL HISTORY

On August 27, 2021, Naicom Corporation, D&V IP Holdings, LLC, Paylink, LLC, and Kiaras, LLC, filed a seven-count complaint against approximately twenty known Defendants and two dozen unknown Defendants. 1 *Compl.* (ECF No. 1). The Court has twice permitted Plaintiffs to amend their complaint, and the Second Amended Complaint is now the operative complaint. *Am. Compl.* (ECF No. 100); *Second Am. Compl.* (ECF No. 130).

The parties categorize the numerous Defendants into four groups: 1) DISH Network LLC, NagraStar LLC, Bert Eichhorn, Emily Rinkel, [2] Jordan Smith, and Kevin Gedeon (the DISH/NagraStar Defendants); 2) DISH Network Corporation (DISH Corp. or DNC); 3) Toltec Investigations, LLC and its President and CEO, Michael Thomas Jaczewski (the Toltec Defendants); and, 4) former U.S. Attorney Rosa E. Rodriguez-Velez, former Assistant U.S. Attorney Jose Capo-Iriarte, Assistant U.S. Attorney Nicholas W. Cannon (the USAO Defendants) and Special Agents and employees of the Federal Bureau of Investigation Douglas Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, and Jason Lopez (the FBI Defendants) (collectively, the Federal Defendants).

***2** Plaintiffs allege: (1) violations of the Racketeer

Influenced and Corrupt Organizations Act (RICO); (2) a RICO conspiracy; (3) violations of the Computer Fraud and Abuse Act (CFAA); (4) violations of the Stored Communications Act (SCA); (5) violations of the Digital Millennium Copyright Act (DMCA); (6) violations of the Defend Trade Secrets Act (DTSA) by misappropriation of trade secrets; and (7) violations of the Puerto Rico Industrial and Trade Secrets Protection Act (PTSA) under the Uniform Trade Secrets Act (Law No. 80). *Second Am. Compl.* ¶¶ 124-202.

On October 31, 2022 and November 1, 2022, each of the four groups of Defendants filed a motion to dismiss the complaint. *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Mot. to Dismiss* (ECF No. 134) (*Defs.' Mot.*); *Def. DISH Network Corp.'s Mot. to Dismiss* (ECF No. 136); *Defs.' Toltec Investigations, L.L.C. and Mike Jaczewski's Mot. to Dismiss* (ECF No. 137); *Fed. Defs.' Mot. to Dismiss* (ECF No. 138).

On December 5, 2022, Plaintiffs filed a response to the DISH/NagraStar Defendants' motion to dismiss. *Mot. in Resp. to Dish/NagraStar Defs.' Mot. to Dismiss* (ECF No. 147) (*Pls.' Opp'n*). On January 18, 2023, Plaintiffs responded to the Federal Defendants' motion. *Mot. in Resp. to the Fed. Defs.' Mot. to Dismiss* (ECF No. 153). On February 21, 2023, the Toltec Defendants withdrew a section of their motion to dismiss, *Unopposed Notice of*

Partial Withdrawal of Toltec Investigations L.L.C. and Mike Jaczewski's 12(b)(2) Mot. to Dismiss (ECF No. 163), and on February 27, 2023, Plaintiffs responded to the remainder of the Toltec Defendants' motion. *Mot. in Resp. to Toltec Investigations and Mike Jaczewski's Mot. to Dismiss* (ECF No. 167). On March 17, 2023, Plaintiffs responded to DISH Corp.'s motion. *Mot. in Resp. to Dish Network Corp.'s Mot. to Dismiss* (ECF No. 179).

Each group of Defendants filed a reply in support of its motion. *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Reply* (ECF No. 164) (*Defs.' Reply*); *Fed. Defs.' Reply* (ECF No. 173); *Defs. Toltec Investigations L.L.C. and Michael Jaczewski's Reply in Supp. of Rule 12(b)(6) Mot. to Dismiss* (ECF No. 185); *DISH Network Corp.'s Reply in Supp. of Its Mot. to Dismiss* (ECF No. 196).

Finally, Plaintiffs filed sur-replies opposing each motion. *Sur-Reply to the Dish Network, LLC and NagraStar, LLC Reply Mot. to Pls.' Resp. to Defs.' Mot. to Dismiss SAC* (ECF No. 182) (*Pls.' Sur-Reply*); *Sur-Reply Mot. to Fed. Defs.' Reply Mot. to Pls.' Resp. to Fed. Defs.' Mot. to Dismiss, SAC* (ECF No. 190); *Sur-Reply Mot. to the Toltec Investigations L.L.C. and Michael Jaczewski's Reply Mot. to Pls.' Resp. to Their Mot. to Dismiss SAC* (ECF No. 195); *Sur-Reply Mot. to Dish Network Corp.'s Reply Mot. to Pls.' Resp. to Mot. to Dismiss SAC* (ECF No. 199).

II. FACTS[3]

a. The Parties

In 2015 and 2016, Darwin Quinones-Pimentel and Victor Vega-Encarnacion founded Naicom Corporation (Naicom) and D&V IP Holdings, LLC (D&V) to offer Internet Protocol Television (IPTV) services. The companies are structured such that D&V holds the proprietary "intellectual technology" created by Mr. Quinones, and Naicom licenses the technology from D&V to distribute television programming. *Second Am. Compl.* ¶ 63.

Kiaras, LLC (Kiaras) and Paylink, LLC (PayLink) are also joint ventures operated by Mr. Quinones and Mr. Vega. *Id.* ¶ 14. Kiaras is a human resources and time-and-attendance management company, and PayLink is a payroll processing company. *Id.* Both Kiaras and Paylink operate on the "PAYLINK AND KIARAS Cloud Network," another proprietary intellectual technology creation of Mr. Quinones. *Id.* ¶¶ 5-6. All four companies are corporations existing under the laws of the commonwealth of Puerto Rico with their places of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907. *Id.* ¶¶ 33-36.

***3** DISH Network Corporation (DISH Corp. or DNC) was

organized in 1995 as a corporation under the laws of the State of Nevada, started offering the DISH® branded pay-tv service in March 1996, and is the nation's third largest pay-tv provider. *Id.* ¶ 37. DISH Network LLC (DISH LLC) was organized in 1987 as a Limited Liability Corporation under the laws of the state of Colorado. *Id.* ¶ 38.

NagraStar, LLC (NagraStar) is a joint venture between DISH Corp. and Kudelski SA formed in 1998. *Id.* ¶ 39. NagraStar's focus is delivering and maintaining security solutions for satellite and Internet-based television systems and other connectivity initiatives in North America, and their mission also includes anti-piracy investigations and cooperation with law enforcement agencies. *Id.* Jordan Smith was at all relevant times a Manager of Field Security & Investigations and Senior Anti-Piracy Investigator for NagraStar. *Id.* ¶ 41. Bert Eichhorn and Emily Rinkel were Managers of Field Security & Investigations for NagraStar. *Id.* ¶¶ 42-43. Kevin Gedeon was a Manager of Fraud Investigations for NagraStar. *Id.* ¶ 44.

Toltec Investigations, LLC (Toltec) is a private investigative agency specializing in investigating the technology and distribution involved in IPTV systems, copyrights, patents, and "Trademark and Brand's Intellectual Property." *Id.* ¶ 40. Michael Thomas Jaczewski, a.k.a. Brian Parsons, was at all relevant times

President and Chief Executive Officer of Toltec. *Id.* ¶ 45.

Rosa Emilia Rodriguez-Velez was at all relevant times the United States Attorney for the District of Puerto Rico. *Id.* ¶ 46. Jose Capo-Iriarte was an Assistant U.S. Attorney (AUSA) and head of the office's Criminal Division. *Id.*
¶ 47. Nicholas Cannon was an AUSA and Deputy Chief of the Cybercrimes Division. *Id.* ¶ 48.

Douglas Leff was at all relevant times Special Agent in Charge of the FBI's San Juan Division. *Id.* ¶ 49. Also in that division, Brad Rex was a Supervisory Special Agent, Lance Lange, Kevin Pearson, and Clay Rehrig were Special Agents, Juan Galarza a Computer Science Officer, and Jason Lopez an Evidence Technician. *Id.* ¶¶ 50-55.

b. Naicom's Origins

Between 2002 and 2012, Mr. Quinones developed the intellectual technology, including the source code, underpinning the Paylink and Kiaras Cloud Workforce Management system and Naicom's IPTV services. *Id.* ¶ 5. The proprietary IPTV system was characterized as a Dynamic Internet Semantic Multicast Environment (DISME), which "enabled for the first time the broadcast of media via private networks and the internet, a new concept of IPTV service to distribute Live-Video

Television Content (media) to residences, business, and primes customers." *Id.* ¶¶ 8-11.

By 2016, Mr. Quinones had completed all DISME technology alpha and beta tests and, alongside Mr. Vega, founded Naicom. *Id.* ¶ 12. Naicom is a network and internet communication platform that delivers live television, video on-demand content, internet, and wireless network services to subscribers worldwide. *Id.* Naicom also provides instant access to television shows, movies, and music/videos on-demand, and live sports and music events through Naicom's set-top box using IPTV and TV Everywhere (TVE) on any mobile device. *Id.*

Mr. Quinones and Mr. Vega registered Naicom as a closed corporation with the State Department of Puerto Rico and complied with all requirements as a legitimate IPTV business. *Id.* ¶ 66. Naicom also requested to manufacture its own brand of set-top boxes for end users through Informir LLC and acquired the programing licenses to distribute on-demand content in the United States, Puerto Rico, and the U.S. Virgin Islands through worldwide television network companies. *Id.* ¶¶ 67-68. In 2017, Naicom became a member of the National Rural Telecommunications Cooperative (NRTC). *Id.* ¶ 68.

***4** On January 6, 2017, Naicom submitted a request to the Apple Corporation to have its TV App added to Apple's AppStore. *Id.* ¶ 69. Apple's legal department

requested that Naicom produce all licenses authorizing the distribution of programming to Naicom's subscribers via Naicom's TV App. *Id.* On February 16, 2017, Apple approved Naicom's App for inclusion in the Apple AppStore. *Id.* ¶ 70. In December 2017, Sam's Club approved Naicom to launch and distribute Naicom's IPTV set-top box in their retail stores. *Id.* ¶ 71.

c. Naicom's Information Security

Naicom went to great lengths to protect its intellectual technology. *Id.* ¶¶ 64-65. D&V IP Holdings and Naicom developed significant amounts of confidential and proprietary information, including non-public information relating to the DISME's source codes, patterns, formulas, algorithms, methods, and techniques; the technological vision for Naicom's IPTV content, distribution, marketing, servicing, research and development efforts and strategies; business and marketing performance strategies; financial data and business plans; technical data; customer development management programs; and subcontractor and vendor relationships (collectively, with the DISME, the Confidential Information or Naicom's Confidential Information). *Id.* ¶ 64.

To protect this information, Plaintiffs only installed on their servers, located at the Naicom Data Center Facility, what is known as compiled executable. *Id.* ¶ 65.

The entire system was installed with an operating system that allowed the hard drive to be encrypted and, to access the servers, an authorized employee would need to enter the secure data facility and provide a username and password. *Id.* The server is not exposed to the internet and could only be accessed from inside the facility. *Id.* The Confidential Information was also downloaded onto a hard disk and kept in a safe box. *Id.*

Plaintiff companies took additional steps to safeguard their confidential information and proprietary data, including restricting employee access, requiring employees to execute non-disclosure agreements, imposing restrictions on remote access, and implementing encryption. *Id.* ¶¶ 72-76.

d. Negotiations with Claro Puerto Rico

In 2017, Naicom entered into negotiations with Claro Puerto Rico [4] (Claro) to distribute Naicom set-top boxes to Claro customers. *Id.* ¶ 77. Claro represented to Naicom that it had approximately 320,000 internet subscribers who received only five megabytes and thus could not subscribe to Claro's IPTV services, which required sixty megabytes to upload programming. *Id.* ¶ 78. During negotiations, Naicom and Claro entered into a mutual non-disclosure agreement prior to discussing and analyzing business information and the contents of the resellers' agreement. *Id.* ¶ 79. Claro's Product

Development Officer, Anibal Rios, projected that the Claro-Naicom business alliance would bring in over $10,000,000 in monthly gross revenue for the first year and over $13,000,000 for the second year only taking into account Claro's corporate and residential subscribers in Puerto Rico. *Id.* ¶ 80. Naicom projected that the Claro-Naicom alliance would add 100,000 new corporate subscribers, plus another 150,000 residential subscribers, bringing in projected monthly gross sales of $9,000,000 in the first year and $12,000,000 in the second year. *Id.* ¶ 81.

***5** Claro had an existing contract with DISH Network Satellite TV, whereby DISH Network provided TV programming to Claro's internet subscribers who could not subscribe to Claro's IPTV services. *Id.* ¶ 82. The Naicom deal represented a cancellation threat to DISH Network's contract with Claro. *Id.* Claro was also considering shutting down its IPTV business division due to loss of revenue. *Id.* During the negotiations for the Claro-Naicom deal, Carlos Garcia, Claro's IPTV business manager, became privy to information that the Claro-Naicom deal would leave him jobless if Claro opted to shut down its IPTV division, which he managed. *Id.* ¶ 83. Mr. Garcia alerted DISH Network that the Claro-Naicom IPTV deal would lead to cancellation of the DISH contract with Claro, which Plaintiffs allege led to "great animosity" between DISH Network and Naicom. *Id.* ¶ 84. On August 14, 2018, after a year of meetings between

Naicom and Claro, Claro pulled out of negotiations without notice. *Id.* ¶ 85. Plaintiffs believe the DISH Network Defendants advised Claro to withdraw because the FBI was investigating Naicom and its founders. *Id.* ¶ 86.

e. The DISH Network Investigation

On August 7, 2017, the DISH/NagraStar and DISH Corp. Defendants instructed the Toltec Defendants to purchase two Naicom TV set-top-box receivers so that the Defendants [5] could reverse engineer Plaintiffs' intellectual technology. *Id.* ¶ 87. The Defendants conducted "sniffing" to determine the direction of Naicom TV traffic and locate Naicom's facility. *Id.* The Defendants also used sniffing to attack and penetrate Naicom's servers and computers, monitoring content and capturing information on the network under the supervision of the Federal Defendants. *Id.* One of the two set-top box receivers was maintained by the DISH/NagraStar Defendants, the other by the Toltec Defendants. *Id.* ¶ 88. Both receivers were used for the attacks on Naicom's data center servers. *Id.*

Mr. Jaczewski purchased the two set-top boxes from Naicom under the false name of "Brian Parsons," and he provided false contact information. *Id.* ¶ 89. According to the Defendants, their investigation revealed that the receiver provided access to approximately forty-three

channels, including Disney, TBS, ESPN, CNN, HBO, Showtime, and Cinemax. *Id.* ¶ 90. The Defendants downloaded the Naicom TV App through the Apple AppStore, which provided access to approximately forty-two channels, and tested Naicom TV several times to determine whether it was providing DISH programming. *Id.* The tests revealed no DISH content. *Id.*

The Defendants also contacted several media companies to inquire into whether Naicom had the appropriate licensing contracts to distribute its programming. *Id.* ¶ 91. On each occasion, the investigators were informed that Naicom was authorized to distribute the network's content. *Id.* The investigators also discovered that Naicom's TV distribution technology was a threat to DISH Network and Sling TV, representing future competition for subscribers in Puerto Rico and the United States. *Id.* ¶ 92.

The DISH/NagraStar Defendants informed the other Defendants that they could not penetrate Naicom's Data Center computers and servers remotely, and thus direct, physical access would be required to extract Naicom's intellectual property. *Id.* ¶ 93. They knew that by entering the data center and shutting down the computers and servers, they would be able to bypass Naicom's security measures and access the internal hard drive. *Id.* ¶ 94.

According to Naicom, the Defendants knew that the intellectual property was extremely valuable and worth obtaining by any means necessary to advance their own television programming distribution system, and the Defendants conspired to misappropriate the technology for economic advantage. *Id.* ¶ 95.

***6** The DISH/NagraStar Defendants thereafter filed a complaint with the Federal Defendants alleging that Naicom was running an IPTV pirate operation. *Id.* ¶ 98. Plaintiffs allege that the motive behind the complaint was to secure NagraStar and DISH Network's participation in a search of Naicom's Data Center and the seizure of Naicom's computers, servers, and other hardware containing Naicom's intellectual property and trade secrets, under the ruse of assisting the Federal Defendants in discovering incriminating evidence. *Id.* Acquiring this information has given the DISH/NagraStar Defendants a competitive advantage over Naicom. *Id.* ¶ 99.

f. The Executions of the Search Warrants

1. The First Search of Naicom's Data Center

On August 27, 2019, the Federal Defendants applied for two search warrants: one for Naicom Corporation located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907, and the other for

Naicom's Data Center located at Villa Fontana, 4SS N2 Via Josefina, Carolina, Puerto Rico. *Id.* ¶¶ 19, 33, 105. Plaintiffs allege that the search warrants were "issued under illegal and unlawful means" because the Federal Defendants provided affidavits they knew to contain false and perjured information. *Id.* ¶ 20.

On August 27, 2019, the Federal and DISH/NagraStar Defendants executed the warrants, with the DISH/NagraStar Defendants "acting as federal agents." *Id.* ¶ 21. They seized documents, hard drives, and thumb drives, and downloaded data from the computers and servers containing Plaintiffs' Confidential Information. *Id.* Plaintiffs allege that the Defendants knew from their investigation prior to the searches that Naicom was authorized to distribute its programming and was not pirating content. *Id.* ¶ 101. The Defendants also allegedly knew that the evidence collected in the Federal Defendants' investigative files "negated any criminal wrongdoing that Naicom's founders were committing the crimes charged in the search and seizure warrant affidavit and application." *Id.* ¶ 102.

At the conclusion of the August 27, 2019 search, the Federal Defendants "learned that Naicom TV counted with all the programming distribution contract and agreements" [6] and instructed Mr. Quinones and Mr. Vega to report to the FBI offices with their licensing contracts for an interview. *Id.* ¶ 103. This interview took

place with the Federal Defendants sitting at one table and the DISH/NagraStar Defendants sitting at another table, allegedly posing as federal agents. *Id.* ¶ 104. The Defendants questioned Mr. Quinones about how Naicom acquired the IPTV distribution contracts and the technology used to distribute the programing. *Id.* They also inspected Naicom's contracts with content providers, which contained trade/business secrets and confidential information regarding DISME technology. *Id.*

2. The Second Search of Naicom's Data Center

On August 29, 2019, U.S. Attorney Rodriguez-Velez and AUSAs Capo-Iriarte and Cannon instructed FBI Agents Lange and Pearson to return to Naicom's data center with DISH/NagraStar Defendants Smith, Gedeon, and Eichhorn. *Id.* ¶ 105. Naicom alleges that the USAO Defendants ordered this search despite knowing beforehand that Naicom was a legitimate business and there was no probable cause for continued investigation. *Id.* Without obtaining new warrants, the Defendants again entered Naicom's data center facility, performed password resets, and installed "pen drives and other electronic instruments" to bypass security measures and download and seize Naicom's Confidential Information. *Id.* ¶¶ 22, 106. The agents used keys taken from Naicom's offices to enter Naicom's data center. *Id.* ¶ 105.

***7** During the search, Agent Pearson contacted Naicom

employee Jaime Echevarria and ordered him to come to the Data Center, as Agent Pearson wanted to speak with him, Mr. Quinones, and Mr. Vega. *Id.* ¶ 107. Upon arriving at the Data Center, Mr. Quinones observed Agents Lange and Pearson allowing Mr. Smith, Mr. Gedeon, and Mr. Eichhorn to access Naicom's Data Center computers, servers, and other hardware equipment without authorization from Naicom. *Id.* ¶ 108.

During the search, Agents Pearson and Lange pressured Mr. Quinones to sign a hold-harmless document accepting that he had run a pirate operation in the past so that they could close the case. *Id.* ¶ 109. Otherwise, they threatened that they would shut down the Data Center operation. *Id.* Mr. Quinones refused, despite Agents Pearson and Lange imploring him to sign the document. *Id.* ¶ 110.

Sometime thereafter, Mr. Vega arrived and, upon entering the Data Center, asked Agents Pearson and Lange if they had another search warrant to enter and search the Data Center. *Id.* ¶ 111. Agent Lange represented to Mr. Vega that the search warrant gave him ten days to come in and out and search the Data Center. *Id.* Mr. Vega told Agent Lange that Agent Lange was violating the United States Constitution and Federal law. *Id.*

Mr. Vega thereafter informed Agents Pearson and Lange

that he had discovered via LinkedIn that the alleged FBI experts who executed the search and interrogated Mr. Quinones and him at the FBI offices were Kevin Gedeon, investigator for DISH Network, and Jordan Smith, Bert Eichhorn, and Emily Rinkel, investigators for NagraStar. *Id.* ¶ 112. Mr. Vega questioned Agents Lange and Pearson as to why the FBI brought in his competition to search, inspect, and photograph private documents and allowed them access to computers and servers containing trade secrets, code sources, and business and intellectual property belonging to Naicom. *Id.* ¶ 113. Mr. Vega called his attorney and told him about the second search. *Id.* ¶ 114. After speaking with Agent Lange, the FBI agents and DISH/NagraStar investigators shut down Naicom's business operation and left the premises. *Id.*

g. The Demand for the Return of Property Under Rule 41(g)

On September 6, 2019, Plaintiffs filed a motion to demand the return of seized property under Rule 41(g) of the Federal Rules of Criminal Procedure. *Id.* ¶ 115. The District Court granted the Plaintiffs' Rule 41(g) motion on November 5, 2019, noting that the Government had waived objections to the court's Report & Recommendation. *Id.* ¶¶ 116-17.

h. Plaintiffs' Alleged Harm

Plaintiffs allege that the criminal investigation caused significant damage to their business reputation and unfairly enriched their competitors. *Id.* ¶¶ 118-19. They allege that prior to the execution of the search warrants, they had a great reputation and were about to close on a $15,000,000 investment deal, but investors pulled out upon learning Naicom was under criminal investigation. *Id.* ¶¶ 120-21. Plaintiffs also allege that Naicom was about to close a multimillion-dollar deal with Claro when Claro learned of the FBI's investigation and pulled out of negotiations. *Id.* ¶ 122. Plaintiffs say they have lost subscribers because of negative publicity resulting from the investigation and that the Defendants' intrusion into Naicom's Data Center computers, servers, and equipment caused damage leaving subscribers without TV programming services for several weeks and cost more than $500,000 to repair. *Id.* ¶ 123.

i. Plaintiffs' Causes of Action

***8** The Plaintiffs bring seven counts. Count One alleges that the Defendants violated RICO by forming an association in fact to advance the criminal objective of stealing Plaintiffs' intellectual property and trade secrets by committing mail and wire fraud, among other crimes. *Id.* ¶¶ 124-53.

Count Two alleges that the Defendants engaged in a

RICO conspiracy by conspiring to plan and execute the scheme outlined in Count One. *Id.* ¶¶ 154-57.

Count Three alleges that the Defendants the CFAA by accessing Naicom's computer systems without authorization or in excess of authorization and obtaining and using valuable information from those computers. *Id.* ¶¶ 158-68.

Count Four alleges that the Defendants violated the SCA by "willfully and intentionally access[ing] without authorization a facility which operates servers, encoders, computers, and telecommunications systems and technology, by electronically transmitting communications involved in Webservers, Email-Servers, Carrier Grade Routers which interconnected with local ISP providers through Border Gateway Protocols (BGP) in exchanging routing information between autonomous systems." *Id.* ¶¶ 169-75.

Count Five alleges that the Defendants violated the DMCA by illegally obtaining Plaintiffs' copyright-protected software programs, documents, confidential information, and research. *Id.* ¶¶ 176-84.

Count Six alleges that the Defendants violated the DTSA by stealing Plaintiffs' trade secrets, including DISME technology, intellectual property, and other confidential information. *Id.* ¶¶ 185-94.

Finally, Count Seven alleges that the Defendants misappropriated Plaintiffs' trade secrets in violation of the PTSA. *Id.* ¶¶ 195-202.

III. THE PARTIES' POSITIONS

a. The DISH/NagraStar Defendants' Motion to Dismiss

The DISH/NagraStar Defendants urge the Court to dismiss Plaintiffs' complaint for eight reasons: 1) "Plaintiffs' factual allegations assert neither a constitutional nor statutory violation under RICO, thus their claims are barred by qualified immunity"; 2) "the DISH/NagraStar Defendants, acting as alleged federal agents, lacked the criminal intent to engage in racketeering activity"; 3) "the *Noerr-Pennington* doctrine bars Plaintiffs' RICO claims"; 4) "Plaintiffs' RICO claims are predicated upon a legal impossibility, as the United States is the proper defendant and has not waived sovereign immunity"; 5) the Second Amended Complaint "fails to satisfy the essential elements of a RICO claim under [18 U.S.C.] § 1962(c)"; 6) Plaintiffs' "RICO conspiracy claim under [18 U.S.C.] § 1962(d) fails without a viable substantive claim and is otherwise inadequately pled"; 7) Plaintiffs' "federal statutory claims cannot satisfy the 'without authorization' elements, are otherwise inadequately pled, and the conduct alleged is

covered by immunity"; and 8) Plaintiffs' "PTSA claim is inadequately pled, the conduct complained of cannot fit within the scope of the 'improper means' element, and is otherwise subject to the Westfall Act." *Defs.' Mot.* at 2-3.

Leading with their qualified immunity argument, the DISH/NagraStar Defendants observe that "courts have consistently held that the qualified immunity doctrine provides a defense to civil RICO claims." *Id.* at 7-8 (citing *Gonzalez v. Otero*, 172 F. Supp. 3d 477, 508 (D.P.R. 2016); and *Gonzalez v. Lee Cnty. Hous. Auth.*, 161 F.3d 1290, 1300 (11th Cir. 1998)). They aver that, even though they are "private individuals," they are "entitled to the qualified immunity defense for the official misconduct alleged by Plaintiffs" because they were " 'acting as federal agents' under color of federal law at the direction and supervision of the Federal Defendants." *Id.* at 8 (quoting *Second Am. Compl.* ¶¶ 21-22).

***9** Next, the DISH/NagraStar Defendants argue that they "lacked the criminal intent to engage in 'racketeering activity.' " *Id.* at 9 (capitalization altered). According to the DISH/NagraStar Defendants, each of the alleged RICO predicate acts "[is] supported by allegations of legitimate government action." *Id.* (alteration in *Def.'s Mot.*) (quoting *Kahre v. Damm*, No. 2:07-CV-00231-DAE-RJJ, 2007 WL 9728869, at *7, 2007 U.S. Dist. LEXIS 95978

at *26 (D. Nev. Dec. 18, 2007)). The DISH/NagraStar Defendants further emphasize that their assistance in the execution of the search warrants does not "render the warrants invalid or constitute illegal trespass, as federal law authorizes government officials to procure assistance from private individuals in aid of a search warrant's execution." *Id.* at 9-10. Finally, the DISH/NagraStar Defendants maintain that "the purchase of IPTV set top box receivers and related subscription services using a pseudonym as part of an undercover federal investigation to detect pirated IPTV content is not mail or wire fraud." *Id.* at 10.

Turning to their *Noerr-Pennington* argument, the DISH/NagraStar Defendants observe that "Plaintiffs' RICO claims are premised on the DISH/NagraStar Defendants' pre-indictment investigative activities conducted at the direction of, and in conjunction with, the Federal Defendants." *Id.* at 12-13. They argue that "[c]ourts applying the *Noerr-Pennington* doctrine have deemed such pre-litigation investigative activities to be necessary predicates to formal legal proceedings and, as such, protected conduct incidental to prosecution under the *Noerr-Pennington* doctrine." *Id.* at 13.

The DISH/NagraStar Defendants then discuss sovereign immunity. Although Plaintiffs purport to sue the Defendants in their individual capacities, the DISH/NagraStar Defendants urge the Court to regard

this case as an official-capacity suit because the Second Amended Complaint "asserts RICO claims against the federal officials and DISH/NagraStar investigators, among others, complaining of actions taken by them in furtherance of official duties." *Id.* at 14. Moreover, the DISH/NagraStar Defendants contend that sovereign immunity bars Plaintiffs' RICO claims because "a suit against federal agencies or federal officials in their official capacity is essentially a suit against the United States," Plaintiffs ask for money damages, and Plaintiffs fail "to allege any unequivocal waiver of the federal government's sovereign immunity for their RICO claims and cannot evade the sovereign immunity bar here through artful pleading." *Id.* at 14-15.

Addressing Plaintiffs' RICO claims, the DISH/NagraStar Defendants first argue that "Plaintiffs cannot plead a cognizable RICO enterprise on the facts." *Id.* at 16 (capitalization altered). They maintain that "Plaintiffs still fail to allege plausible facts supporting the required structural features of an association-in-fact enterprise." *Id.* at 18. According to the DISH/NagraStar Defendants, their "alleged association with the Federal Defendants in carrying out law enforcement activities of investigative work and execution of search warrants does not give rise to a cognizable RICO enterprise and those claims must be dismissed." *Id.* at 18-19.

The DISH/NagraStar Defendants further maintain that

"Plaintiffs cannot plead conduct of a criminal enterprise that is separate and apart from the conduct of Defendants' own affairs." *Id.* at 19 (capitalization altered). They assert that "Plaintiffs fail to plead factual allegations establishing how the DISH/NagraStar Defendants took any part in the 'operation or management' of the alleged RICO enterprise," *id.* at 20 (quoting *Reves v. Ernst & Young*, 507 U.S. 170, 185, 113 S.Ct. 1163, 122 L.Ed.2d 525 (1993)), and that "any contention that the DISH/NagraStar Defendants operated or managed the enterprise's affairs directly contradicts Plaintiffs' own allegations that the DISH/NagraStar Defendants acted 'as federal agents' under color of federal law at the direction and supervision of the Federal Defendants." *Id.* (quoting *Second Am. Compl.* ¶¶ 21-22).

***10** In the DISH/NagraStar Defendants' view, Plaintiffs also "cannot plead a pattern of racketeering activity on the facts." *Id.* at 20 (capitalization altered). The DISH/NagraStar Defendants argue that the acts identified by Plaintiffs "are insufficient to establish predicate offenses under RICO or the continuity required to demonstrate RICO's pattern of racketeering activity." *Id.* They further conclude that the Second Amended Complaint "alleges no 'distinct threat of long-term racketeering activity,' real risk of 'future criminal conduct,' or predicate acts that 'are part of an ongoing entity's regular way of doing business,' " meaning that

Plaintiffs have failed to allege the pattern of racketeering activity necessary to support a civil RICO claim. *Id.* at 21-22 (quoting *H.J. Inc. v. Nw. Bell Tel. Co.*, 492 U.S. 229, 242-43, 109 S.Ct. 2893, 106 L.Ed.2d 195 (1989)).

Turning to Plaintiffs' RICO conspiracy claim, the DISH/NagraStar Defendants suggest this claim "fails for two independent reasons." *Id.* at 22. First, they contend that the RICO conspiracy claim must be dismissed because Plaintiffs failed to plead a viable substantive RICO claim. *Id.* Further, they argue that "Plaintiffs' allegations of agreement and conspiracy are too vague and conclusory to state a claim for relief." *Id.*

Having fully addressed Plaintiffs' RICO claims, the DISH/NagraStar Defendants turn to the CFAA claim. According to the DISH/NagraStar Defendants, the Second Amended Complaint fails "to state a viable CFAA violation for two independent reasons: (i) accessing Plaintiffs' computers pursuant to a search warrant under color of federal law at the direction and supervision of the Federal Defendants does not constitute 'unauthorized access' or 'exceeding authorized access'; and (ii) Plaintiffs' claims of lost profits and trade secrets are not cognizable losses under the CFAA." *Id.* at 23-24. The DISH/NagraStar Defendants add that "Plaintiffs' assertion that the DISH/NagraStar Defendants harvested some malicious motive in aiding the Federal Defendants' execution of the search warrants ... does not

alter this analysis." *Id.* at 26 n.17 (citing *Van Buren v. United States*, 593 U.S. 374, 141 S. Ct. 1648, 1655, 210 L.Ed.2d 26 (2021)).

Similarly, the DISH/NagraStar Defendants contend that "Plaintiffs' SCA claim is legally untenable because ... any wire or electronic communications purportedly accessed by the DISH/NagraStar Defendants, during the warrants' execution" are exempt from SCA liability under the statutory exceptions for law enforcement activity and good-faith reliance on a search warrant. *Id.* at 26-27. They put forth a similar argument with respect to Plaintiffs' DMCA claim, maintaining that their "conduct falls squarely within the DMCA's law enforcement activity exception and is exempt from liability." *Id.* at 28. Moreover, according to the DISH/NagraStar Defendants, Plaintiffs' allegation that they "used password dumps under the direction and supervision of the Federal Defendants" is insufficient to trigger DMCA liability because "[t]hat conduct ... does not constitute 'circumvention' for DMCA purposes." *Id.*

Finally, the DISH/NagraStar Defendants discuss Plaintiffs' DTSA and PTSA claims. They argue that their "conduct does not fall within the scope of conduct prohibited under the DTSA" because lawful means of acquisition are exempted from the statute. *Id.* at 29. Further, the DISH/NagraStar Defendants say that because their "purported acquisition of Plaintiffs' trade

secrets represents either a lawful disclosure made in confidence to federal officials for the purpose of 'investigating a suspected violation of law,' or a 'lawful means of acquisition' conducted at the behest of federal officials in compliance with a search warrant, a cause of action under the DTSA is untenable." *Id.* at 30. Relatedly, the DISH/NagraStar Defendants assert that the PTSA claim fails because their conduct did not constitute "misappropriation," and Plaintiffs cannot satisfy the "improper means" requirement of the statute. *Id.* at 30-31.

***11** The DISH/NagraStar Defendants conclude by asking the Court to dismiss all the claims in the Second Amended Complaint with prejudice because "any further amendments would be futile and further exhaust the resources of the Court, the Federal Defendants, and the DISH/NagraStar Defendants." *Id.* at 31-32.

b. Plaintiffs' Opposition

In response, Plaintiffs first argue that "the DISH/NagraStar Defendants are not entitled to qualified immunity from Plaintiffs' RICO claims." *Pls.' Opp'n* at 11. According to Plaintiffs, the "special policy concerns involved in suing government officials" are "lacking" with respect to private parties. *Id.* at 13 (citing *Wyatt v. Cole*, 504 U.S. 158, 112 S.Ct. 1827, 118 L.Ed.2d 504 (1992)). Even if private parties can invoke qualified immunity,

Plaintiffs continue, "the proposed [Second Amended Complaint] also states the Dish/Nagrastar defendants' criminal and civil violations were clearly established and prohibited at the time they committed the crime." *Id.* at 14.

Plaintiffs then pivot to arguing that "the procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Id.* at 18 (capitalization altered). They contend that the DISH/NagraStar Defendants and the Federal Defendants jointly procured search warrants that "contained materially false representations and perjured testimony," and ultimately lacked probable cause. *Id.* at 18-19. Additionally, Plaintiffs submit that "the alleged initial probable cause dissipated with the first search warrant execution," and thus the second search was "illegal and warrantless." *Id.* at 22.

Plaintiffs go on to argue that "the affidavit in support of the search warrant was defective on its face." *Id.* at 24 (capitalization altered). They contend that their computer systems were protected under the SCA, that the "conclusory" statements in the affidavit were insufficient to justify a search, and that the search ultimately did not comply with the SCA. *Id.* at 24-25. According to Plaintiffs, the Federal Defendants "did not seek authorization from the Magistrate to bring

Plaintiffs' competitors, the Dish/Nagrastar defendants, to execute the search warrant,"and although Plaintiffs concede that 18 U.S.C. § 3105 allows private parties to assist in the execution of a search warrant, they counter that "the statute clearly prohibited the executing officer from bringing to the search a party which had another interest, profit, or other marketplace incentive." *Id.* at 28-29. Further, Plaintiffs submit that the DISH/NagraStar Defendants cannot rely on the search warrants to justify their actions because the Federal Defendants conceded the invalidity of the search warrants when they did not oppose Plaintiffs' motion for return of property under Federal Rule of Criminal Procedure 41(g). *Id.* at 30-32.

Shifting gears, Plaintiffs contend that "the *Noerr-Pennington* doctrine does not apply to the case at bar." *Id.* at 33 (capitalization altered). This is so, they continue, because the DISH/NagraStar Defendants' "grievance was a sham, knowingly assisted and carried out by the Federal defendants in order to gain access to Plaintiffs' premises and deprive them of their intellectual and trade secret property." *Id.* at 35-36. Plaintiffs maintain that the *Noerr-Pennington* doctrine "does not protect 'objectively baseless' sham litigation." *Id.* at 36.

***12** Plaintiffs next argue that RICO does not contain any waiver of sovereign immunity. *Id.* at 36-37. They submit

further that "the charges in this civil action were not brought against the United States, but against specific federal official/agents and the Dish/NagraStar defendants, in their individual and personal capacities, for criminal actions indictable under RICO, falling outside their scope of employment, and beyond their statutory authority," and thus, "Plaintiffs are allowed to prosecute under equitable civil remedies of the United States laws." *Id.* at 37.

Turning to the RICO counts, Plaintiffs submit that they have pleaded "a colorable RICO claim on the facts" because they have pleaded "enough facts in the [Second Amended Complaint to give] defendants a fair notice of what there is, and the grounds upon [which] they rest." *Id.* at 37-38 (capitalization altered). They add that they have also "pleaded a cognizable RICO enterprise on the facts." *Id.* at 39-41 (capitalization altered).

Plaintiffs further maintain that they have sufficiently "pleaded conduct of a criminal enterprise that is separate and apart from the conduct of Defendants' own affairs." *Id.* at 41 (capitalization altered). In their view, the three required elements for establishing a RICO enterprise are: 1) "an ongoing organization, formal or informal"; 2) that "the various associate[s] function as a continuing unit"; and 3) that the enterprise exists "separate and apart from the pattern of activity in which it engages." *Id.* at 42 (quoting *United States v. Turkette*, 452 U.S. 576, 583,

101 S.Ct. 2524, 69 L.Ed.2d 246 (1981)). Plaintiffs assert that while they "will ultimately need to establish each of these factors, at this early juncture it is sufficient to merely [ ] allege the existence of an association-in-fact enterprise." *Id.* (quoting *Pappa v. Unum Life Ins. Co. of Am.*, No. 3:07-cv-0708, 2008 WL 744820, at *——– – ——–, 2008 U.S. Dist. LEXIS 21500 at *29-30 (M.D. Pa. Mar. 18, 2008)). They add that it is reasonable to infer from the Second Amended Complaint that "the Association in Fact defendants functioned as a continuing unit and had an ascertainable structure distinct from that inherent in the conduct of a pattern of racketeering activity." *Id.* at 44.

Plaintiffs argue that they have established a pattern of racketeering activity because they have "pleaded that the Association in Fact defendants committed over 30 racketeering acts ranging from Mail and Wire fraud to theft of trade secrets, in a period of two years which began in July 2017 and ended in August 2019." *Id.* at 46. In their view, these "facts satisfied the closed period of repeated conduct," and there are also "allegations of a threat of continued activity, in reference to the Dish Network and Nagrastar corporation joint venture." *Id.* at 46-47.

Plaintiffs submit further that they have pleaded a viable RICO conspiracy claim because 18 U.S.C. § 1962(d) "criminalizes an agreement rather than any substantive

criminal offense," meaning that "an agreement to associate with and participate in a yet-to-be formed racketeering enterprise that would affect interstate commerce constitutes a completed offense under § 1962(d)." *Id.* at 48-49 (citing *Salinas v. United States*, 522 U.S. 52, 62, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997)). Plaintiffs therefore conclude that a substantive RICO claim is not required for a viable RICO conspiracy claim, although they maintain they have adequately alleged a substantive RICO claim. *Id.* at 49-50.

Turning to their CFAA claim, Plaintiffs first argue that they do not need to satisfy the heightened pleading requirements of Federal Rule of Civil Procedure 9(b). *Id.* at 50. They then reiterate their view that the DISH/ NagraStar Defendants cannot rely on the search warrants because the government, in failing to oppose Plaintiffs' motion for return of property, conceded that the warrants were invalid. *Id.* at 51-52. Further, Plaintiffs maintain that they have demonstrated cognizable losses under the CFAA because they "allege they incurred damages and loss in excess of $5,000 as a proximate result of Defendants' conduct." *Id.* at 53, 118 S.Ct. 469.

***13** Plaintiffs similarly argue that the DISH/NagraStar Defendants cannot rely on the warrants as a defense to the SCA claim because "the Magistrate did not authorize access into Plaintiffs' electronic communications"

pursuant to the SCA. *Id.* at 55. They then argue that they have satisfied the first and second elements of a SCA claim. *Id.* at 58-63. In particular, with respect to the second element, Plaintiffs maintain that the second search of the Data Center was a trespass, and "[p]ermission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances." *Id.* at 59-61.

Briefly addressing their DMCA claim, Plaintiffs argue that the DISH/NagraStar Defendants' motion should be denied for the "same factual and legal reasons" that apply to Plaintiffs' CFAA and SCA claims. *Id.* at 63-64.

Finally, Plaintiffs address their DTSA and PTSA claims. *Id.* at 64-68. They maintain that they have pleaded all the elements of a viable DTSA claim and urge the Court to "find that it is likely Plaintiff will be able to demonstrate a present and ongoing threat to its trade secrets." *Id.* at 66-67. According to Plaintiffs, "the DTSA authorizes relief even in cases of threatened misappropriation," and, regardless, the Second Amended Complaint demonstrates that the DISH/NagraStar Defendants misappropriated their trade secrets. *Id.* at 67-68. Plaintiffs suggest that because they adequately pleaded their DTSA claim, their PTSA claim must also survive because the standards under both statutes are the same. *Id.* at 64-65.

c. The DISH/NagraStar Defendants' Reply

The DISH/NagraStar Defendants begin by reiterating that Plaintiffs' RICO claims are barred by qualified immunity. *Defs.' Reply* at 2-4. They submit further that the Federal Defendants did not waive qualified immunity by failing to oppose the motion for return of property, arguing that "the Federal Defendants were not required to raise the qualified immunity defense in that proceeding to preserve their defense," and the Federal Defendants "did not make any concessions concerning the qualified immunity defense." *Id.* at 2-3.

Next, the DISH/NagraStar Defendants argue that Plaintiffs' reliance on the "sham" exception to *Noerr-Pennington* immunity "is misplaced." *Id.* at 5. This is so, they continue, because "a magistrate judge found probable cause sufficient to issue search warrants based on the petitioning conduct." *Id.* at 6. The DISH/NagraStar Defendants further aver that "Plaintiffs cannot dispute that the DISH/NagraStar Defendants' petitioning conduct was to procure legitimate government action to halt what they believed to be infringement and circumvention of copyrighted content." *Id.* at 6. Therefore, the DISH/NagraStar Defendants maintain that their "alleged petitioning activities prompting the government's investigation into Plaintiffs' infringing conduct can hardly be said to have been a sham." *Id.* at 7.

Turning to the elements of Plaintiffs' RICO claims, the DISH/NagraStar Defendants assert that "Plaintiffs make no attempt to detail the structure of the alleged RICO enterprise." *Id.* at 8. In their view, the allegations in the Second Amended Complaint "indicate neither the mechanics of a cohesive organization nor the efforts of a collaborative, decision-making operation guiding the enterprise's misdeeds." *Id.* at 10. The DISH/NagraStar Defendants further reiterate that their "alleged association with the Federal Defendants to carry out legitimate law enforcement activity simply cannot constitute a cognizable RICO enterprise and the RICO claim must be dismissed." *Id.*

***14** The DISH/NagraStar Defendants then submit that an additional reason for dismissal of the Second Amended Complaint is that "Plaintiffs plead no factual allegations establishing how the DISH/NagraStar Defendants took any part in the 'operation or management' of the alleged RICO enterprise and do not identify, which, if any, DISH/NagraStar Defendant, had a role in 'directing' the alleged enterprise's affairs." *Id.* at 11.

Similarly, the DISH/NagraStar Defendants argue that "Plaintiffs fail to plead any actionable predicate offenses much less a pattern of racketeering activity." *Id.* (capitalization altered). They contend that "Plaintiffs rely on dicta in *Bellville v. Town of Northboro*, 375 F.3d 25, 32

(1st Cir. 2004)" to inaccurately claim "that the First Circuit issued guidelines governing law enforcement's use of civilians in aid of a warrant's execution and to imply that prior judicial approval is required before procuring civilian assistance." *Id.* at 13. Further, they maintain that "the 30+ online purchases made using a pseudonym as part of an undercover investigation to detect pirated IPTV content do no constitute mail fraud or wire fraud, but rather protected, pre-indictment petitioning activities." *Id.* at 14.

Briefly addressing Plaintiffs' RICO conspiracy claim, the DISH/NagraStar Defendants urge dismissal because "Plaintiffs do not allege facts demonstrating that any Defendant agreed to anything—much less that each of them consciously agreed to commit at least two predicate acts or understood the overall objective of the alleged enterprise and knowingly agreed to further its affairs or participate in an 'endeavor, which, if completed, would satisfy all the elements of a substantive [RICO] offense.' " *Id.* at 16 (quoting *United States v. Rodríguez-Torres*, 939 F.3d 16, 23 (1st Cir. 2019)).

Moving on to Plaintiffs' CFAA claim, the DISH/NagraStar Defendants reiterate that their actions were authorized pursuant to valid search warrants, and "Plaintiffs' contention that the search warrants were invalid does not vitiate the Federal Defendants or the DISH/NagraStar Defendants' 'authorized access.' " *Id.* at

16-17. The DISH/ NagraStar Defendants further maintain that Plaintiffs "fail to satisfy the statutory damages requirement" and "their attempt to now proffer text messages and invoices in support of the same should be rejected." *Id.* at 17-18.

In a similar vein, the DISH/NagraStar Defendants argue that "because Plaintiffs' SCA claim is predicated upon the DISH/NagraStar Defendants' alleged access to Plaintiffs' computers during the Federal Defendants' execution of the search warrants, any wire or electronic communications purportedly accessed by the DISH/NagraStar Defendants falls within" enumerated statutory exceptions for law enforcement conduct or good-faith reliance on a search warrant. *Id.* at 18-19.

Turning to Plaintiffs' DMCA claim, the DISH/NagraStar Defendants suggest that Plaintiffs' opposition brief contains new allegations under the DMCA's anti-trafficking provisions. *Id.* at 19. "To the extent Plaintiffs seek to amend their [Second Amended Complaint] to advance an anti-trafficking claim," the DISH/NagraStar Defendants continue, "their motion to amend should be denied." *Id.* Further, the DISH/NagraStar Defendants reiterate that Plaintiffs' DMCA claim should be dismissed because "the alleged conduct does not constitute 'circumvention' " and "it falls squarely within the DMCA's law enforcement activity exception." *Id.* at 20.

***15** Finally, the DISH/NagraStar Defendants discuss Plaintiffs' DTSA and PTSA claims. *Id.* at 20-21. In their view, "Plaintiffs' DTSA claim does not plausibly plead misappropriation ... because [the Second Amended Complaint] makes plain that rather than acquiring trade secrets by improper means, the DISH/NagraStar Defendants purportedly acquired them while 'acting as federal agents' under the direction and supervision of the Federal Defendants." *Id.* at 20 (quoting *Second Am. Compl.* ¶¶ 21-22). Additionally, the DISH/NagraStar Defendants argue their conduct "is otherwise exempt from liability under the lawful government activity provision or the immunized disclosure parameters." *Id.* The DISH/NagraStar Defendants aver that Plaintiffs' PTSA claim should be dismissed for similar reasons. *Id.* at 21.

d. Plaintiffs' Sur-Reply

In their sur-reply, Plaintiffs request that the Court reject or strike all the arguments in the DISH/NagraStar Defendants' reply that do not address a "new matter." *Pls.' Reply* at 1-2. Plaintiffs aver that the only "new matter" in the DISH/NagraStar Defendants' reply is the contention that Plaintiffs are trying to further amend their complaint to assert anti-trafficking claims under the DMCA. *Id.* at 2. Plaintiffs therefore ask the Court to disregard the remainder of the DISH/NagraStar

Defendants' reply. *Id.* at 3-6. Further, Plaintiffs argue that their Second Amended Complaint includes allegations pursuant to the anti-trafficking provisions of the DMCA. *Id.* at 6.

Plaintiffs conclude by asking the Court to deny the DISH/NagraStar Defendants' motion to dismiss because the Second Amended Complaint "sets forth a short and plain statement showing that they are entitled to relief" and to strike all the defenses raised by the DISH/NagraStar Defendants. *Id.* at 8-9.

IV. LEGAL STANDARD

Rule 12(b)(6) requires dismissal of a complaint that "fail[s] to state a claim upon which relief can be granted." FED. R. CIV. P. 12(b)(6). To state a claim, a complaint must contain, among other things, "a short and plain statement of the claim showing that the pleader is entitled to relief." FED. R. CIV. P. 8(a)(2). In other words, a complaint must contain "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting *Bell Atl. Corp*. v. *Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). A claim is facially plausible when "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing

Twombly, 550 U.S. at 556, 127 S.Ct. 1955). Plausible means " 'something more than merely possible' or 'merely consistent with a defendant's liability.' " *Germanowski v. Harris*, 854 F.3d 68, 71-72 (1st Cir. 2017) (internal citation omitted) (quoting *Schatz v. Republican State Leadership Comm.*, 669 F.3d 50, 55 (1st Cir. 2012)); *Ocasio-Hernández v. Fortuño-Burset*, 640 F.3d 1, 11 (1st Cir. 2011). This is a " 'context-specific' job that compels [judges] 'to draw on' [their] 'judicial experience and common sense.' " *Schatz*, 669 F.3d at 55 (quoting *Iqbal*, 556 U.S. at 679, 129 S.Ct. 1937).

This is a "two-step analysis." *Cardigan Mountain Sch. v. N.H. Ins. Co.*, 787 F.3d 82, 84 (1st Cir. 2015). "First, the court must distinguish 'the complaint's factual allegations (which must be accepted as true) from its conclusory legal allegations (which need not be credited).' " *García-Catalán v. United States*, 734 F.3d 100, 103 (1st Cir. 2013) (quoting *Morales-Cruz v. Univ. of P.R.*, 676 F.3d 220, 224 (1st Cir. 2012)); *see also Schatz*, 669 F.3d at 55 (stating that a court may "isolate and ignore statements in the complaint that simply offer legal labels and conclusions or merely rehash cause-of-action elements"). "Second, the court must determine whether the factual allegations are sufficient to support 'the reasonable inference that the defendant is liable for the misconduct alleged.' " *García-Catalán*, 734 F.3d at 103 (quoting *Haley v. City of Boston*, 657 F.3d 39, 46 (1st Cir. 2011)).

V. DISCUSSION

a. Plaintiffs' Request to Strike the DISH/NagraStar Defendants' Reply

***16** The Court begins by addressing Plaintiffs' argument that "the Court should either reject and/or strike from the Dish/NagraStar defendants' Reply any portion not addressing a new matter." *Pls.' Sur-Reply* at 1. Plaintiffs submit "that [upon] close examination[,] the Dish/Nagrastar defendants' factual argument and legal authorities[ ] did not contribute anything new that they had not already discussed in their [motion to dismiss], and their Reply is nothing more than a second response." *Id.* at 2.

The Court disagrees. Plaintiffs rely on District of Puerto Rico Local Civil Rule 7(c), which provides:

With prior leave of court and within seven (7) days of the service of any objection to a motion, the moving party may file a reply, which shall not exceed ten (10) pages in length, and which shall be strictly confined to responding to new matters raised in the objection or opposing memorandum. As this rule makes clear, a reply is proper so long as it addresses "new matters raised in the ... opposing memorandum." *Id.*

Plaintiffs reason that the DISH/NagraStar Defendants' reply is noncompliant because it contains the same general arguments as their motion to dismiss. For example, Plaintiffs ask the Court to strike the reply's discussion of the *Noerr-Pennington* doctrine because "this issue was raised and discussed by the DISH/NagraStar Defendants in their [motion to dismiss]." *Pls.' Sur-Reply* at 4. But this reads Local Rule 7(c) too narrowly and the DISH/ NagraStar Defendants' reply too strictly. The Court does not view Local Rule 7(c) as prohibiting a reply from expanding upon issues raised both in the original memorandum and the response so long as the response addressed the issue. *See Torres-Talavera v. Ford Motor Co.*, 965 F. Supp. 2d 220, 222 n.3 (D.P.R. 2013) (noting that, pursuant to Local Civil Rule 7(c), the plaintiffs' sur-reply was "confined to respond to the arguments made in defendant Ford's reply").

The Court's review of the reply's discussion of the *Noerr-Pennington* doctrine reveals that it focuses on Plaintiffs' argument, raised for the first time in their opposition brief, that the "sham" exception to the *Noerr-Pennington* doctrine applies. *See Defs.' Reply* at 4-7. The Court's further examination of the other supposedly recycled arguments in the DISH/NagraStar Defendants' reply yields similar results. While the DISH/NagraStar Defendants' reply discusses the same subject matter as their motion to dismiss, the specific arguments in the reply are different and respond to the arguments in

Plaintiffs' opposition brief. Therefore, the reply is proper under Local Civil Rule 7(c).

The Court denies Plaintiffs' request to strike. [7]

b. Plaintiffs' RICO and RICO Conspiracy Claims

To state a civil RICO claim under 18 U.S.C. § 1962(c), a plaintiff must allege four elements: (1) conduct; (2) of an enterprise; (3) through a pattern; (4) of racketeering activity. *Lerner v. Colman*, 26 F.4th 71, 77 (1st Cir. 2022) (citing *Sedima, S.P.R.L. v. Imrex Co.*, 472 U.S. 479, 496, 105 S.Ct. 2787, 86 L.Ed.2d 384 (1985)). "Racketeering activity" is defined to include a variety of predicate offenses, including mail fraud, wire fraud, and theft of trade secrets. 18 U.S.C. § 1961(1). The civil-suit provision of the RICO statute grants the right to sue to "[a]ny person injured in his business or property by reason of a violation of" the substantive provisions of the statute. *Id.* § 1964(c).

***17** Civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron v. Embassy Suites (P.R.), Inc.*, 223 F.3d 12, 20 (1st Cir. 2000). "[I]n cases alleging civil RICO violations, particular care is required to balance the liberality of the Civil Rules with the necessity of preventing abusive or vexatious treatment of

defendants." *Miranda v. Ponce Fed. Bank*, 948 F.2d 41, 44 (1st Cir. 1991), *abrogated on other grounds by Salinas v. United States*, 522 U.S. 52, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997). "Civil RICO is an unusually potent weapon—the litigation equivalent of a thermonuclear device. The very pendency of a RICO suit can be stigmatizing and its consummation can be costly." *Id.* Accordingly, "courts should strive to flush out frivolous RICO allegations at an early stage of the litigation." *Figueroa Ruiz v. Alegria*, 896 F.2d 645, 650 (1st Cir. 1990).

1. RICO Enterprise

a. Legal Framework

In interpreting the RICO "enterprise" requirement, the Supreme Court has explained that "there is no restriction upon the associations embraced by the definition: an enterprise includes any union or group of individuals associated in fact." *Turkette*, 452 U.S. at 580, 101 S.Ct. 2524. The enterprise concept is not unbounded, however, because an enterprise must be "an entity, for present purposes a group of persons associated together for a common purpose of engaging in a course of conduct." *Id.* at 583, 101 S.Ct. 2524. In cases "involving an alleged associated-in-fact RICO enterprise, the existence of the charged enterprise does not follow, ipso facto, from evidence that those named as the enterprise's associates engaged in crimes that collectively may be characterized

as a 'pattern of racketeering activity.' " *United States v. Cianci*, 378 F.3d 71, 81 (1st Cir. 2004).

Put differently, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of 'racketeering activity' do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.* at 82. Ultimately, the First Circuit has "read *Turkette* to impose a requirement that those associated in fact function as an ongoing unit and constitute an ongoing organization. Also important to such an enterprise is that its members share a common purpose." *Id.* at 82 (internal quotations omitted). Finally, the existence of an enterprise "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Turkette*, 452 U.S. at 583, 101 S.Ct. 2524.

"Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice," *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937, especially where "plaintiffs attempt to camouflage conclusory statements as allegations of fact." *A.G. ex rel. Maddox v. Elsevier, Inc.*, 732 F.3d 77, 81 (1st Cir. 2013).

b. Analysis

After sifting out Plaintiffs' conclusory statements, Court views the RICO allegations as pleaded as wafer thin, and the well-pleaded facts remaining are insufficient to establish that the alleged association in fact "function[ed] as an ongoing unit" or constituted an "ongoing organization." *Cianci*, 378 F.3d at 82 (internal quotations omitted).

As to the enterprise requirement, the Second Amended Complaint offers that, starting in 2017, all Defendants conspired at the outset and together "formed an Association in Fact, [including] Legal Entity Enterprises that would help the Association in Fact defendants advance the purpose and goals of the Racketeering Enterprises' conspiratorial objectives in misappropriating themselves from Plaintiffs' DISME intellectual technology property, and trade secrets." *Second Am. Compl.* ¶¶ 17-18; *see also id.* ¶¶ 126-28. It adds that the "Association-In-Fact defendants knowingly agreed, combined, and conspired to conduct the affairs of the Racketeering Enterprise in attempting and committing theft of trade secrets through a hoax criminal investigation operation." *Id.* ¶ 155.

***18** The Second Amended Complaint does assert that on August 7, 2017, Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel "instructed" Mr. Jaczewski to purchase a

Naicom TV set-top-box receiver as part of an operation "supervised and approved" by the Federal Defendants. *Id.* ¶¶ 133-34. It also alleges that Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel subsequently "supervised and approved" Mr. Jaczewski's payments to Naicom. *Id.* ¶ 135. However, these allegations are almost entirely vague, conclusory, and devoid of factual development. At best, they describe the inner workings of the association in fact in a few isolated instances. But they fail to adequately describe how, apart from these isolated instances, the alleged association in fact 'function[ed] as an ongoing unit' or constituted an "ongoing organization" during the two-plus years it allegedly existed. *Cianci*, 378 F.3d at 82 (internal quotations omitted). In short, Plaintiffs offer virtually no well-pleaded facts explaining how the conspirators functioned together as an ongoing unit or organization.

Plaintiffs attempt to compensate for this lack of well-pleaded facts by offering that "[t]he Association-In-Fact defendants had an ongoing organizational framework for carrying out the Racketeering Enterprises' criminal objectives" because "[t]he Association-In-Fact defendants could not have carried out the intricate task of robbing Plaintiffs' Intellectual Property and Trade Secrets ... unless it had some structure for making and communicating group decisions." *Second Am. Compl.* ¶ 130. The Court views this allegation as the epitome of a "[t]hreadbare recital[ ] of the elements of a cause of

action, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937. It merely restates the requirement that the enterprise have an organizational framework, supported by nothing but the circular logic that the purported enterprise could not have succeeded unless it were truly an enterprise. There is, however, an obvious alternative explanation: the DISH/NagraStar Defendants were assisting the Federal Defendants with a legitimate law enforcement investigation, not joining with them to steal Plaintiffs' intellectual property as part of an elaborate conspiracy. These allegations do not adequately plead the existence of an "ongoing unit" or "ongoing organization" required for a RICO claim. *Cianci*, 378 F.3d at 82 (internal quotations omitted)

Furthermore, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of 'racketeering activity' do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.*; *see also Bachman v. Bear Stearns & Co., Inc.,* 178 F.3d 930, 932 (7th Cir. 1999) (noting that a contrary rule would erroneously make "every conspiracy to commit fraud ... a RICO [enterprise] and consequently every fraud that requires more than one person to commit ... a RICO violation"). While Plaintiffs assert that the DISH/NagraStar Defendants have

previously been involved in trade secret misconduct, [8] *see Second Am Compl.* ¶ 129; *Pls.' Opp'n* at 4-5, they do not allege that this association in fact as a whole has engaged or will engage in any misconduct unrelated to the one-off goal of stealing Plaintiffs' intellectual property. In its review of the Second Amended Complaint, the Court is unable to find the "[s]omething more" that "must be found ... that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Cianci*, 378 F.3d at 82.

***19** As noted earlier, Civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron*, 223 F.3d at 20. Ultimately the Court concludes that the Second Amended Complaint, when stripped of its conclusory allegations, does not assert sufficient facts to plead the existence of a RICO enterprise, and that Plaintiffs' RICO claim must fail.

2. Pattern of Racketeering Activity

Plaintiffs must also plead a "pattern of racketeering activity," which "means the commission of at least two related acts of racketeering activity during a period of ten years." *Humana, Inc. v. Biogen, Inc.*, 666 F. Supp. 3d 135, 147 n.4 (D. Mass. 2023) (citing 18 U.S.C. § 1961(5)). "Racketeering activity" is defined to include a variety of

predicate offenses, including mail fraud, wire fraud, and theft of trade secrets. 18 U.S.C. § 1961(1). The First Circuit has observed that the Supreme Court has found "that the civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements." *In re Neurontin Mktg. & Sales Pracs. Litig.*, 712 F.3d 21, 34 (1st Cir. 2013) (citing *Holmes v. Secs. Investor Prot. Corp.,* 503 U.S. 258, 268, 112 S.Ct. 1311, 117 L.Ed.2d 532 (1992)).

Plaintiffs allege that the purported RICO conspiracy's pattern of racketeering activity involved numerous predicate acts, including:

Acts indictable under Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy to Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.), while in addition, committing the possible underlying criminal offenses as prohibited under [the Computer] Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.), 18 U.S.C.A. § 2235-Search warrant procured maliciously; 18 U.S.C.A. § 1621-Perjury generally; 18 U.S.C.A. § 1001-Statements or entries generally, 18 U.S.C.A. § 912-Officer or employee of the United States; 18 U.S.C.A. § 2234-Authority exceeded in executing warrant; 18 U.S.C.A. § 2236-Searches without warrant,

18 U.S.C.A. § 1905-Disclosure of Confidential Information, while accomplishing their racketeering objectives. Second Am. Compl. ¶ 132.

Most of these alleged offenses are not "predicate acts" under the RICO statute. Mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), and theft of trade secrets (18 U.S.C. §§ 1831-1832) [9] qualify; the rest do not. *See* 18 U.S.C. § 1961(1) (listing qualifying offenses).

a. Wire and Mail Fraud

"Mail or wire fraud requires proof of (1) a scheme to defraud based on false pretenses; (2) the defendant's knowing and willing participation in the scheme with the specific intent to defraud; and (3) the use of interstate mail or wire communications in furtherance of the scheme." *Sanchez v. Triple-S Mgmt., Corp.*, 492 F.3d 1, 9-10 (1st Cir. 2007). "The 'in furtherance' requirement is to be read broadly." *United States v. Simon*, 12 F.4th 1, 33 (1st Cir. 2021). "[T]he mails need not be an essential element of the scheme. It is sufficient for the mailing to be incident to an essential part of the scheme, or a step in [the] plot." *Schmuck v. United States*, 489 U.S. 705, 710-11, 109 S.Ct. 1443, 103 L.Ed.2d 734 (1989) (second alteration in original) (internal citations and quotations omitted).

***20** Federal Rule of Civil Procedure 9(b) requires that

"[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." FED. R. CIV. P. 9(b); *see also Humana*, 666 F. Supp. 3d at 154 ("Civil RICO claims based on the predicates of mail or wire fraud must meet the heightened pleading standard of Rule 9(b)"). A complaint must specify "the time, place, and content of an alleged false representation." *United States ex. rel. Kelly v. Novartis Pharms. Corp.*, 827 F.3d 5, 13 (1st Cir. 2016) (quoting *Doyle v. Hasbro, Inc.*, 103 F.3d 186, 194 (1st Cir. 1996)). Furthermore, "[t]he false or fraudulent representation [in a mail or wire fraud claim] must be material." *United States v. Appolon*, 715 F.3d 362, 367 (1st Cir. 2013) (first alteration in original) (citation omitted).

Plaintiffs' mail and wire fraud claims are limited to allegations that Mr. Jaczewski—in an operation "instructed" by Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel and "supervised and approved" by the Federal Defendants—used an alias to purchase two Naicom set-top boxes and a monthly subscription he maintained for two years. *Second Am. Compl.* ¶¶ 132-37. In Plaintiffs' view, each purchase or payment "constitutes a wire fraud racketeering act since [Mr. Jaczewski, acting under the alias] Brian Parsons, posed as [a] legitimate client and used the interstate internet electronic services to access Naicom's website, and register online under the false pretenses of BRIAN PARSONS" and "made online

payments through the use of interstate internet electronic services ... to defraud and deprive Naicom Corporation of its legitimate products, intellectual property and trade secrets." *Id.* ¶ 134. Between the initial purchases and monthly subscription payments, Plaintiffs tally 22 acts of wire fraud. *Id.* ¶ 135. Finally, they also consider the initial purchase to constitute mail fraud because Mr. Jaczewski "posed as a legitimate client and used the United States Postal Services to have Naicom mail him the IPTV Set Top Box to a fake address." *Id.* ¶ 133.

Accepting these allegations as true, the Court concludes that the facts are insufficient to support Plaintiffs' wire and mail fraud claims because the purportedly fraudulent representations (limited to Mr. Jaczewski's use of an alias for the set-top box purchase and subscription) were not material. Nor could the mail and wire fraud allegations be predicate acts for Plaintiffs' RICO claim because the set-top-box operation was not causally connected to Plaintiffs' damages.

A material statement "has a natural tendency to influence, or [is] capable of influencing, the decision of the decision-making body to which it was addressed" but plaintiffs "need not prove that the decisionmaker actually relied on the falsehood or that the falsehood led to actual damages." *Appolon*, 715 F.3d at 368 (alteration in original) (citations and internal quotation omitted). In

Appolon, the defendant provided untrue responses on a mortgage application, in response to questions "that specifically sought information regarding the purchaser's income, assets, and intent to reside in the property." *Id.* The First Circuit considered the false responses material because the questions "were designed to assess the borrower's creditworthiness" and thus the statements "were capable of influencing [the lender's] decision." *Id.*

The purported false statements here are far afield from providing false financial information on a mortgage application. Naicom's set-top boxes are commercial electronic products sold in retail stores like Sam's Club, and its subscription services are available on Apple's AppStore as the Naicom TV App. *Second Am. Compl.* ¶ 70 ("On February 16, 2017, Apple Corporation approved Naicom Corporation App for Apple's AppStore as Naicom TV App"); *id.* ¶ 71 ("On December 15, 2017, Sam's Club approved Naicom Corporation to officially launch and distribute in their retail stores [ ] Naicom's IPTV Set Top Box which offered the distribution of tv programming to customers in Puerto Rico"). Parsing Plaintiffs' allegations, they allege that Mr. Jaczewski committed wire and mail fraud by providing a false name "of BRIAN PARSONS, fake Phone (727) 409-9464, fake Email: parsons.brian716@outlook.com and Address: 9079 FOURTH STREET NORTH SAINT PETERS FL 33702 IP: 70.127.233.139, and made online payments

through the use of interstate internet electronic services using the PM Visa ending in 2775." *Id.* ¶ 134. Plaintiffs also allege that Mr. Jaczewski used the alias of Brian Parsons when purchasing two Naicom set-top boxes. *Id.* ¶ 133.

***21** The allegations confirm that Mr. Jaczewski used the false name of Brian Parsons. It is unclear, however, what Plaintiffs mean by a "fake Phone"—whether Mr. Jaczewski used a different phone as part of the alias or if the number provided was entirely made up. Plaintiffs have not adequately pleaded that the remainder of the "false" statements are actually false. The Second Amended Complaint does not allege that email services require customers to use their real name in their email address. Thus, the Second Amended Complaint fails to allege that using an email with "parsons-brian" in the address is a false statement as there is no allegation that the address itself does not actually exist. It is unclear what Plaintiffs mean by a "fake" address, but again, the Second Amended Complaint also does not allege that online retail customers are prohibited from having a product shipped to any address they desire, and Plaintiffs have offered nothing to suggest that this constitutes a false representation. [10] Likewise, nothing in the Second Amended Complaint suggests that the IP address or credit card involved false statements. [11]

The Court is thus left to consider whether Mr. Jaczewski's purchase of two commercially available products and an accompanying subscription using the name Brian Parsons can support Plaintiffs' alleged mail and wire fraud violations. The Court concludes that it cannot, because—absent allegations to the contrary—a customer providing a false name in such circumstances does not have "a natural tendency to influence, [nor is it] capable of influencing, the decision of the decision-making body to which it was addressed." *Appolon*, 715 F.3d at 368. Nothing in the Second Amended Complaint suggests that the use of this alias was material to Plaintiffs' decision to sell Mr. Jaczewski their commercially available product. There is no allegation that Mr Jaczewski was either known to Plaintiffs or prohibited from purchasing Plaintiffs' products. What is missing is an allegation that the alias could have reasonably affected the "decision of the decision-making body" (for example, Naicom's sales department's decision to process Mr. Jaczewski's payment or ship his order). Absent allegations regarding how Mr. Jaczewski's alias affected Naicom's decision to sell him their product, Plaintiffs have not pleaded material fraud with the requisite particularity. Plaintiffs' wire and mail fraud claims cannot stand and thus do not count as predicate acts in support of their RICO claim.

Furthermore, even if the Court did find the alleged representations material, Plaintiffs' claims fall short of

the causation standard required for a wire or mail fraud-based RICO claim. *Neurontin*, 712 F.3d at 34 ("[T]he civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements" (citing *Holmes,* 503 U.S. at 268, 112 S.Ct. 1311). "The 'central question' in evaluating proximate causation in the RICO context 'is whether the alleged violation led directly to the plaintiff's injuries.' " *Sterling Suffolk Racecourse, LLC v. Wynn Resorts, Ltd.*, 990 F.3d 31, 35 (1st Cir. 2021) (quoting *Anza v. Ideal Steel Supply Corp.*, 547 U.S. 451, 461, 126 S.Ct. 1991, 164 L.Ed.2d 720 (2006)). Quoting the U.S. Supreme Court, the First Circuit has noted that "[a] link [between the RICO predicate acts and the plaintiff's injuries] that is too remote, purely contingent, or indirect is insufficient to show proximate cause." *Id.* (alterations in original) (quoting *Hemi Grp., LLC v. City of New York*, 559 U.S. 1, 9, 130 S.Ct. 983, 175 L.Ed.2d 943 (2010)). In addition, the First Circuit has identified "three functional factors with which to assess whether proximate cause exists under RICO." [12] *Id.* (quoting *Neurontin*, 712 F.3d at 35-36)). The but-for causation question, in contrast, asks whether the plaintiff would have suffered the same injury absent the defendant's violation. *See Neurontin*, 712 F.3d at 34.

***22** Here, the alleged violations fail both causation tests because Plaintiffs portray the set-top-box operation as an unmitigated failure that only provided further proof that Naicom was a legitimate company. They allege that

"after testing Naicom TV several times to identify if it was providing DISH programming, on each case the test *revealed no DISH content*." *Second Am. Compl.* ¶ 90 (emphasis added). After attempting to use the boxes to penetrate Plaintiffs' network and steal their secrets, the "Dish/Nagrastar defendants also informed the Racketeering Enterprises that the Association in Fact defendants couldn't penetrate Naicom's Data Center computers, servers, encoders electronic security system, and that a physical intrusion was necessary to extract the intellectual property from the computers, servers, and encoders by physical access." *Id.* ¶ 93. They allege further that the operation did not yield evidence that would support a search warrant and thus the defendants had to provide "affidavits they knew contained material information known to be false and perjured to create probable cause to gain legal access into Plaintiffs [']private business." *Id.* ¶ 20.

As the Court understands the Second Amended Complaint, Plaintiffs allege that all Defendants conspired from the outset to steal their intellectual property. The set-top-box operation was an attempt to steal Plaintiffs' secrets by reverse engineering the technology and/or penetrating Plaintiffs' networks. But the operation failed. All the Defendants gained was more proof that Naicom was a legitimate company, and they then had to resort to falsifying affidavits to justify physical access to Naicom's Data Center (through a

search warrant) that would finally allow them access to the desired technology. Plaintiffs have not alleged any harm prior or unrelated to the execution of the warrants. Nor have Plaintiffs alleged that the Defendants would not have sought and executed the search warrants had they not undertaken the set-top-box operation.

The Court concludes that there is no connection—proximate or but-for—between the allegedly fraudulent set-top-box purchase and Defendants acquiring Plaintiffs' intellectual property during the execution of the warrants. The alleged mail and wire fraud is "too remote" from Plaintiffs' alleged harms, *Hemi Grp.*, 559 U.S. at 9, 130 S.Ct. 983, and there is no indication that Plaintiffs would not have suffered their alleged harms absent the set-top-box operation. Plaintiffs' Second Amended Complaint thus falls short on both the materiality and causation standards for wire and mail fraud as predicate acts.

b. Theft of Trade Secrets

Plaintiffs also plead that the Federal Defendants committed RICO predicate acts by misappropriating their trade secrets. *See Second Am. Compl.* ¶¶ 138-41. As noted above, RICO predicate offenses include any act indictable under 18 U.S.C. § 1832, relating to theft of trade secrets under the DTSA. 18 U.S.C. § 1961(1). 18 U.S.C. § 1832 provides that "[w]hoever, with intent to

convert a trade secret ... to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information," or attempts to do so, shall be subject to criminal penalties. *Id.* § 1832(a)(1), (a)(4). "Trade secret" is defined broadly to include "all forms and types of financial, business, scientific, technical, economic, or engineering information," as long as "the owner thereof has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." *Id.* § 1839(3). Critically, however, the DTSA also provides that "[t]his chapter does not prohibit ... any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State." *Id.* § 1833(a)(1).

***23** The scope of Plaintiffs' DTSA claims is unclear. Plaintiffs generally allege that "[b]eginning on or before August 7, 2017," Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel, along with the Federal Defendants: "stole, and without authorization misappropriated, took, carried away, or by fraud, artifice, or deception obtained

trade secrets," *Second Am. Compl.* ¶ 138; "did without authorization, spy, reverse engineered, copied, duplicated, downloaded, uploaded, altered, destroyed, replicated, transmitted, delivered, sent, communicated, and/ or conveyed intellectual property and trade secrets," *id.* ¶ 139; and "misappropriated, obtained, or converted without authorization [the trade secrets] to the economic benefit of [the] Racketeering Enterprises and other defendant coconspirators." *Id.* ¶ 140. Additionally, the Second Amended Complaint clearly alleges that the *Federal Defendants* violated the DTSA on August 27 and 29, 2019 (the dates of the search-warrant executions) by "facilitating and assisting" the DISH/NagraStar Defendants' entry into Naicom's facility to steal Naicom's trade secrets. *Id.* ¶ 141. However, it is unclear whether this allegation encompasses the DISH/NagraStar Defendants, as it appears to be targeted at the Federal Defendants.

The only clarity in Plaintiffs' 69-page opposition is their contention that "[t]he record also supports the finding that the Dish/Nagrastar defendants' misappropriations of Plaintiffs' trade secrets by illegal means is unlawful given the way Dish/Nagrastar defendants obtained the same through the illegal search warrant, warrantless executions, and trespass." *Pls.' Opp'n* at 68. Based on the content of Plaintiffs' Second Amended Complaint and their statements in opposition to the DISH/NagraStar Defendants' motion to dismiss, the Court narrows the

scope of the DTSA inquiry to the DISH/NagraStar Defendants' actions related to obtaining and executing the search warrants—discarding any other DTSA allegations as pleaded with insufficient particularity.

The DISH/NagraStar Defendants dispute Plaintiffs' misappropriation of trade secrets claim by arguing that their conduct was "supported by allegations of legitimate government action." [13] *Defs.' Mot.* at 9 (quoting *Kahre v. Damm*, No. 2:07-CV-00231-DAE-RJJ, 2007 WL 9728869, at *7, 2007 U.S. Dist. LEXIS 95978 at *26 (D. Nev. Dec. 18, 2007)). They further submit that "as private individuals enlisted by the Federal Defendants, 'acting as federal agents' under color of federal law at the direction of and in conjunction with the Federal Defendants, to assist in discharging essential government activities, including the ... execution of the search warrants, the DISH/ NagraStar Defendants are not subject to liability under RICO." *Id.* at 11.

In response, Plaintiffs argue that the "procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Pls.' Opp'n* at 18. Because Plaintiffs' misappropriation claims center on the execution of the warrants, and they dispute the validity of the warrants, the Court addresses this issue first.

As a threshold matter, the Court addresses whether the DISH/NagraStar Defendants, as private parties, can justify their actions based on the search warrants. The DISH/NagraStar Defendants submit that their "aiding the Federal Defendants in their execution of search warrants" does not "render the warrants invalid or constitute illegal trespass, as federal law authorizes government officials to procure assistance from private individuals in aid of a search warrant's execution." *Defs.' Mot.* at 9-10. Plaintiffs concede that "[f]ederal constitutional law does not proscribe the use of civilians in searches," and "[c]ourts have recently upheld the practice." *Pls.' Opp'n* at 26-27. They counter, however, that the search warrants here were issued and executed illegally because 1) 18 U.S.C. § 3105 "clearly prohibit[s] the executing officer from bringing to the search a party which had another interest, profit, or other marketplace incentive," 2) the government did not "seek authorization from the Magistrate to bring Plaintiffs' competitors," and 3) "the Dish/Nagrastar defendants were executing the search warrant on their own, as they wanted." *Id.* at 28-29, 130 S.Ct. 983. None of Plaintiffs' arguments has merit.

***24** As Plaintiffs concede, federal law allows private parties to assist in the execution of search warrants. 18 U.S.C. § 3105 provides, in its entirety:

> A search warrant may in all cases be served by

> any of the officers mentioned in its direction or by an officer authorized by law to serve such a warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution.

On its face, the statute allows private parties to assist in the execution of search warrants "in aid of the officer on his requiring it." *Id.*

Plaintiffs contend that 18 U.S.C. § 3105 "clearly prohibit[s]" officers from being assisted by private parties with economic interests adverse to those of a search warrant's target. *Id.* at 29, 130 S.Ct. 983. But the statute does not mention such a prohibition. Further, since the statute allows private-party assistance, enlisting the DISH/NagraStar Defendants may well have been desirable in this case, given the specialized, technical nature of the evidence sought by investigators. *See generally Pls.' Opp'n*, Attach 1. at 272-94, *Aff. in Supp. of an Application for a Search Warrant* (*Warrant Aff.*). Notwithstanding Plaintiffs' insistence to the contrary, the Federal Defendants' decision to enlist the DISN/NagraStar Defendants strikes the Court as reasonable, given the DISH/NagraStar Defendants' likely familiarity with evidence of digital piracy.

Plaintiffs also maintain that the First Circuit, in *Bellville v. Town of Northboro*, 375 F.3d 25 (1st Cir.

2004), announced a rule that any private-party assistance must be authorized by a magistrate judge. *Pls.' Opp'n* at 27-29.

This arguments rests on a misreading of *Bellville*. In *Bellville*, the First Circuit noted that there was *no* authority for a rule requiring magistrate approval for private-party assistance and therefore declined to impose such a rule. *Bellville*, 375 F.3d at 33. The First Circuit did observe that "it might be a 'better practice,' if circumstances permit, for law enforcement officers to disclose to the magistrate that civilians will be involved in the execution of the search and for the warrant to indicate that the magistrate permitted this involvement." *Id.* at 34. But a best practice is not a rule, and the Court declines Plaintiffs' invitation to make the best practice outlined in *Bellville* binding on law enforcement.

Finally, Plaintiffs suggest that the DISH/NagraStar Defendants cannot rely on the warrants because "[t]he evidence collected in this case clearly demonstrates that the Dish/Nagrastar defendants were executing the search warrant on their own, and as they wanted." *Pls.' Opp'n* at 29. From a factual perspective, this contention is inconsistent with the allegations in the Second Amended Complaint. *See Second Am. Compl.* ¶¶ 21-22 (noting the DISH/ NagraStar Defendants were "acting as federal agents"); *id.* ¶ 106 (noting that, during the August 29, 2019 search, the FBI Defendants gave Mr. Smith, Mr.

Gedeon, and Mr. Eichhorn "permission to penetrate Naicom's Data Center and introduce pen drives"). Further, even assuming the DISH/NagraStar Defendants were executing the searches without supervision, that alone does not invalidate the searches. *See Bellville*, 375 F.3d at 34 ("[T]he Fourth Amendment does not explicitly require official presence during a warrant's execution; therefore it is not an automatic violation if no officer is present during a search" (quoting *United States v. Bach*, 310 F.3d 1063, 1066-67 (8th Cir. 2002))). Other than the wholly conclusory allegation that the DISH/NagraStar Defendants were executing the search warrants "as they wanted," Plaintiffs make no allegation that the DISH/NagraStar Defendants did "anything that [they] would not have done if [the Federal Defendants] had been in the room." *See id.*

***25** In short, then, Plaintiffs' arguments that the search warrants were invalid because of the involvement of the DISH/NagraStar Defendants are all unavailing. The Second Amended Complaint clearly alleges, multiple times, that the DISH/NagraStar Defendants were "acting as federal agents" while assisting with the execution of the search warrants. Because such assistance was legally permissible, the Court concludes that the DISH/NagraStar Defendants are able to rely on the search warrants in defending against Plaintiffs' misappropriation claims. Thus, the key question becomes whether the warrants themselves were valid.

The relevant standard for evaluating the validity of a warrant is the *Franks v. Delaware* framework, which requires Plaintiffs to adequately allege that both (1) "a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit" and (2) "the allegedly false statement is necessary to the finding of probable cause." *United States v. Reiner*, 500 F.3d 10, 14 (1st Cir. 2007) (quoting *Franks v. Delaware*, 438 U.S. 154, 155-56, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978)). Plaintiffs cite ten statements that they allege the Defendants "falsely submitted to the Court" in an affidavit supporting their search-warrant application. *Pls.' Opp'n* at 19. The Court has examined each and concludes that none supports Plaintiffs' claims.

The first purportedly false statement identified by Plaintiffs is the Defendants' statement that they believed there was probable cause that Plaintiffs were violating copyright and money laundering laws. *Id.* Plaintiffs allege that this statement is false because:

The execution of the search and seizure warrant in this case did not produce any criminal evidence whatsoever; there was no probable cause. That is why the United States never opposed Plaintiffs ['] Motion for Return of Property under Rule 41(g) of the Fed.R.Crim.P. In fact, they didn't even contend the serious violations Plaintiffs

imputed under *Franks* in the Rule 41(g) motion.

Id. This logic is unavailing. Plaintiffs cannot rely on the circular reasoning that the search's alleged failure to produce incriminating evidence thereby proves the Defendants could not have believed there was probable cause to search. *See Karamanoglu v. Town of Yarmouth*, 15 F.4th 82, 88 (1st Cir. 2021) (defining the probable cause inquiry as "whether, on balance, the facts *known to the officer at the time of the arrest* support probable cause" (emphasis in original)).

Equally inadequate is Plaintiffs' claim that the Federal Defendants' failure to oppose Plaintiffs' motion to return the seized property proves not only that the seized property was not incriminating, but also that there was no probable cause to search in the first place. *See United States v. Pierre*, 484 F.3d 75, 87 (1st Cir. 2007) ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return"). The government's return of the seized hard drives and thumb drives, which—unlike drugs or illegal firearms—are not inherently contraband and can easily be downloaded or duplicated, is consistent with *Pierre*.

Furthermore, Plaintiffs are simply incorrect that success on a Rule 41(g) motion conclusively establishes the invalidity of a search. Rule 41(g) allows motions for return of property from "[a] person aggrieved by an

unlawful search and seizure of property *or* by the deprivation of property." FED. R. CRIM. P. 41(g) (emphasis supplied). Without more, the property's return alone cannot demonstrate an absence of probable cause to search and seize in the first place. Ultimately, Plaintiffs' first purportedly false statement offers nothing to undermine the validity of the warrants and searches.

***26** Second, Plaintiffs offer that the Defendants "assured the Court they had evidence based on an investigation conducted by Nagrastar of Naicom's unauthorized use of Direct TV signal to distribute its programming to its paid subscribers." *Pls.' Opp'n* at 19. Plaintiffs assert that this statement was false because "[t]he United States did not produce any evidence as to the above allegations," whereas "Naicom did produce all the documentary evidence establishing that they were authorized to distribute the copyright material and running a legitimate IPTV system." *Id.*

Again, Plaintiffs appear to be suggesting that exculpatory evidence they produced during the search proves that the affidavit was false. These conclusory assertions tied together by circular logic do not adequately demonstrate the falsity of the affidavit. While Plaintiffs contend that the affidavit did not "produce any evidence" supporting the suggestion that Naicom was distributing DirecTV content without authorization, the affidavit avers that

Naicom's system displayed DirecTV error messages on at least 16 channels (and includes a photo of the message), that Naicom's satellite dishes were precisely oriented in a manner necessary to receive DirecTV satellite signals, that representatives of the companies offering some channels Naicom purported to provide confirmed that Naicom was not licensed to provide them, and other indicia of piracy. *See Warrant Aff.* Simply put, Plaintiffs' argument that the affidavit contained no evidence of piracy is incorrect.

Third, Plaintiffs assert that, during a 2018 FBI site visit of Naicom's property, Mr. Vega "repeatedly told the agent that Naicom was a legal corporation and showed the agent a certificate from the National Cable Television Cooperative (NCTC) on the wall," yet the Federal Defendants still "filed the affidavit containing materially false and perjured statements." *Pls.' Opp'n* at 19-20. It is not clear specifically which "materially false and perjured statements" Plaintiffs are referring to, but the affidavit states that the FBI called NCTC's management group, which confirmed that Naicom was *not* a member. *Warrant Aff.* ¶ 15. Nothing in Plaintiffs' assertion that Mr. Vega told the FBI his company was legitimate and showed them a certificate on the wall establishes that the affidavit's claim—that NCTC management represented to the FBI that Naicom was not a member—was perjured.

Fourth, Plaintiffs contend that the affidavit's claim that Naicom was using the NCTC certificate to create the appearance of legal access to channels was a "false and perjured statement" because an FBI agent took pictures of "Naicom's National Rural Telecommunications Cooperative 'NRCT' Certificate" and Naicom had licenses with other networks. *Pls.' Opp'n* at 20.

Fifth, Plaintiffs focus on the affidavit's claim that an FBI agent spoke with NCTC management, who confirmed that Naicom was not a member of their organization. *Id.* They allege that this "is a false and perjured statement" because Naicom provided evidence that it is a member of the NRTC. *Id.*

The distinction between NCTC and NRTC here is somewhat confusing. It appears that Plaintiffs are alleging that the FBI took pictures of a NRTC certificate on the wall but incorrectly referred to it in the affidavit as a NCTC certificate, or that the FBI mistook their NRTC certificate for an NCTC certificate. However, Plaintiffs also claim that the affidavit's assertion that they are not a member of the NCTC is a perjured statement because they provided evidence that they are a member of the NRTC. Plaintiffs offer no evidence that the latter statement was perjured because proving they are a NRTC member does not contradict the claim that they are not a NCTC member. To the extent that the FBI may have misidentified a NRTC certificate as a NCTC

certificate, the record does not suggest that this "allegedly false statement is necessary to the finding of probable cause," especially given the strength of the other supporting claims in the affidavit. *United States v. Patterson*, 877 F.3d 419, 424 (1st Cir. 2017) (quoting *Franks*, 438 U.S. at 156, 98 S.Ct. 2674).

***27** Sixth, Plaintiffs turn to the affidavit's assertion that FBI agents contacted officials at HBO and DirecTV, who verified that Naicom did not have a relationship with their organizations despite offering HBO content. *Pls.' Opp'n* at 20-21. Plaintiffs claim that "[t]his is a false and perjured statement" because "Naicom provided evidence that it is licensed to distribute HBO and Cinemax programming." *Id.* at 21 (citing *Pls.' Opp'n*, Attach. 1 at 356 (HBO invoice dated August 31, 2019, for roughly $200 per month for "Cable — Private Home" services)). Plaintiffs' claim is unpersuasive for two reasons: (1) this invoice for inexpensive "Cable – Private Home" services does not appear to provide evidence of a licensing agreement; and (2) Plaintiffs have not directly contradicted the purportedly perjured claim, which was that HBO and DirecTV officials represented to the FBI that they did not have a relationship with Naicom.

Seventh, Plaintiffs focus on the affidavit's claim that the "external appearance of the Data Center offered indicia of piracy," calling it a "false and perjured statement" because "[a]t the conclusion of the search and seizure

warrant execution the FBI agents found that [ ] Naicom's equipment (encoders) were provided by the networks authorizing the programming distribution and that the use of the satellite was in fact to download the codes provided by the networks." *Pls.' Opp'n* at 21. Plaintiffs again rely on circular logic, as the discovery of exculpatory evidence at the conclusion of a warrant's execution does not provide a "substantial preliminary showing" that the underlying affidavit was perjured. *Franks*, 438 U.S. at 155-56, 98 S.Ct. 2674.

Plaintiffs' eighth point suffers from the same defect. They claim that the affidavit's statements that there were suspicious financial transactions between Naicom and other businesses owned by Mr. Quinones and Mr. Vega were false and perjured because "[d]uring the execution of the Search Warrant S/A Lange interviewed employees from the Business Office and was provided with financial records," which established "that none of the Corporations were involved in any money laundering activities." *Pls.' Opp'n* at 21-22. Again, the fact that a search did not uncover incriminating evidence does not establish that it was predicated on a perjured affidavit.

Plaintiffs' ninth point takes issue with the affidavit's request to seize computers and data based on claimed probable cause that they contained evidence. *Id.* at 22. Plaintiffs contend that this statement was perjured because "the FBI agents were not looking for any

criminal evidence" during the search and they did "not find[ ] any evidence whatsoever of the crimes described in the warrant, which also denied any probable cause." *Id.* The Court does not fully follow Plaintiffs' logic across these seemingly contradictory assertions, but they appear to use the same circular reasoning (the assertion of probable cause was perjured because the resulting search "denied any probable cause"), along with the conclusory contention that the FBI was not actually looking for evidence. These claims do not undermine the validity of the warrants.

Tenth, Plaintiffs claim that the affidavit's request to seize evidence relating to statutory violations was "false and perjured" because the FBI did not find any evidence at the conclusion of the search-warrant execution. *Id.* Beyond the fact that this argument relies on the same circular logic, an affidavit's request to seize "things and ... records" is not an assertion of fact and cannot be false or perjured. *Id.*

To summarize, none of these purportedly false statements, alone or in combination, satisfies Plaintiffs' burden under the *Franks* standard to overcome the presumed validity of the warrants. Moreover, Plaintiffs offer several additional arguments that are similarly unavailing.

Plaintiffs submit that the August 29, 2019, search was

"illegal" and "warrantless" because "[t]he Federal and Dish/Nagrastar defendants knew for a fact that the first search warrant execution had already denied any criminal wrongdoing, and that the initial alleged probable cause had dissipated." *Id.* at 29. This assertion—that the Defendants knew probable cause had dissipated—is wholly conclusory (especially in light of Plaintiffs' argument that the entire investigation was a hoax, and the agents knew probable cause never existed). Furthermore, the warrant did not expire until September 4, 2019 and courts generally recognize a "reasonable continuation rule" providing that a search may be reasonably continued if the warrant remains valid. [14] *See United States v. Keszthelyi*, 308 F.3d 557, 568-569 (6th Cir. 2002) (describing the rule and collecting cases). Plaintiffs have not offered any well-pleaded, nonconclusory allegations suggesting that the continuance here was unreasonable. [15]

***28** Plaintiffs also contend that the searches were unlawful because the Federal Defendants did not follow the procedure to obtain a Stored Communications Act warrant (also known as an SCA order). *Pls.' Opp'n* at 24-26. But this argument lacks merit because the Federal Defendants appropriately obtained a traditional search warrant in lieu of an SCA order.

SCA orders are different from traditional search

warrants. As one court has explained:

> SCA warrants "are not like the search warrants used in the physical world: they are 'executed' when a law enforcement agent delivers (sometimes by fax) the warrant to the [service provider]. The [service provider], not the agent, performs the 'search'; the [service provider] 'produces' the relevant material to the agent; the user associated with the inbox often never learns that his inbox has been 'searched.' In sum, these are not search warrants at all and to call them such confuses legal terminology."

In re Info. Associated with @gmail.com, No. 16-mj-00757 (BAH), 2017 WL 3445634, at *18, 2017 U.S. Dist. LEXIS 130153, at *52-53 (D.D.C. July 31, 2017) (quoting Paul K. Ohm, *Parallel–Effect Statutes and E–Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1610-11 (2004)). Additionally, the standard for an SCA order is "less stringent than the probable cause standard generally required for a search warrant." *United States v. Taylor*, 54 F.4th 795, 804 (4th Cir. 2022). Finally, even if the Federal Defendants were seeking information protected by the SCA, the statute gives them the option of seeking either an SCA order or a traditional search warrant. [16] *See* 18 U.S.C. § 2703(b) (the government may obtain "a

court order for such disclosure under subsection (d) of this section" *or* "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"); *id.* § 2703(c) (same).

Plaintiffs' argument is groundless because the Federal Defendants were primarily—if not entirely—seeking information not protected by the SCA. Regardless, they obtained search warrants for the facility and computer systems, thereby satisfying the requirements of the SCA. Finally, Plaintiffs submit once again that "[t]he Dish/Nagrastar defendants can't raise at this time the defense that the execution of the search and seizure warrant was authorized, legal and constitutional, which was waived during the Rule 41(g) proceedings, and abandoned forever." *Pls.' Opp'n* at 32. However, as the Court has already explained, the government's decision not to oppose a motion to return property does not affect the validity of the warrant or seizure. *See Pierre*, 484 F.3d at 87 ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return").

In sum, Plaintiffs have failed to adequately challenge the validity of the search warrants or establish that any DISH/NagraStar Defendant impermissibly assisted in the warrants' execution. Plaintiffs have thus failed to plead a DTSA violation as a predicate act in support of their RICO claim. *See* 18 U.S.C. § 1833(a)(1) ("This

chapter does not prohibit ... any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State"). Absent both an enterprise and a pattern of racketeering activity, Plaintiffs' RICO claim must be dismissed as to the DISH/NagraStar Defendants.

***29** These same pleading shortfalls doom Plaintiffs' RICO conspiracy claim. *See Efron*, 223 F.3d at 21 (1st Cir. 2000) ("A conspiracy claim under section 1962(d) may survive a *factfinder's* conclusion that there is insufficient evidence to prove a RICO violation, but if the pleadings do not state a substantive RICO claim upon which relief may be granted, then the conspiracy claim also fails" (citations omitted) (emphasis in original)); *see also Salinas*
v. United States, 522 U.S. 52, 64, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997) ("A conspirator must intend to further an endeavor which, if completed, *would satisfy all of the elements of a substantive criminal offense*, but it suffices that he adopt the goal of furthering or facilitating the criminal endeavor" (emphasis supplied)). The Court therefore dismisses Plaintiffs' RICO conspiracy claim.

c. Plaintiffs' DTSA, CFAA, SCA, and DMCA Claims

The Court's determination that the DISH/NagraStar Defendants' conduct was authorized by valid search

warrants is ultimately also fatal to Plaintiffs' DTSA, CFAA, SCA, and DMCA claims, because each statute has a similar exception for law enforcement activity.

i. The DTSA Claim

Plaintiffs' freestanding DTSA claim alleges the same violation as the DTSA claim offered as a predicate act for the RICO claim, and thus fails for the reasons previously described. While the DTSA does provide a private right of action for owners "of a trade secret that is misappropriated ... if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce," 18 U.S.C. § 1836, this right of action cannot be used to challenge "otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State." *Id.* § 1833(a)(1). The Court dismisses Plaintiffs' DTSA claim.

ii. The CFAA Claim

The CFAA contains virtually the same exception for law enforcement activity. *Compare* 18 U.S.C. § 1833(a)(1) (the DTSA "does not prohibit or create a private right of action for any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State"), *with id.* § 1030(f) (the CFAA "does not prohibit any lawfully authorized

investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States"). In *Smith v. Aldridge*, the plaintiff "allege[d] that Defendant stole his smartphone, which is legally protected under CFAA" but also admitted "that Defendant had a warrant when she accessed his phone." *Smith v. Aldridge*, No. 3:17-cv-01485-HZ, 2018 WL 1434813, at*6, 2018 U.S. Dist. LEXIS 47021 at *18 (D. Or.
Mar. 22, 2018). The district judge observed that "Defendant, therefore, had legal authority to access Plaintiff's phone at the time that she did" and because "Plaintiff admits that Defendant had a warrant, [and] Plaintiff would have to show that the warrant was invalid in order to show that the access was unauthorized [For the plaintiff] to prevail on this CFAA claim, the Court would have to determine that Plaintiff's Fourth Amendment Rights were violated." *Id.* at *18 & n.4.

Because the DISH/NagraStar Defendants' challenged conduct was "lawfully authorized investigative activity" under the search warrants, Plaintiffs have not pleaded a viable CFAA claim. [17]

iii. The SCA Claim

***30** Turning to the SCA claim, "courts in the First Circuit have consistently applied CFAA caselaw in analyzing the

SCA. Thus, the Court's analysis under this statute is the same as under the CFAA." *Sun West Mortg. Co. v. Flores*, No. 15-1082 (GAG), 2016 WL 1030074, at *4, 2016 U.S. Dist. LEXIS 31149 at *11 (D.P.R. Mar. 10, 2016) (citation omitted); *see also Cheng v. Romo*, No. 11-10007-DJC, 2012 WL 602136, at *4, 2012 U.S. Dist. LEXIS 169535 at *10 (D. Mass. Nov. 28, 2012) ("Other district courts within this Circuit have addressed 'access without authorization' and 'exceeding authorization' in considering the analogous provision of the CFAA"). As the Court noted previously, even if the DISH/NagraStar Defendants were helping the Federal Defendants search for information protected by the SCA, the statute gives them an option of seeking either an SCA order or a traditional search warrant. *See* 18 U.S.C. § 2703(b) (the government may obtain "a court order for such disclosure under subsection (d) of this section" *or* "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"); *id.* § 2703(c) (same). Furthermore, even if the warrants were not valid, the SCA still provides that "[a] good faith reliance on ... a court warrant or order is a complete defense to any civil or criminal action brought under this chapter or any other law." *Id.* § 2707(e).

Even if the Court were to assume that the Federal Defendants and the DISH/NagraStar Defendants seized electronic communications protected by the SCA, they did so pursuant to valid warrants and thus did not violate the

statute. Furthermore, even if the warrants were not valid, Plaintiffs' allegations of bad faith are conclusory, and the Defendants would thus still be protected by the good faith defense. *See John K. MacIver Inst. for Pub. Pol'y, Inc. v. Schmitz*, 243 F. Supp. 3d 1028, 1035 (W.D. Wis. 2017), *aff'd*, 885 F.3d 1004 (7th Cir. 2018) ("Given the absence of any case law even suggesting that a state search warrant issued under similar circumstances may be invalid under the SCA, plaintiff's conclusory allegation of a lack of good faith is also wholly insufficient to support a claim that defendants 'actually knew that the [warrant] was invalid [under the SCA]' " (emphasis omitted) (alterations in original) (quoting *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1181 (9th Cir. 2013))). Plaintiffs' SCA claim will not lie against the DISH/NagraStar Defendants for essentially the same reasons as their CFAA claim.

iv. The DMCA Claim

Similarly, the DMCA explicitly provides that it "does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State." 17 U.S.C. § 1201(e). This language is virtually identical to the CFAA's law enforcement exception. *Cf.* 18 U.S.C. § 1030(f) (the CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law

enforcement agency of the United States, a State, or a political subdivision of a State"). This provision of the DMCA has been interpreted as "broadly exempting official law enforcement activity." *Green v. U.S. Dep't of Just.*, 392 F. Supp. 3d 68, 77 (D.D.C. 2019).

As with the DTSA, CFAA, and SCA claims, even assuming Plaintiffs had established all the other elements of a DMCA claim, their claim would still be stymied by the statute's law enforcement exception. Plaintiffs' DTSA, CFAA, SCA, and DMCA claims all fail as pleaded because the challenged searches were conducted pursuant to lawfully authorized warrants.

d. Plaintiffs' PTSA Claim

***31** Finally, Plaintiffs' PTSA claim fails for substantially the same reasons as their CFAA, SCA, DMCA, and DTSA claims. The PTSA provides that "[a]ny natural or juridical person who misappropriates a trade secret shall be held accountable for any damages caused to its owner." P.R. LAWS ANN. tit. 10, § 4134. Relevant here, the PTSA defines "misappropriation" as:

> (a) The acquisition of a trade secret belonging to another by a person who knew or should have known that he/ she acquired such secret directly or indirectly through improper means, or

(b) the disclosure or use of a trade secret belonging to another without his/her express or implicit consent, by a person who:

(1) Used improper means to gain knowledge of the trade secret, or

(2) at the time of disclosure or use, such person knew or should have known that such trade secret was:

(A) Obtained through a person who acquired such information through the use of improper means;

(B) obtained under circumstances from which a duty to maintain confidentiality or to limit use ensues;

(C) obtained through a person who had the duty-bound to the trade secret's owner to maintain confidentiality or limit use, or

(D) known by accident or by mistake.

Id. The PTSA further defines "improper means" as "[u]nlawful means not allowed under the law or which is contrary to free competition and to laws and regulations

in effect, whereby a trade secret is obtained, including, but not limited to, misappropriation, theft, bribery, malfeasance, deceit, breach of contractual duties, wiretapping, or espionage through electronic or other means." *Id.* § 4131.

Like their DTSA claim, Plaintiffs' PTSA claim is not a picture of clarity. Plaintiffs allege that the DISH/NagraStar Defendants "misappropriated" and "exfiltrated" their trade secrets from Naicom's computer system, *Second Am. Compl.* ¶ 197, and that "[e]ach Defendant disclosed, received, and used these misappropriated trade secrets without Plaintiffs' consent, knowing or having reason to know that the trade secrets were acquired by improper means." *Id.* ¶ 199. In opposing the DISH/NagraStar Defendants' motion to dismiss, Plaintiffs represent that the "elements for a misappropriation claim" under the PTSA "are fundamentally the same" as those for a DTSA claim. *Pls.' Opp'n* at 64-65. After parsing the language in the Second Amended Complaint and taking into account Plaintiffs' equation of the DTSA with the PTSA, the Court narrows Plaintiffs' PTSA claim to cover only the DISH/NagraStar Defendants' actions in conjunction with the search-warrant execution and discards all other allegations as insufficiently pleaded.

Plaintiffs' allegations related to the search-warrant executions are insufficient to state a claim for relief

under the PTSA. As noted above, "misappropriation" under the PTSA requires the use of "improper means," which are "means not allowed under the law." But the DISH/NagraStar Defendants' conduct was "allowed under the law," as they were assisting the Federal Defendants with the execution of valid search warrants. Since Plaintiffs are unable to overcome the validity of the search warrants, they cannot show that they are entitled to relief under the PTSA. Therefore, the Court dismisses this claim as well.

VI. CONCLUSION

The Court GRANTS DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel and Jordan Smith's Motion to Dismiss (ECF No. 134). The Court DISMISSES Counts I through VII of the Second Amended Complaint as pleaded against the DISH/NagraStar Defendants.

SO ORDERED.

All Citations

Not Reported in Fed. Supp., 2024 WL 1363462

Footnotes

1 This is the second lawsuit arising out of the underlying events at issue. On August 25, 2020, a group of plaintiffs, including many of Plaintiffs here, filed a *Bivens* action against many of the same defendants. *See Quinones-Pimentel v. Cannon*, No. 3:20-cv-01443-JAW, 2022 WL 826344, at *——–———, 2022 U.S. Dist. LEXIS 48109 at *2-3 (D.P.R. Mar. 17, 2022). On March 17, 2022, the Court dismissed the plaintiffs' *Bivens* action. *Id.* at *88. The plaintiffs appealed, and the Court of Appeals for the First Circuit affirmed the Court's dismissal on October 27, 2023. *Quinones-Pimentel v. Cannon*, 85 F.4th 63, 66-68 (1st Cir. 2023).

2 In their Second Amended Complaint, Plaintiffs use the spelling, "Rinkle." *See, e.g.*, *Second Am. Compl.* ¶ 43. In her filings, however, Ms. Rinkel uses the spelling, "Rinkel." *See, e.g.*, *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Mot. to Dismiss* at 1. No doubt, Ms. Rinkel knows how to spell her own name, and the Court uses "Rinkel" throughout this order.

3 Consistent with Federal Rule of Civil Procedure 12(b)(6), in describing the facts, the Court has relied upon the allegations in the Plaintiffs' Second Amended Complaint. *Foley v. Wells Fargo Bank, N.A.*, 772 F.3d 63, 68 (1st Cir. 2014); *Medina-Velázquez v. Hernández-Gregorat*, 767 F.3d 103, 108 (1st Cir. 2014) ("We examine whether the operative complaint states a claim for which relief can be granted when we construe the well-pleaded

facts in the light most favorable to the plaintiffs, accepting their truth and drawing all reasonable inferences in plaintiffs' favor" (internal citation omitted)).

4 Presumably because Claro Puerto Rico is a well-known business in Puerto Rico, the Second Amended Complaint does not describe Claro Puerto Rico except by name. *See Second Am. Compl.* ¶ 68. According to Wikipedia, Claro Puerto Rico is the one of the largest telecommunications companies in Puerto Rico. *See Claro P.R.*, WIKIPEDIA (updated Oct. 14, 2023), *https://en.Wikipedia.org/wiki/Claro_Puerto_Rico.*

5 Plaintiffs often refer in the Second Amended Complaint to the "Association in Fact defendants." *See, e.g.*, *id.* ¶ 87. As the Court interprets Plaintiffs' complaint, this term refers to all Defendants collectively. *See id.* ¶¶ 17, 62 (listing all the Defendants as together "form[ing] an Association in Fact").

6 Here, the Court quotes the language in the Second Amended Complaint. *Second Am. Compl.* ¶ 103. In the context of this sentence, the meaning of the verb, "counted," is unclear. It would make more sense if the sentence used "complied with," rather than "counted." Whichever verb is correct, however, makes no difference in the Court's ruling on the motion to dismiss.

7 Plaintiffs also suggest that the Court should strike

all the defenses raised by the DISH/NagraStar Defendants under Federal Rule of Civil Procedure 12(f) because "there are no factual issues or issues of law to be resolved before the validity of the defenses in the present context may be determined." *Pls.' Sur-Reply* at 7-8. The Court declines to do so.

8 This allegation is supported only by citations to other lawsuits involving the DISH/NagraStar Defendants. *See Second Am. Compl.* ¶ 129; *Pls.' Opp'n* at 4-5. Even assuming the association in fact involved only the DISH/NagraStar Defendants, which runs counter to many allegations in the Second Amended Complaint, Plaintiffs have still failed to allege how this alternative association in fact functioned as an ongoing unit.

9 The statutory provision cited by Plaintiffs—18 U.S.C. § 1836—discusses civil proceedings for misappropriation of trade secrets and is not listed as a predicate act in 18 U.S.C. § 1961(1). Since the Court assumes that Plaintiffs' reference to 18 U.S.C. § 1836 was in error, the Court has recharacterized their predicate-act allegations relating to theft of trade secrets as arising under 18 U.S.C. §§ 1831 and 1832.

10 In theory, Mr. Jaczewski could have provided an address that was entirely made up. This seems unlikely, however, in light of the Second Amended Complaint's allegations that the Defendants used the set-top boxes to attempt remote attacks on Naicom's servers. Had the boxes been shipped to an address that didn't exist, they

would have been returned to Naicom as undeliverable, meaning that the Defendants could not have used them to launch sniffing attacks. The Plaintiffs do not appear to allege that the mailing address is a fake address, and the Court doubts that they could do so, based on the information in this case.

11 To the contrary, in the Second Amended Complaint, Plaintiffs include a table listing all the payments made to Naicom by Mr. Jaczewski posing as Brian Parsons. *Second Am. Compl.* ¶ 136. In the Court's view, these payments confirm that the credit card number provided by Mr. Jaczewski was valid.

12 These factors are:

(1) "concerns about proof" because "the less direct an injury is, the more difficult it becomes to ascertain the amount of a plaintiff's damages attributable to the violation, as distinct from other, independent, factors," ... (2) "concerns about administrability and the avoidance of multiple recoveries," ... and (3) "the societal interest in deterring illegal conduct and whether that interest would be served in a particular case[.]"*Sterling Suffolk Racecourse*, 990 F.3d at 35-36 (quoting *Neurontin*, 712 F.3d at 35-36).

13 Here, the Court is quoting from the section of the motion that argues the DISH/NagraStar Defendants lacked the requisite criminal intent for liability under RICO. However, from the Court's perspective, these

arguments apply with equal force here because the reason the Defendants lacked criminal intent was that they were acting pursuant to warrants.

14 The "reasonable continuation rule" requires the satisfaction of two conditions: 1) "the subsequent entry must indeed be a continuation of the original search, and not a new and separate search"; and 2) "the decision to conduct a second entry to continue the search must be reasonable under the totality of the circumstances." *Keszthelyi*, 308 F.3d at 569.

15 The closest Plaintiffs come to a nonconclusory allegation is their assertion that U.S. Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned, after the execution of the first search warrant, that Naicom complied with "all the programming distribution contract and agreements." *Second Am. Compl.* ¶ 103. But this allegation is still conclusory, and it is undercut by the sentence immediately following it, which alleges that the USAO Defendants instructed S/A Pearson "to order Darwin Quinones and Victor Vega to report to the FBI Offices in San Juan with the licensing contracts for an interview regarding Naicom's company." *Id.* Clearly, whatever U.S Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned did not absolve Naicom of wrongdoing; otherwise, there would have been no need to conduct an interview.

16 Further, "the statute offers no express direction as

to when the government should seek a warrant versus" a SCA order. *Taylor*, 54 F.4th at 804.

17 Plaintiffs cannot avoid this result by insisting that the DISH/NagraStar Defendants were only assisting the Federal Defendants so that they could steal Plaintiffs' intellectual property. The relevant inquiry is whether the DISH/NagraStar Defendants had authorization to access the information, not whether they harbored ill motives. *See Van Buren v. United States*, 593 U.S. 374, 141 S. Ct. 1648, 1652, 210 L.Ed.2d 26 (2021) (holding that the CFAA "does not cover those who ... have improper motives for obtaining information that is otherwise available to them").

2024 WL 1363755
Only the Westlaw citation is currently available. United States District Court, D. Puerto Rico.
NAICOM CORPORATION, et al., Plaintiffs, v.
DISH NETWORK CORPORATION, et al., Defendants.

No. 3:21-cv-01405-JAW
|
Signed March 29, 2024

Attorneys and Law Firms

Rafael F. Castro-Lang, Castro & Castro Law Office, San Juan, PR, for Plaintiffs.

Chad M. Hagan, Pro Hac Vice, Timothy Frank, Pro Hac Vice, Hagan Noll & Boyle, LLC, Houston, TX, Jose L. Ramirez-Coll, Carolina V. Cabrera-Bou, Antonetti Montalvo & Ramirez-Coll, San Juan, PR, for Defendants Dish Network Corporation, DISH Network L.L.C., NagraStar LLC, Bert Eichhorn, Emily Rinkle, Jordan Smith, Kevin Gedeon, Michael Thomas Jaczewski.

Patrick B. Fenior, DOJ-Civ, Washington, DC, Priscila M. Acevedo-Roman, U.S. Attorney's Office for the District of Puerto Rico, San Juan, PR, for Defendants United States Attorney for the District of Puerto Rico, Rosa Emilia Rodriguez-Velez, Jose Capo, Nicholas W. Cannon, Federal Bureau of Investigations San Juan Field in Puerto Rico,

Douglas A. Leff, Bradely Rex, Lance Lange, Clay Rehrig, Juan Galarza, Jason Lopez, Kevin Pearson, United States Attorney's Office.
Jose L. Ramirez-Coll, Carolina V. Cabrera-Bou, Antonetti Montalvo & Ramirez-Coll, San Juan, PR, for Defendant Toltec Investigations, LLC.

ORDER ON DISH NETWORK CORPORATION'S MOTION TO DISMISS

JOHN A. WOODCOCK, JR., UNITED STATES DISTRICT JUDGE

***1** A corporation moves to dismiss plaintiffs' seven-count complaint alleging the corporation assisted in a conspiracy to steal plaintiffs' intellectual property under the guise of a legitimate law enforcement investigation. The Court grants the motion, dismissing all seven counts of the complaint. At the outset, the Court dismisses the Computer Fraud and Abuse Act claim, the Stored Communications Act claim, the Digital Millennium Copyright Act claim, and the Defend Trade Secrets Act claim because the corporation lacks sufficient minimum contacts with Puerto Rico. The Court dismisses the RICO claims because plaintiffs have not adequately pleaded the existence of an enterprise, a pattern of racketeering activity, or a conspiracy. Finally, having dismissed all claims over which it has original jurisdiction, the Court declines to exercise supplemental jurisdiction over the

Puerto Rico Uniform Trade Secrets Act claim and instead dismisses it.

I. PROCEDURAL HISTORY

On August 27, 2021, Naicom Corporation, D&V IP Holdings, LLC, Paylink, LLC, and Kiaras, LLC filed a seven-count complaint against approximately twenty known Defendants and two dozen unknown Defendants. [1] *Compl.* (ECF No. 1). The Court has twice permitted Plaintiffs to amend their complaint, and the Second Amended Complaint is now the operative complaint. *Am. Compl.* (ECF No. 100); *Second Am. Compl.* (ECF No. 130).

The parties categorize the numerous Defendants into four groups: 1) DISH Network LLC, NagraStar LLC, Bert Eichhorn, Emily Rinkel, [2] Jordan Smith, and Kevin Gedeon (the DISH/NagraStar Defendants); 2) DISH Network Corporation (DISH Corp. or DNC); 3) Toltec Investigations, LLC and its President and CEO, Michael Thomas Jaczewski (the Toltec Defendants); and 4) former U.S. Attorney Rosa E. Rodriguez-Velez, former Assistant U.S. Attorney Jose Capo-Iriarte, Assistant U.S. Attorney Nicholas W. Cannon (the USAO Defendants) and Special Agents and employees of the Federal Bureau of Investigation Douglas Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan

Galarza, and Jason Lopez (the FBI Defendants) (collectively, the Federal Defendants).

***2** Plaintiffs allege: 1) violations of the Racketeer Influenced and Corrupt Organizations Act (RICO); 2) a RICO conspiracy; 3) violations of the Computer Fraud and Abuse Act (CFAA); 4) violations of the Stored Communications Act (SCA); 5) violations of the Digital Millennium Copyright Act (DMCA); 6) violations of the Defend Trade Secrets Act (DTSA) by misappropriation of trade secrets; and 7) violations of the Puerto Rico Industrial and Trade Secrets Protection Act (PTSA) under the Uniform Trade Secrets Act (Law No. 80). *Second Am. Compl.* ¶¶ 124-202.

On October 31, 2022, and November 1, 2022, each of the four groups of Defendants filed a motion to dismiss the Second Amended Complaint. *Def. DISH Network Corp.'s Mot. to Dismiss* (ECF No. 136) (*Def.'s Mot.*); *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Mot. to Dismiss* (ECF No. 134); *Defs.' Toltec Investigations, L.L.C. and Mike Jaczewski's Mot. to Dismiss* (ECF No. 137); *Fed. Defs.' Mot. to Dismiss* (ECF No. 138).

On December 5, 2022, Plaintiffs responded to the DISH/NagraStar Defendants' motion to dismiss. *Mot. in Resp. to Dish/NagraStar Defs.' Mot. to Dismiss* (ECF No. 147) (*Pls.' Opp'n to DISH/NagraStar Mot.*). On January

18, 2023, Plaintiffs responded to the Federal Defendants' motion. *Mot. in Resp. to the Fed. Defs.' Mot. to Dismiss* (ECF No. 153). On February 21, 2023, the Toltec Defendants withdrew a section of their motion to dismiss, *Unopposed Notice of Partial Withdrawal of Toltec Investigations L.L.C. and Mike Jaczewski's 12(b)(2) Mot. to Dismiss* (ECF No. 163), and on February 27, 2023, Plaintiffs responded to the remainder of the Toltec Defendants' motion. *Mot. in Resp. to Toltec Investigations and Mike Jaczewski's Mot. to Dismiss* (ECF No. 167). On March 17, 2023, Plaintiffs responded to DISH Corp.'s motion. *Mot. in Resp. to Dish Network Corp.'s Mot. to Dismiss* (ECF No. 179) (*Pls.' Opp'n*).

Each group of Defendants filed a reply in support of its motion. *DISH Network Corp.'s Reply in Supp. of Its Mot. to Dismiss* (ECF No. 196) (*Def.'s Reply*); *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Reply* (ECF No. 164); *Fed. Defs.' Reply* (ECF No. 173); *Defs. Toltec Investigations L.L.C. and Michael Jaczewski's Reply in Supp. of Rule 12(b)(6) Mot. to Dismiss* (ECF No. 185).

Finally, Plaintiffs filed sur-replies opposing each motion. *Sur-Reply Mot. to Dish Network Corp.'s Reply Mot. to Pls.' Resp. to Mot. to Dismiss SAC* (ECF No. 199) (*Pls.' Sur-Reply*); *Sur-Reply to the Dish Network, LLC and NagraStar, LLC Reply Mot. to Pls.' Resp. to Defs.' Mot. to Dismiss SAC* (ECF No. 182); *Sur-Reply Mot. to Fed.*

Defs.' Reply Mot. to Pls.' Resp. to Fed. Defs.' Mot. to Dismiss, SAC (ECF No. 190); *Sur-Reply Mot. to the Toltec Investigations L.L.C. and Michael Jaczewski's Reply Mot. to Pls.' Resp. to Their Mot. to Dismiss SAC* (ECF No. 195).

II. FACTS [3]

A. The Parties

In 2015 and 2016, Darwin Quinones-Pimentel and Victor Vega-Encarnacion founded Naicom Corporation (Naicom) and D&V IP Holdings, LLC to offer Internet Protocol Television (IPTV) services. The companies are structured such that D&V holds the proprietary "intellectual technology" created by Mr. Quinones, and Naicom licenses the technology from D&V to distribute television programming. *Second Am. Compl.* ¶ 63. Kiaras, LLC (Kiaras) and Paylink, LLC (Paylink) are also joint ventures operated by Mr. Quinones and Mr. Vega. *Id.* ¶ 14. Kiaras is a human resources and time-and-attendance management company, and Paylink is a payroll processing company. *Id.* Both Kiaras and Paylink operate on the "PAYLINK AND KIARAS Cloud Network," another proprietary intellectual technology creation of Mr. Quinones. *Id.* ¶¶ 5-6. All four companies are corporations existing under the laws of the commonwealth of Puerto Rico with their places of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907. *Id.* ¶¶ 33-36.

***3** DISH Network Corporation (DISH Corp.) was organized in 1995 as a corporation under the laws of the State of Nevada, started offering the DISH® branded pay-tv service in March 1996, and is the nation's third largest pay-tv provider. *Id.* ¶ 37. DISH Network LLC (DISH LLC) was organized in 1987 as a Limited Liability Corporation under the laws of the state of Colorado. *Id.* ¶ 38.

NagraStar, LLC is a joint venture between DISH Corp. and Kudelski SA formed in 1998. *Id.* ¶ 39. NagraStar's focus is delivering and maintaining security solutions for satellite and Internet-based television systems and other connectivity initiatives in North America, and its mission also includes anti-piracy investigations and cooperation with law enforcement agencies. *Id.* Jordan Smith was at all relevant times a Manager of Field Security & Investigations and Senior Anti-Piracy Investigator for NagraStar. *Id.* ¶ 41. Bert Eichhorn and Emily Rinkel were Managers of Field Security & Investigations for NagraStar. *Id.* ¶¶ 42-43. Kevin Gedeon was a Manager of Fraud Investigations for NagraStar. *Id.* ¶ 44.

Toltec Investigations, LLC (Toltec) is a private investigative agency specializing in investigating the technology and distribution involved in IPTV systems, copyrights, patents, and "Trademark and Brand's Intellectual Property." *Id.* ¶ 40. Michael Thomas

Jaczewski, a.k.a. Brian Parsons, was at all relevant times President and Chief Executive Officer of Toltec. *Id.* ¶ 45.

Rosa Emilia Rodriguez-Velez was at all relevant times the United States Attorney for the District of Puerto Rico. *Id.* ¶ 46. Jose Capo-Iriarte was an Assistant U.S. Attorney (AUSA) and head of the office's Criminal Division. *Id.* ¶ 47. Nicholas Cannon was an AUSA and Deputy Chief of the Cybercrimes Division. *Id.* ¶ 48.

Douglas Leff was at all relevant times Special Agent in Charge of the FBI's San Juan Division. *Id.* ¶ 49. Also in that division, Brad Rex was a Supervisory Special Agent; Lance Lange, Kevin Pearson, and Clay Rehrig were Special Agents; Juan Galarza a Computer Science Officer; and Jason Lopez an Evidence Technician. *Id.* ¶¶ 50-55.

B. Naicom's Origins

Between 2002 and 2012, Mr. Quinones developed the intellectual technology, including the source code, underpinning the Paylink and Kiaras Cloud Workforce Management system and Naicom's IPTV services. *Id.* ¶ 5. The proprietary IPTV system was characterized as a Dynamic Internet Semantic Multicast Environment (DISME), which "enabled for the first time the broadcast of media via private networks and the internet, a new concept of IPTV service to distribute Live-Video

Television Content (media) to residences, business, and primes customers." *Id.* ¶¶ 8-11.

By 2016, Mr. Quinones had completed all DISME technology alpha and beta tests and, alongside Mr. Vega, founded Naicom. *Id.* ¶ 12. Naicom is a network and internet communication platform that delivers live television, video on-demand content, internet, and wireless network services to subscribers worldwide. *Id.* Naicom also provides instant access to television shows, movies, and music/videos on-demand, and live sports and music events through Naicom's set-top box using IPTV and TV Everywhere (TVE) on any mobile device. *Id.*

Mr. Quinones and Mr. Vega registered Naicom as a closed corporation with the State Department of Puerto Rico and complied with all requirements as a legitimate IPTV business. *Id.* ¶ 66. Naicom also requested to manufacture its own brand of set-top boxes for end users through Informir LLC and acquired the programing licenses to distribute on-demand content in the United States, Puerto Rico, and the U.S. Virgin Islands through worldwide television network companies. *Id.* ¶¶ 67-68. In 2017, Naicom became a member of the National Rural Telecommunications Cooperative (NRTC). *Id.* ¶ 68.

***4** On January 6, 2017, Naicom submitted a request to the Apple Corporation to have its TV App added to Apple's AppStore. *Id.* ¶ 69. Apple's legal department

requested that Naicom produce all licenses authorizing the distribution of programming to Naicom's subscribers via Naicom's TV App. *Id.* On February 16, 2017, Apple approved Naicom's App for inclusion in the Apple AppStore. *Id.* ¶ 70. In December 2017, Sam's Club approved Naicom to launch and distribute Naicom's IPTV set-top box in their retail stores. *Id.* ¶ 71.

C. Naicom's Information Security

Naicom went to great lengths to protect its intellectual technology. *Id.* ¶¶ 64-65. D&V IP Holdings and Naicom developed significant amounts of confidential and proprietary information, including non-public information relating to the DISME's source codes, patterns, formulas, algorithms, methods, and techniques; the technological vision for Naicom's IPTV content, distribution, marketing, servicing, research and development efforts and strategies; business and marketing performance strategies; financial data and business plans; technical data; customer development management programs; and subcontractor and vendor relationships (collectively, with the DISME, the Confidential Information or Naicom's Confidential Information). *Id.* ¶ 64.

To protect this information, Plaintiffs only installed on their servers, located at the Naicom Data Center Facility, what is known as a compiled executable. *Id.* ¶

65. The entire system was installed with an operating system that allowed the hard drive to be encrypted and, to access the servers, an authorized employee would need to enter the secure data facility and provide a username and password. *Id.* The server is not exposed to the internet and could only be accessed from inside the facility. *Id.* The Confidential Information was also downloaded onto a hard disk and kept in a safe box. *Id.*

Plaintiff companies took additional steps to safeguard their confidential information and proprietary data, including restricting employee access, requiring employees to execute non-disclosure agreements, imposing restrictions on remote access, and implementing encryption. *Id.* ¶¶ 72-76.

D. Negotiations with Claro Puerto Rico

In 2017, Naicom entered into negotiations with Claro Puerto Rico [4] (Claro) to distribute Naicom set-top boxes to Claro customers. *Id.* ¶ 77. Claro represented to Naicom that it had approximately 320,000 internet subscribers who received only five megabytes and thus could not subscribe to Claro's IPTV services, which required sixty megabytes to upload programming. *Id.* ¶ 78. During negotiations, Naicom and Claro entered into a mutual non-disclosure agreement prior to discussing and analyzing business information and the contents of the resellers' agreement. *Id.* ¶ 79. Claro's Product

Development Officer, Anibal Rios, projected that the Claro-Naicom business alliance would bring in over $10,000,000 in monthly gross revenue for the first year and over $13,000,000 for the second year only taking into account Claro's corporate and residential subscribers in Puerto Rico. *Id.* ¶ 80. Naicom projected that the Claro-Naicom alliance would add 100,000 new corporate subscribers, plus another 150,000 residential subscribers, bringing in projected monthly gross sales of $9,000,000 in the first year and $12,000,000 in the second year. *Id.* ¶ 81.

***5** Claro had an existing contract with DISH Network Satellite TV, whereby DISH Network provided TV programming to Claro's internet subscribers who could not subscribe to Claro's IPTV services. *Id.* ¶ 82. The Naicom deal represented a cancellation threat to DISH Network's contract with Claro. *Id.* Claro was also considering shutting down its IPTV business division due to loss of revenue. *Id.* During the negotiations for the Claro-Naicom deal, Carlos Garcia, Claro's IPTV business manager, became privy to information that the Claro-Naicom deal would leave him jobless if Claro opted to shut down its IPTV division. *Id.* ¶ 83. Mr. Garcia alerted DISH Network that the Claro-Naicom IPTV deal would lead to cancellation of the DISH contract with Claro, which Plaintiffs allege led to "great animosity" between DISH Network and Naicom. *Id.* ¶ 84. On August 14, 2018, after a year of meetings between Naicom and

Claro, Claro pulled out of negotiations without notice. *Id.* ¶ 85. Plaintiffs believe the DISH Network Defendants advised Claro to withdraw because the FBI was investigating Naicom and its founders. *Id.* ¶ 86.

E. The DISH Network Investigation

On August 7, 2017, the DISH/NagraStar Defendants and DISH Corp. instructed the Toltec Defendants to purchase two Naicom TV set-top box receivers so that the Defendants [5] could reverse engineer Plaintiffs' intellectual technology. *Id.* ¶ 87. The Defendants conducted "sniffing" to determine the direction of Naicom TV traffic and locate Naicom's facility. *Id.* The Defendants also used sniffing to attack and penetrate Naicom's servers and computers, monitoring content and capturing information on the network under the supervision of the Federal Defendants. *Id.* One of the two set-top box receivers was maintained by the DISH/NagraStar Defendants, the other by the Toltec Defendants. *Id.* ¶ 88. Both receivers were used for the attacks on Naicom's data center servers. *Id.*

Mr. Jaczewski purchased the two set-top boxes from Naicom under the false name of "Brian Parsons," and he provided false contact information. *Id.* ¶ 89. The Defendants' investigation revealed that the receiver provided access to approximately forty-three channels, including Disney, TBS, ESPN, CNN, HBO, Showtime,

and Cinemax. *Id.* ¶ 90. The Defendants downloaded the Naicom TV App through the Apple AppStore, which provided access to approximately forty-two channels, and tested Naicom TV several times to determine whether it was providing DISH programming. *Id.* In each case, the tests revealed no DISH content. *Id.*

The Defendants also contacted several media companies to inquire into whether Naicom had the appropriate licensing contracts to distribute programming. *Id.* ¶ 91. On each occasion, the investigators were informed that Naicom was authorized to distribute the network's content. *Id.* The investigators also discovered that Naicom's TV distribution technology was a threat to DISH Network and Sling TV, representing future competition for subscribers in Puerto Rico and the United States. *Id.* ¶ 92.

The DISH/NagraStar Defendants informed the other Defendants that they could not penetrate Naicom's Data Center computers and servers remotely, and thus direct, physical access would be required to extract Naicom's intellectual property. *Id.* ¶ 93. They knew that by entering the data center and shutting down the computers and servers, they would be able to bypass Naicom's security measures and access the internal hard drive. *Id.* ¶ 94.

According to Naicom, the Defendants knew that the

intellectual property was extremely valuable and worth obtaining by any means necessary to advance their own television programming distribution system, and the Defendants conspired to misappropriate the technology for economic advantage. *Id.* ¶ 95.

***6** The DISH/NagraStar Defendants thereafter filed a complaint with the Federal Defendants alleging that Naicom was running an IPTV pirate operation. *Id.* ¶ 98. Plaintiffs allege that the motive behind the complaint was to secure NagraStar and DISH Network's participation in a search of Naicom's Data Center and the seizure of Naicom's computers, servers, and other hardware containing Naicom's intellectual property and trade secrets, under the ruse of assisting the Federal Defendants in discovering incriminating evidence. *Id.* Acquiring this information has given the DISH/NagraStar Defendants a competitive advantage over Naicom. *Id.* ¶ 99.

F. Execution of the Search Warrants

1. The First Search of Naicom's Data Center

On August 27, 2019, the Federal Defendants applied for two search warrants: one for Naicom Corporation located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907, and the other for Naicom's Data Center located at Villa Fontana, 4SS N2

Via Josefina, Carolina, Puerto Rico. *Id.* ¶¶ 19, 33, 105. Plaintiffs allege that the search warrants were "issued under illegal and unlawful means" because the Federal Defendants provided affidavits they knew to contain false and perjured information. *Id.* ¶ 20.

On August 27, 2019, the Federal and DISH/NagraStar Defendants executed the warrants, with the DISH/NagraStar Defendants "acting as federal agents." *Id.* ¶ 21. They seized documents, hard drives, and thumb drives, and downloaded data from the computers and servers containing Plaintiffs' Confidential Information. *Id.* Plaintiffs allege that the Defendants knew from their investigation prior to the searches that Naicom was authorized to distribute its programming and was not pirating content. *Id.* ¶ 101. The Defendants also allegedly knew that the evidence collected in the Federal Defendants' investigative files "negated any criminal wrongdoing that Naicom's founders were committing the crimes charged in the search and seizure warrant affidavit and application." *Id.* ¶ 102.

At the conclusion of the August 27, 2019, search, the Federal Defendants "learned that Naicom TV counted with all the programming distribution contract and agreements" [6] and instructed Mr. Quinones and Mr. Vega to report to the FBI offices with their licensing contracts for an interview. *Id.* ¶ 103. This interview took place with the Federal Defendants sitting at one table

and the DISH/NagraStar Defendants sitting at another table, allegedly posing as federal agents. *Id.* ¶ 104. The Defendants questioned Mr. Quinones about how Naicom acquired the IPTV distribution contracts and the technology used to distribute the programing. *Id.* They also inspected Naicom's contracts with content providers, which contained trade/business secrets and confidential information regarding DISME technology. *Id.*

2. The Second Search of Naicom's Data Center

On August 29, 2019, U.S. Attorney Rodriguez-Velez and AUSAs Capo-Iriarte and Cannon instructed FBI Agents Lange and Pearson to return to Naicom's data center with DISH/NagraStar Defendants Smith, Gedeon, and Eichhorn. *Id.* ¶ 105. Naicom alleges that the USAO Defendants ordered this search despite knowing beforehand that Naicom was a legitimate business and there was no probable cause for continued investigation. *Id.* Without obtaining new warrants, Defendants again entered Naicom's data center facility, performed password resets, and installed "pen drives and other electronic instruments" to bypass security measures and download and seize Naicom's Confidential Information. *Id.* ¶¶ 22, 106. The agents used keys taken from Naicom's offices to enter Naicom's data center. *Id.* ¶ 105.

***7** During the search, Agent Pearson contacted Naicom employee Jaime Echevarria and ordered him to come to

the Data Center, as Agent Pearson wanted to speak with him, Mr. Quinones, and Mr. Vega. *Id.* ¶ 107. Upon arriving at the Data Center, Mr. Quinones observed Agents Lange and Pearson allowing Mr. Smith, Mr. Gedeon, and Mr. Eichhorn to access Naicom's Data Center computers, servers, and other hardware equipment without authorization from Naicom. *Id.* ¶ 108.

During the search, Agents Pearson and Lange pressured Mr. Quinones to sign a hold-harmless document accepting that he had run a pirate operation in the past so that they could close the case. *Id.* ¶ 109. Otherwise, they threatened that they would shut down the Data Center operation. *Id.* Mr. Quinones refused, despite Agents Pearson and Lange imploring him to sign the document. *Id.* ¶ 110.

Sometime thereafter, Mr. Vega arrived and, upon entering the Data Center, asked Agents Pearson and Lange if they had another search warrant to enter and search the Data Center. *Id.* ¶ 111. Agent Lange represented to Mr. Vega that the search warrant gave him ten days to come in and out and search the Data Center. *Id.* Mr. Vega told Agent Lange that Agent Lange was violating the United States Constitution and Federal law. *Id.*

Mr. Vega thereafter informed Agents Pearson and Lange that he had discovered via LinkedIn that the alleged FBI

experts who executed the search and interrogated Mr. Quinones and him at the FBI offices were Kevin Gedeon, investigator for DISH Network, and Jordan Smith, Bert Eichhorn, and Emily Rinkel, investigators for NagraStar. *Id.* ¶ 112. Mr. Vega questioned Agents Lange and Pearson as to why the FBI brought in his competition to search, inspect, and photograph private documents and allowed them access to computers and servers containing trade secrets, code sources, and business and intellectual property belonging to Naicom. *Id.* ¶ 113. Mr. Vega called his attorney and told him about the second search. *Id.* ¶ 114. After speaking with Agent Lange, the FBI agents and DISH/NagraStar investigators shut down Naicom's business operation and left the premises. *Id.*

G. The Demand for the Return of Property Under Rule 41(g)

On September 6, 2019, Plaintiffs filed a motion to demand the return of seized property under Rule 41(g) of the Federal Rules of Criminal Procedure. *Id.* ¶ 115. The District Court granted the Plaintiffs' Rule 41(g) motion on November 5, 2019, noting that the Government had waived objections to the court's Report & Recommendation. *Id.* ¶¶ 116-17.

H. Plaintiffs' Alleged Harm

Plaintiffs allege that the criminal investigation caused significant damage to their business reputation and unfairly enriched their competitors. *Id.* ¶¶ 118-19. They allege that prior to the execution of the search warrants, they had a great reputation and were about to close on a $15,000,000 investment deal, but investors pulled out upon learning Naicom was under criminal investigation. *Id.* ¶¶ 120-21. Plaintiffs also allege that Naicom was about to close a multimillion-dollar deal with Claro when Claro learned of the FBI's investigation and pulled out of negotiations. *Id.* ¶ 122. Plaintiffs say they have lost subscribers because of negative publicity resulting from the investigation and that the Defendants' intrusion into Naicom's Data Center computers, servers, and equipment caused damage leaving subscribers without TV programming services for several weeks and cost more than $500,000 to repair. *Id.* ¶ 123.

I. Plaintiffs' Causes of Action

***8** Plaintiffs bring seven counts. Count One alleges the Defendants violated RICO by forming an association in fact to advance the criminal objective of stealing Plaintiffs' intellectual property and trade secrets by committing mail and wire fraud, among other crimes. *Id.* ¶¶ 124-53. Count Two alleges the Defendants engaged in a RICO conspiracy by conspiring to plan and execute the scheme outlined in Count One. *Id.* ¶¶ 154-57. Count Three alleges the Defendants violated the CFAA by

accessing Naicom's computer systems without authorization, or in excess of authorization, and obtaining and using valuable information from those computers. *Id.* ¶¶ 158-68. Count Four alleges the Defendants violated the SCA by "willfully and intentionally access[ing] without authorization a facility which operates servers, encoders, computers, and telecommunications systems and technology, by electronically transmitting communications involved in Webservers, Email-Servers, Carrier Grade Routers which interconnected with local ISP providers through Border Gateway Protocols (BGP) in exchanging routing information between autonomous systems." *Id.* ¶¶ 169-75. Count Five alleges the Defendants violated the DMCA by illegally obtaining Plaintiffs' copyright-protected software programs, documents, confidential information, and research. *Id.* ¶¶ 176-84. Count Six alleges the Defendants violated the DTSA by stealing Plaintiffs' trade secrets, including DISME technology, intellectual property, and other confidential information. *Id.* ¶¶ 185-94. Finally, Count Seven alleges the Defendants misappropriated Plaintiffs' trade secrets in violation the PTSA. *Id.* ¶¶ 195-202.

III. THE PARTIES' POSITIONS

A. DISH Network Corporation's Motion to Dismiss

DISH Corp. first argues that "Plaintiffs' claims against DNC should be dismissed because the Court lacks personal jurisdiction over DNC as a matter of law." *Def.'s Mot.* at 4 (capitalization altered).

Regarding general personal jurisdiction, DISH Corp. maintains that "DNC's contacts with Puerto Rico are not continuous or systematic," *id.* at 6, because 1) "DNC is neither incorporated [in Puerto Rico] nor maintains its principal place of business there," 2) "DNC conducts no business at all in Puerto Rico, is not registered or qualified to conduct business in Puerto Rico and maintains no registered agent for service of process there," 3) DNC does not "own, manage, or lease any real or tangible property in Puerto Rico," and 4) DNC does not "maintain any retail stores, warehouses, offices, mailing addresses, bank accounts, telephone listings, agents, or employees in Puerto Rico." *Id.* Further, DISH Corp. insists that DISH LLC's "contacts with Puerto Rico cannot be attributed to DNC to confer general jurisdiction over DNC." *Id.* at 6-7. Therefore, DISH Corp. asserts that "DNC has none of the type of contacts with Puerto Rico that would warrant this Court's exercise of general personal jurisdiction over it." *Id.* at 7.

Turning to specific personal jurisdiction, DISH Corp. initially notes that "[t]he First Circuit has interpreted Puerto Rico's long-arm statute to extend personal jurisdiction 'as far as the Federal Constitution permits.'

" *Id.* at 5 (quoting *Pritzker v. Yari*, 42 F.3d 53, 60 (1st Cir. 1994)). Next, DISH Corp. avers that "Plaintiffs' claims do not relate to *any* contacts with DNC because DNC conducts no business in Puerto Rico." *Id.* at 8 (emphasis in original) (capitalization altered). In particular, DISH Corp. emphasizes that "DNC was neither a party to the searches and seizure that took place on August 27 and 29, 2019 that form the basis of Plaintiffs' claims, nor was it or any of its officers involved in any criminal investigation complained of by Plaintiffs." *Id.* at 9.

***9** DISH Corp. further submits that "Plaintiffs cannot rely upon the contacts of DNC's indirect subsidiary to establish DNC's purposeful availment of the forum because [DISH LLC's] forum-related contacts are not imputable to DNC by virtue of DNC's status as [DISH LLC's] indirect parent." *Id.* Likewise, DISH Corp. contends that Plaintiffs cannot "rely on DNC's stock ownership in [DISH LLC] to establish that DNC transacted business in the forum through [DISH LLC]." *Id.* at 10. In addition, DISH Corp. declares that "the lack of allegations or evidentiary proffers renders the exercise of specific jurisdiction over DNC in this case unreasonable, unfair, and contrary to traditional notions of fair play and substantial justice." *Id.*

Moving onto its second argument, DISH Corp. argues that "Plaintiffs cannot rely upon their spurious RICO claims to evade due process requirements and obtain

personal jurisdiction over DNC." *Id.* at 11 (capitalization altered). DISH Corp. insists that "[t]o the extent Plaintiffs seek to invoke [18 U.S.C.] § 1965 as a source of this Court's personal jurisdiction to permit a broader reach over their RICO claims against DNC, Plaintiffs still fail to establish that the Court's exercise of personal jurisdiction over DNC would be proper." *Id.*

Acknowledging that the First Circuit has not announced a definitive interpretation of 18 U.S.C. § 1965, DISH Corp. urges the Court to follow the approach of the Second, Seventh, Ninth, and Tenth Circuits. *Id.* at 11-12. Under this approach, DISH Corp. suggests the Court lacks personal jurisdiction because "the 'ends of justice' certainly do not justify it." *Id.* at 12 (quoting *World Depot Corp. v. Onofri*, No. 16-12439-FDS, 2017 U.S. Dist. LEXIS 198814 at *13, 2017 WL 6003052 (D. Mass. Dec. 4, 2017)). This is so, DISH Corp. continues, because "DNC is not a necessary party to a full adjudication of Plaintiffs' claims and Plaintiffs have failed to allege a colorable RICO claim against DNC premised on the factual allegations asserted in this case." *Id.*

DISH Corp. then discusses its perceived shortcomings of Plaintiffs' RICO claims. *Id.* at 12-22. First, it suggests that "Plaintiffs cannot plead a viable RICO enterprise on the facts." *Id.* at 13 (capitalization altered). DISH Corp. represents that "DNC has taken no part in the course of conduct of any enterprise alleged in this case, as it was

not a party to the searches and seizure conducted in August 2019 nor did it or any of its officers participate in any criminal investigation or activities for which Plaintiffs now complain." *Id.* at 15 (internal quotation omitted) (emphasis in original). Further, it submits that the conduct Plaintiffs "attribute to DNC was not in furtherance of some shared illicit purpose reminiscent of an enterprise, but rather due to lawfully authorized investigative activity designed to detect pirated IPTV content." *Id.*

Next, DISH Corp. asserts that "Plaintiffs cannot plead the conduct of a criminal enterprise that is separate and apart from the conduct of Defendants' own affairs." *Id.* at 16 (capitalization altered). In particular, DISH Corp. observes that "Plaintiffs fail to plead any factual allegations establishing how DNC took any part in the 'operation or management' of the alleged RICO enterprise." *Id.* at 17 (quoting *Reves v. Ernst & Young*, 507 U.S. 170, 185, 113 S.Ct. 1163, 122 L.Ed.2d 525 (1993)).

DISH Corp. also argues that "DNC committed no predicate offenses." *Id.* at 18. It avers that each of the predicate acts alleged by Plaintiffs " '[is] supported by allegations of legitimate government action' and 'even when viewed in the inflammatory light bestowed upon them by Plaintiff[s], in no way resemble criminal activity.' " *Id.* (alterations in *Def.'s Mot.*) (quoting *Kahre*

v. Damm, No. 2:07-CV-00231-DAE-RJJ, 2007 U.S. Dist. LEXIS 95978 at *26, 2007 WL 9728869 (D. Nev. Dec. 18, 2007)). Moreover, DISH Corp. reiterates that "DNC did not participate in the Federal Defendants' criminal investigation, execution of search warrants at Plaintiffs' business premises or the seizure of Plaintiffs' business effects." *Id.* at 20.

***10** In a similar vein, DISH Corp. maintains that it "lacked the criminal intent to engage in 'racketeering activity,' " *id.* (capitalization altered), because "all actions taken by DNC were performed under color of federal law, and at the direction and supervision of the Federal Defendants to assist them in discharging their governmental duties." *Id.*

Even if Plaintiffs could sufficiently allege one or more predicate acts, DISH Corp. continues, "Plaintiffs cannot plead an actionable pattern of racketeering activity on the facts." *Id.* at 21. According to DISH Corp., "[w]hen, as here, a complaint explicitly presents a distinct and non-reoccurring scheme with a built-in termination point and provides no indication that the perpetrators have engaged or will engage in similar misconduct, the complaint does not sufficiently allege continuity for § 1962(c) purposes even if the purported scheme takes several years to unfold, involves a variety of criminal acts, and targets more than one victim." *Id.* at 22 (quoting *Gamboa v. Velez*, 457 F.3d 703, 708-09 (7th Cir. 2006)).

Turning to Plaintiffs' RICO conspiracy claim, DISH Corp. argues that this claim "fails for two independent reasons." *Id.* First, it submits that Plaintiffs' RICO conspiracy claim should be dismissed because "Plaintiffs have failed to allege an actionable substantive RICO claim." *Id.* Further, it avers that "Plaintiffs' allegations of agreement and conspiracy are too vague and conclusory to state a claim for relief and consist ... of formulaic recitations and conclusory allegations." *Id.* at 23 (internal quotations omitted).

DISH Corp. concludes by asking the Court to dismiss Plaintiffs' claims with prejudice. *Id.* at 23-24.

B. Plaintiffs' Opposition

In response, Plaintiffs first argue that "the Court has personal jurisdiction over [ ] DNC as a matter of law." *Pls.' Opp'n* at 12 (capitalization altered). Plaintiffs submit that "whether the DNC defendants transacted business within the meaning of Puerto Rico's long-arm statute depends on whether Plaintiffs can establish that the DNC defendants have sufficient minimum contacts with Puerto Rico through NagraStar." [7] *Id.* at 16. Plaintiffs surmise that NagraStar has sufficient minimum contacts with Puerto Rico, and they claim that these contacts should be imputed to DISH Corp. because "the DNC defendants are equally liable for the actions of

their NagraStar partners under Colorado state law." *Id.* at 18-19. In Plaintiffs' view, this is so because DISH Corp. and NagraStar are parties to a joint venture, and "[u]nder Colorado law joint venturers are jointly and severally liable for the negligence of another joint venturer." *Id.* at 16-17.

Plaintiffs also maintain that the Court has personal jurisdiction over DISH Corp. for the RICO claims because "under [18 U.S.C. § 1965 and Federal Rule of Civil Procedure 4], personal jurisdiction over defendants can be obtained in RICO cases under circumstances where it otherwise might not exist." *Id.* at 21. Plaintiffs urge the Court to adopt the interpretation of 18 U.S.C. § 1965 articulated by the Fourth and Eleventh Circuits, which "have held that § 1965(d) is the controlling provision—that is, personal jurisdiction exists over all defendants if any one defendant has 'minimum contacts with the United States—the relevant sovereign.' " *Id.* at 22 (quoting *Republic of Panama v. BCCI Holdings (Lux.) S.A.*, 119 F.3d 935, 946 n.21 (11th Cir. 1997)).

***11** Shifting to the merits of their claims, Plaintiffs argue that "the procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Id.* at 25 (capitalization altered). They contend that all Defendants "jointly and collectively" procured search

warrants containing "material false representations and perjured testimony," which ultimately lacked probable cause. *Id.* Plaintiffs further submit that "the alleged initial probable cause dissipated with the first search warrant execution," and thus the second search was "illegal and warrantless." *Id.* at 30.

Plaintiffs go on to argue that "the affidavit in support of the search warrant was defective on its face." *Id.* at 31 (capitalization altered). They contend that their computer systems were protected under the SCA, that the "conclusory" statements in the affidavit were insufficient to justify a search, and that the search ultimately did not comply with the SCA. *Id.* at 31-33, 35. According to Plaintiffs, the Federal Defendants did not "seek authorization from the Magistrate to bring Plaintiffs' competitors, the Dish/NagraStar Defendants, to execute the search warrant, depriving the Magistrate of the opportunity to prohibit their participation in its execution." *Id.* at 35. Further, although Plaintiffs concede that 18 U.S.C. § 3105 allows private parties to assist in the execution of a search warrant, they counter that "the statute clearly prohibited the executing officer from bringing to the search a party which had another interest, profit, or other marketplace incentive." *Id.* at 35-36. Plaintiffs also submit that DISH Corp. cannot rely on the search warrants because the Federal Defendants conceded the invalidity of the warrants when they did not oppose Plaintiffs' motion for return of property under

Federal Rule of Criminal Procedure 41(g).
Id. at 38-40.

Shifting gears, Plaintiffs argue that "the *Noerr-Pennington* doctrine does not apply to the case at bar." *Id.* at 40 (capitalization altered). They also contend that sovereign immunity does not apply because "the charges in this civil action were not brought against the United States, but against specific federal official/agent[ ]/Dish/NagraStar and the DNC Defendants, in their individual and personal capacities, for criminal actions indictable under RICO, falling outside their scope of employment, and beyond their statutory authority." *Id.* at 40-41.

Turning to the elements of the RICO counts, Plaintiffs submit that they have "pleaded a colorable RICO claim on the facts," *id.* at 42 (capitalization altered), because they have pleaded "enough facts in the [Second Amended Complaint to give the] DNC defendants a fair notice of what there is, and the grounds upon [which] they rest." *Id.* at 42-43. Plaintiffs add that they have also "pleaded a cognizable RICO enterprise on the facts." *Id.* at 43-46 (capitalization altered).

Plaintiffs further maintain that they have sufficiently "pleaded conduct of a criminal enterprise that is separate and apart from the conduct of Defendants' own affairs." *Id.* at 46 (capitalization altered). In their view, the three

required elements for establishing a RICO enterprise are: 1) "an ongoing organization, formal or informal"; 2) that "the various associate[s] function as a continuing unit"; and 3) that the enterprise exists "separate and apart from the pattern of activity in which it engages." *Id.* at 46 (quoting *United States v. Turkette*, 452 U.S. 576, 583, 101 S.Ct. 2524, 69 L.Ed.2d 246 (1981)). Plaintiffs assert that while they "will ultimately need to establish each of these factors, at this early juncture it is sufficient to merely [ ] allege the existence of an association-in-fact enterprise." *Id.* at 46-47 (quoting *Pappa v. Unum Life Ins. Co. of Am.*, No. 3:07-cv-0708, 2008 U.S. Dist. LEXIS 21500 at *29-30, 2008 WL 744820 (M.D. Pa. Mar. 18, 2008)). They add that it is reasonable to infer from the complaint that "the Association in Fact defendants functioned as a continuing unit and had an ascertainable structure distinct from that inherent in the conduct of a pattern of racketeering activity." *Id.* at 48.

***12** Plaintiffs go on to argue that "the DNC defendants committed the predicate offense[s] and acted with criminal intent and in bad faith." *Id.* at 50 (capitalization altered). In Plaintiffs' view, "the DNC Defendants' conspiratorial agreement to violate mail and wire predicate acts are criminal and indictable." *Id.* at 51 (capitalization altered). Plaintiffs also maintain that, even if the alleged misrepresentations did not amount to mail or wire fraud, they nevertheless contributed to the Defendants' theft of trade secrets under 18 U.S.C. §§

1831 and 1832. *Id.* at 50-51.

Plaintiffs then maintain that they have "pleaded a pattern of racketeering activities on the facts," *id.* at 52 (capitalization altered), because have "pleaded that the Association in Fact defendants ... committed over 30 racketeering acts ranging from Mail and Wire fraud to theft of trade secrets, in a period of two years." *Id.* at 54. In Plaintiffs' view, these facts "satisfied the closed period of repeated conduct," and there are also "allegations of a threat of continued activity, in reference to the DNC, Dish Network and NagraStar corporation's joint venture." *Id.* at 54-55.

Finally, Plaintiffs submit that they have pleaded a viable RICO conspiracy claim because 18 U.S.C. § 1962(d) "criminalizes an agreement rather than any substantive criminal offense," meaning that "an agreement to associate with and participate in a yet-to-be-formed racketeering enterprise that would affect interstate commerce constitutes a completed offense under § 1962(d)." *Id.* at 57. Therefore, Plaintiffs conclude that a substantive RICO claim is not required for a viable RICO conspiracy claim, although they maintain that they have adequately alleged a substantive RICO claim." *Id.*

C. DISH Network Corporation's Reply

In its reply, DISH Corp. reiterates that "Plaintiffs' claims

against DNC should be dismissed because the Court lacks personal jurisdiction over DNC as a matter of law." *Def.'s Reply* at 2. DISH Corp. reads Plaintiffs' reply as conceding that "DNC is not subject to general jurisdiction in Puerto Rico [and] that [DISH LLC's] contacts with Puerto Rico cannot be attributed to DNC to confer personal jurisdiction over DNC." *Id.* at 3. DISH Corp. further points out that "Plaintiffs do not contest" that "neither DNC nor any of its officers were involved in the Federal Defendants' criminal investigation of Plaintiffs, execution of search warrants at Plaintiffs' business premises or the seizure of Plaintiffs' business effects." *Id.* at 4.

Turning to Plaintiffs' argument that "the exercise of specific jurisdiction over DNC is nevertheless proper under a 'joint enterprise' theory with NagraStar, premised on Colorado law," DISH Corp. argues that Plaintiffs' theory "lacks merit and impermissibly confuses the concepts of liability and personal jurisdiction." *Id.* at 4. DISH Corp. insists that "Plaintiffs fail to even allege facts concerning DNC's transaction of business in Puerto Rico either personally or through NagraStar as an agent." *Id.* at 5. In DISH Corp.'s view, "Plaintiffs' unsupported allegations that DNC may have engaged in a joint venture with NagraStar is insufficient to attribute NagraStar's contacts to DNC for jurisdictional purposes under either Puerto Rico's long-arm statute or in compliance with the Due Process Clause

of the Fifth Amendment." *Id.*

Addressing Plaintiffs' contention that 18 U.S.C. § 1965(d) creates personal jurisdiction for the RICO claims, DISH Corp. remarks that "Plaintiffs' position has been rejected by a majority of circuit courts that have considered the issue, including at least three district courts within this circuit." *Id.* at 6. DISH Corp. maintains that 18 U.S.C. § 1965(b) authorizes "nationwide service of process and govern[s] the exercise of personal jurisdiction over a civil RICO defendant." *Id.* ***13** Further, according to DISH Corp., 18 U.S.C. § 1965(b) "is inapplicable here," *id.* at 7 (capitalization altered), because "the ends of justice do not justify the conferral of personal jurisdiction over DNC, since DNC is not a necessary party to a full adjudication of Plaintiffs' claims in this case." *Id.* (internal quotation omitted). DISH Corp. also suggests that "if the Court dismisses Plaintiffs' RICO claims pursuant to the 12(b)(6) motions filed by the Federal Defendants, the DISH/NagraStar Defendants and the Toltec Defendants, it is unnecessary for the Court to reach DNC's jurisdictional challenge or the applicability of RICO's nationwide service of process provision." *Id.* at 7-8.

Next, DISH Corp. briefly addresses the issue of jurisdictional discovery, arguing that it should not be allowed in this case. *Id.* at 8-9. This is so, it continues, because "Plaintiffs make no effort to describe DNC's specific activities (as opposed to conduct attributed to the

myriad of other named Defendants) that caused their alleged injuries," "[n]or do they set forth any allegations of specific contacts among DNC, Plaintiffs, and Puerto Rico sufficient to demonstrate that personal jurisdiction is authorized and consistent with due process requirements." *Id.*

Finally, DISH Corp. suggests that "Plaintiffs' failure to address their remaining claims related to DNC renders their claims waived or abandoned." *Id.* at 9 (capitalization altered). DISH Corp. then reiterates that the Second Amended Complaint should be dismissed with prejudice. *Id.* at 10.

D. Plaintiffs' Sur-Reply

In their sur-reply, Plaintiffs suggest that the Court should "either reject and/or strike from the DNC defendants' Reply any portion not addressing a new matter." *Pls.' Sur-Reply* at 2. They submit that, with one exception, DISH Corp.'s reply "did not contribute anything new that had not already [been] discussed in their" motion to dismiss. *Id.* Plaintiffs also ask the Court to strike all defenses raised by DISH Corp. pursuant to Federal Rule of Civil Procedure 12(f). *Id.* at 9-10.

Turning to the substance of DISH Corp.'s arguments, Plaintiffs contend that selected passages from DISH Corp.'s annual report prove that "DNC is more than a

publicly traded holding company and does participate in their subsidiaries' business operations through its employees." *Id.* at 7. Plaintiffs maintain that "by hatching the conspiracy to unlawfully deprive Plaintiffs of their trade secrets and intellectual property through its subsidiary (NagraStar) ... DNC purposefully not only availed itself of the privilege of conducting business activities, but also protected its business in [Puerto Rico] through its partner in business NagraStar." *Id.* at 7 (internal citation omitted).

Finally, Plaintiffs argue that each of the Defendants "is sufficiently distinct from the RICO enterprise to satisfy the statute's distinctness requirement." *Id.* at 9.

IV. LEGAL STANDARDS

A. Motion to Dismiss for Lack of Personal Jurisdiction

DISH Corp. moves to dismiss Plaintiffs' Second Amended Complaint for lack of personal jurisdiction under Federal Rule of Civil Procedure 12(b)(2). "To hear a case, the court must have personal jurisdiction over the parties, 'that is the power to require the parties to obey its decrees.' " *Astro-Med, Inc. v. Nihon Kohden Am., Inc.*, 591 F.3d 1, 8 (1st Cir. 2009) (quoting *United States v. Swiss Am. Bank, Ltd.*, 191 F.3d 30, 35 (1st Cir. 1999)). "On a motion to dismiss for want of personal jurisdiction,

the plaintiff ultimately bears the burden of persuading the court that jurisdiction exists." *Id.* (citing *McNutt v. Gen. Motors Acceptance Corp.*, 298 U.S. 178, 189, 56 S.Ct. 780, 80 L.Ed. 1135 (1936); and *Mass Sch. of Law at Andover, Inc. v. Am. Bar Ass'n*, 142 F.3d 26, 34 (1st Cir. 1998)). "Faced with a motion to dismiss for lack of personal jurisdiction, a district court 'may choose from among several methods for determining whether the plaintiff has met [its] burden.' " *Id.* (alteration in original) (quoting *Adelson v. Hananel*, 510 F.3d 43, 48 (1st Cir. 2007)). "The different methods involve application by the district court of different legal standards." *Boit v. Gar-Tec Prods., Inc.*, 967 F.2d 671, 674 (1st Cir. 1992); *see also Foster-Miller, Inc. v. Babcock & Wilcox Can.*, 46 F.3d 138, 145-47 (1st Cir. 1995) (describing the prima facie, preponderance and likelihood standards). ***14** Here, the Court elects to use "the 'prima facie method' or the 'prima facie evidentiary standard,' rather than adjudicating the jurisdictional facts." *Astro-Med*, 591 F.3d at 8. Under the prima facie standard, "the inquiry is whether the plaintiff has proffered evidence which, if credited, is sufficient to support findings of all facts essential to personal jurisdiction." *Bluetarp Fin., Inc. v. Matrix Constr. Co.*, 709 F.3d 72, 79 (1st Cir. 2013) (quoting *Phillips v. Prairie Eye Ctr.*, 530 F.3d 22, 26 (1st Cir. 2008)). In conducting such an inquiry, the Court draws "the relevant facts from 'the pleadings and whatever supplemental filings (such as affidavits) are contained in the record, giving credence to

plaintiff's version of genuinely contested facts.' " *Ward v. AlphaCore Pharma, LLC*, 89 F.4th 203, 209 (1st Cir. 2023) (quoting *Baskin-Robbins Franchising LLC v. Alpenrose Dairy, Inc.*, 825 F.3d 28, 34 (1st Cir. 2016)). The Court may also consider "undisputed facts put forth by the defendant." *Baskin-Robbins*, 925 F.3d at 34. "Withal, the district court acts not as a factfinder, but as a data collector." *Foster-Miller*, 46 F.3d at 145.

Under the prima facie method, "the plaintiff cannot rely solely on conclusory averments but must 'adduce evidence of specific facts.' " *Chen v. U.S. Sports Acad., Inc.*, 956 F.3d 45, 54 (1st Cir. 2020) (quoting *Foster-Miller*, 46 F.3d at 145). Likewise, the Court does not "credit conclusory allegations or draw farfetched inferences." *Ward*, 89 F.4th at 209 (quoting *Ticketmaster-N.Y., Inc. v. Alioto*, 25 F.3d 201, 203 (1st Cir. 1994)). The "inquiry must be governed by 'evidence of specific facts set forth in the record' — not simply predicated upon a plaintiff's 'unsupported allegations in their pleadings.' " *Id.* (quoting *Boit*, 967 F.2d at 675). "Ordinarily, such evidence will be contained in affidavits, authenticated documents, and the like, submitted by one or more of the parties." *Id.*

B. Motion to Dismiss for Failure to State a Claim

Rule 12(b)(6) requires dismissal of a complaint that "fail[s] to state a claim upon which relief can be granted." FED. R. CIV. P. 12(b)(6). To state a claim, a complaint

must contain, among other things, "a short and plain statement of the claim showing that the pleader is entitled to relief." FED. R. CIV. P. 8(a)(2). In other words, a complaint must contain "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). A claim is facially plausible when "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly*, 550 U.S. at 556, 127 S.Ct. 1955). Plausible means " 'something more than merely possible' or 'merely consistent with a defendant's liability.' " *Germanowski v. Harris*, 854 F.3d 68, 71-72 (1st Cir. 2017) (internal citation omitted) (quoting *Schatz v. Republican State Leadership Comm.*, 669 F.3d 50, 55 (1st Cir. 2012); *Ocasio-Hernández v. Fortuño-Burset*, 640 F.3d 1, 11 (1st Cir. 2011)). This is a " 'context-specific' job that compels [judges] 'to draw on' [their] 'judicial experience and common sense.' " *Schatz*, 669 F.3d at 55 (quoting *Iqbal*, 556 U.S. at 679, 129 S.Ct. 1937).

This is a "two-step analysis." *Cardigan Mountain Sch. v. N.H. Ins. Co.*, 787 F.3d 82, 84 (1st Cir. 2015). "First, the court must distinguish 'the complaint's factual allegations (which must be accepted as true) from its conclusory legal allegations (which need not be credited).'

" *García-Catalán v. United States*, 734 F.3d 100, 103 (1st Cir. 2013) (quoting *Morales-Cruz v. Univ. of P.R.*, 676 F.3d 220, 224 (1st Cir. 2012)); *see also Schatz*, 669 F.3d at 55 (stating that a court may "isolate and ignore statements in the complaint that simply offer legal labels and conclusions or merely rehash cause-of-action elements"). "Second, the court must determine whether the factual allegations are sufficient to support 'the reasonable inference that the defendant is liable for the misconduct alleged.' " *García-Catalán*, 734 F.3d at 103 (quoting *Haley v. City of Boston*, 657 F.3d 39, 46 (1st Cir. 2011)).

V. DISCUSSION

A. Plaintiffs' Request to Strike the DISH Network Corporation's Reply

***15** Before turning to the merits of DISH Corp.'s motion to dismiss, the Court briefly addresses Plaintiffs' contention that the Court should "reject and/or strike" any portion of DISH Corp.'s reply "not addressing a new matter." *Pls.' Sur-Reply* at 2. Plaintiffs submit that, with one exception, DISH Corp.'s "factual argument and legal discussion[ ] did not contribute anything new that had not already [been] discussed in their [motion to dismiss], and their Reply is nothing more than a second response." *Id.*

The Court disagrees. Plaintiffs rely on District of Puerto Rico Local Civil Rule 7(c), which provides:

With prior leave of court and within seven (7) days of the service of any objection to a motion, the moving party may file a reply, which shall not exceed ten (10) pages in length, and which shall be strictly confined to responding to new matters raised in the objection or opposing memorandum.

As this rule makes clear, a reply is proper so long as it addresses "new matters raised in the ... opposing memorandum."

Plaintiffs reason that DISH Corp.'s reply is noncompliant because it contains the same general arguments as the motion to dismiss. For example, Plaintiffs claim that DISH Corp. is "re-submitting for a second time allegations regarding the Court's lack of Personal Jurisdiction over DNC as a matter of law." *Pls.' Sur-Reply* at 4.

But this reads Local Civil Rule 7(c) too narrowly and the DISH Corp.'s' reply too strictly. The Court does not view Local Civil Rule 7(c) as prohibiting a reply from expanding upon issues raised both in the original memorandum and the response so long as the response addressed the issues generated in the motion. *See Torres-Talavera v. Ford Motor Co.*, 965 F. Supp. 2d 220, 222 n.3

(D.P.R. 2013) (noting that, pursuant to Local Civil Rule 7(c), the plaintiffs' sur-reply was "confined to respond to the arguments made in defendant Ford's reply"). Local Civil Rule 7(c) is a rule of basic fairness, clearly prohibiting the use a reply to introduce new arguments not previously addressed by the respondent.

A closer examination of the reply reveals that DISH Corp. is responding to the arguments made in Plaintiffs' opposition brief. *See, e.g.*, *Def.'s Reply* at 4 (responding to Plaintiffs' argument "that the exercise of specific jurisdiction over DNC is nevertheless proper under a joint enterprise theory with NagraStar" (internal quotation omitted)). While DISH Corp.'s reply discusses the same subject matter as the motion to dismiss, the specific argumentation in the reply is different and responds to the arguments in Plaintiffs' opposition brief. Therefore, the reply is proper under Local Civil Rule 7(c). The Court denies Plaintiffs' request to strike. [8]

B. Personal Jurisdiction for Counts III Through VI

1. Analytical Framework

Plaintiffs assert that the Court has federal question jurisdiction over their federal statutory claims (Counts I through VI) and supplemental jurisdiction over their PTSA claim (Count VII). *Second Am. Compl.* ¶¶ 28-29.

"When a district court's subject matter jurisdiction is founded upon a federal question, the constitutional limits of the court's personal jurisdiction are fixed, in the first instance, not by the Fourteenth Amendment but by the Due Process Clause of the Fifth Amendment." *United Elec., Radio and Mach. Workers of Am. v. 163 Pleasant Street Corp.*, 960 F.2d 1080, 1085 (1st Cir. 1992). "In such circumstances, the Constitution requires only that the defendant have the requisite minimum contacts with the United States, rather than with the particular forum state (as would be required in a diversity case)." *Id.*; *S.E.C. v. Gastauer*, 93 F.4th 1, 8 (1st Cir. 2024).

***16** However, to exercise personal jurisdiction over any defendant, service of process must be "grounded within a federal statute or Civil Rule." *Id.*; *see also BNSF Ry. Co. v. Tyrrell*, 581 U.S. 402, 137 S. Ct. 1549, 1556, 198 L.Ed.2d 36 (2017) ("[A]bsent consent, a basis for service of a summons on the defendant is prerequisite to the exercise of personal jurisdiction"); *Omni Cap. Int'l, Ltd. v. Rudolf Wolff & Co., Ltd.*, 484 U.S. 97, 104, 108 S.Ct. 404, 98 L.Ed.2d 415 (1987) ("Before a federal court may exercise personal jurisdiction over a defendant, the procedural requirement of service of summons must be satisfied"). In other words, for the Court to have personal jurisdiction over DISH Corp., Plaintiffs "must show that (1) the exercise of personal jurisdiction comports with the Fifth Amendment Due Process Clause, and (2) [DISH Corp.] is subject to service of process under a federal

statute or rule." *Goya Foods Inc. v. Golla Oy*, 959 F. Supp. 2d 206, 212 (D.P.R. 2013).

Here, the parties clash over whether DISH Corp. can be properly served under a federal statute or rule. Federal Rule of Civil Procedure 4(k)(1) "limits the instances in which '[s]erving a summons or filing a waiver of service establishes personal jurisdiction over a defendant.' " *Waters v. Day & Zimmermann NPS, Inc.*, 23 F.4th 84, 93 (1st Cir. 2022) (emphasis omitted) (quoting FED. R. CIV. P. 4(k)(1)). Relevant here, service of process establishes personal jurisdiction when made upon a defendant "who is subject to the jurisdiction of a court of general jurisdiction in the state where the district court is located" or when "authorized by a federal statute." FED. R. CIV. P. 4(k)(1).

The Second Amended Complaint implicates both these methods of service. 18 U.S.C. § 1965, which is part of the RICO statute, "provides for nationwide service of process in civil cases under certain circumstances." *World Depot Corp.*, 2017 U.S. Dist. LEXIS 198814, at *12, 2017 WL 6003052. By contrast, the CFAA, SCA, DMCA, and DTSA do not authorize nationwide service of process. For those statutory claims, service of process is proper only if authorized by Puerto Rico's long-arm statute. *See Goya Foods*, 959 F. Supp. 2d at 212 ("No federal statute authorizing nationwide service of process applies here. Thus, jurisdiction over the defendants must be based on

Puerto Rico's long-arm statute"). Since the service-of-process framework differs for Plaintiffs' various federal statutory claims, the Court first addresses whether Plaintiffs have demonstrated that personal jurisdiction exists for Counts III through VI under Puerto Rico's long-arm statute.

The First Circuit has interpreted Puerto Rico's long-arm statute as "coextensive with the outer limits of the Constitution." *Rodríguez-Rivera v. Allscripts Healthcare Solutions, Inc.*, 43 F.4th 150, 160 (1st Cir. 2022). "Under the Due Process Clause, a nonresident defendant may be subjected to jurisdiction within a forum only if [it] has 'certain minimum contacts with it such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice.' " *Id.* (quoting *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316, 66 S.Ct. 154, 90 L.Ed. 95 (1945)). "As long as due process concerns are satisfied, a federal court 'may exercise either general or specific jurisdiction over a defendant.' " *Chen*, 956 F.3d at 55 (quoting *Baskin-Robbins*, 825 F.3d at 35).

As the Supreme Court has explained, "[a] court may assert general jurisdiction over foreign (sister-state or foreign country) corporations to hear any and all claims against them when their affiliations with the State are so continuous and systematic as to render them essentially at home in the forum State." *Daimler AG v. Bauman*, 571 U.S. 117, 127, 134 S.Ct. 746, 187 L.Ed.2d 624 (2014)

(alteration in original) (quoting *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915, 919, 131 S.Ct. 2846, 180 L.Ed.2d 796 (2011)). "The paradigmatic examples of locales in which a defendant corporation is considered at home are its state of incorporation and the state that houses its principal place of business." *Chen*, 956 F.3d at 57 (citing *BNSF Ry. Co.*, 137 S. Ct. at 1558). "In 'exceptional case[s],' though, a defendant corporation's general business operations in a state in which it is neither incorporated nor headquartered 'may be so substantial and of such a nature as to render the corporation at home in that state.' " *Id.* (alteration in original) (quoting *Daimler*, 571 U.S. at 139, 134 S.Ct. 746).

***17** Specific jurisdiction is the other variety of personal jurisdiction. It is transaction specific. *See Daimler*, 571 U.S. at 127, 134 S.Ct. 746 (noting that courts exercise specific jurisdiction when the suit "aris[es] out of or relate[s] to the defendant's contacts with the forum") (alterations in original) (quoting *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408, 414 n.8, 104 S.Ct. 1868, 80 L.Ed.2d 404 (1984)). "A litigant seeking to establish that a court has specific jurisdiction over a defendant must satisfy three criteria." *Ward*, 89 F.4th at 209. "First, the plaintiff's claim must directly arise from or relate to the defendant's activities in the forum." *Id.* at 209-10 (quoting *Chen*, 956 F.3d at 59). "Second the defendant's forum-state contacts must represent a

purposeful availment of the privilege of conducting activities in that state." *Id.* at 210 (quoting *Chen*, 956 F.3d at 59). "Third, 'the exercise of specific jurisdiction in the forum must be reasonable under the circumstances.' " *Id.* (quoting *Chen*, 956 F.3d at 59).

2. Application

As noted above, for Plaintiffs to meet their burden of establishing personal jurisdiction, they must "adduce evidence of specific facts," *Chen*, 956 F.3d at 54 (quoting *Foster-Miller*, 46 F.3d at 145), and they "may not 'rely on unsupported allegations.' " *Scottsdale Cap. Advisors Corp. v. The Deal, LLC*, 887 F.3d 17, 20 (1st Cir. 2018) (quoting *A Corp. v. All Am. Plumbing, Inc.*, 812 F.3d 54, 58 (1st Cir. 2016)). Plaintiffs apparently seek to establish personal jurisdiction over DISH Corp. based on the Second Amended Complaint and one attachment to their sur-reply. As far as the Court can tell, Plaintiffs have not proffered any other facts, as they attached no additional evidence to their other filings, including previous versions of the complaint. The Court concludes that Plaintiffs have failed to offer any specific facts suggesting a nexus between DISH Corp. and Puerto Rico and, as a result, Plaintiffs have failed to demonstrate that the Court has either general or specific jurisdiction over DISH Corp.

With respect to the allegations in the Second Amended

Complaint, the First Circuit has repeatedly cautioned that plaintiffs seeking to establish personal jurisdiction cannot rest on "unsupported allegations in their pleadings." *Ward*, 89 F.4th at 209 (quoting *Boit*, 967 F.2d at 675). Further, the jurisdictional allegations related to DISH Corp. in the Second Amended Complaint are wholly conclusory. Apart from their general allegation that DISH Corp. participated in an elaborate conspiracy to steal their intellectual property from Puerto Rico, [9] Plaintiffs merely allege that DISH Corp. "does business, as Dish Network, PR, in San Juan, Puerto Rico." *Second Am. Compl.* ¶ 32. But this is neither a "specific fact[ ]," nor is it supported by any evidence. *See Boit*, 967 F.2d at 675. Plaintiffs do not say whether DISH Corp. has employees in Puerto Rico, whether it owns property in Puerto Rico, or anything else about the nature of DISH Corp's alleged business activities in Puerto Rico. [10] Without more, the Court does not "credit [Plaintiff's] conclusory allegations." *Ward*, 89 F.4th at 209 (quoting *Ticketmaster-N.Y.*, 25 F.3d at 203).

***18** The attachment to Plaintiffs' sur-reply is no more enlightening. This attachment consists of selected pages from DISH Network's 2022 Annual Report and DISH Corp.'s 2022 SEC Form 10-K, which primarily detail DISH Corp.'s officers and relationships with other companies in which it holds an ownership stake. *See Pls.' Sur-Reply*, Attach. 1, *DISH Corp. Form 10-K*. But this

attachment nowhere mentions Puerto Rico, nor does it provide any insight into DISH Corp.'s contacts with Puerto Rico. As such, it does not shed any light into whether the Court has personal jurisdiction over DISH Corp. pursuant to Puerto Rico's long-arm statute.

All told, Plaintiffs have not proffered any nonconclusory evidence connecting DISH Corp. to Puerto Rico. Therefore, the Court concludes that Plaintiffs failed to meet their burden of establishing personal jurisdiction over DISH Corp. pursuant to Puerto Rico's long-arm statute. *See United States v. Swiss Am. Bank, Ltd.*, 274 F.3d 610, 621 (1st Cir. 2001) (noting that "there can be no requisite nexus between the contacts and the cause of action if no contacts exist").

Plaintiffs attempt to overcome this lack of facts by asserting that NagraStar's contacts should be imputed to DISH Corp. for purposes of personal jurisdiction. *See Pls.' Opp'n* at 16 ("[T]he question [of] whether the DNC defendants transacted business within the meaning of Puerto Rico's long-arm statute depends on whether Plaintiffs can establish that the DNC defendants have sufficient minimum contacts with Puerto Rico through Nagrastar"). The First Circuit has cautioned that "generally, the jurisdictional contacts of a subsidiary corporation are not imputed to its parent." *Rodríguez-Rivera*, 43 F.4th at 161. "The mere fact that a subsidiary company does business within a state does not confer

jurisdiction over its nonresident parent, even if the parent is the sole owner of the subsidiary." *Id.* (quoting *Escude Cruz v. Ortho Pharm. Corp.*, 619 F.2d 902, 905 (1st Cir. 1980)). "To establish jurisdiction over a parent company, under Puerto Rico law, a plaintiff 'must produce strong and robust evidence of control by the parent company over the subsidiary, rendering the latter a mere shell.' " *Id.* (quoting *De Castro v. Sanifill, Inc.*, 198 F.3d 282, 283-84 (1st Cir. 1999)).

In their briefing, Plaintiffs adduce evidence that DISH Corp. owns a 50% stake in NagraStar, and that NagraStar supplies DISH Corp. with "encryption and related security systems." *Pls.' Sur-Reply*, Attach. 1, *DISH Corp. Form 10-K* at 8. The Second Amended Complaint also alleges that NagraStar "is located onsite with Dish in Colorado." *Second Am. Compl.* ¶ 39. But contracting for services and sharing office space falls short of "strong and robust evidence of control" that would "render[NagraStar] a mere shell." *Rodríguez-Rivera*, 43 F.4th at 161 (quoting *De Castro*, 198 F.3d at 283-84). Accepting Plaintiffs' proffers as true, they simply establish that DISH Corp. and NagraStar maintain an ongoing business relationship. Accordingly, Plaintiffs have failed to overcome the "presumption of corporate separateness." *Negron-Torres v. Verizon Commc'ns, Inc.*, 478 F.3d 19, 27 (1st Cir. 2007) (quoting *Escude Cruz*, 619 F.2d at 905). Therefore, NagraStar's contacts with Puerto Rico cannot be imputed to DISH

Corp. for purposes of the jurisdictional analysis.

Plaintiffs further attempt to use NagraStar to create personal jurisdiction over DISH Corp. by arguing that because "joint venturers are jointly and severally liable for the negligence of another joint venturer" under Colorado law, DISH Corp. is "equally liable for the actions of [its] Nagrastar partners." *Pls.' Opp'n* at 16-19. This argument confuses liability with personal jurisdiction. Plaintiffs' argument explicitly relies on Colorado state law. But in federal court, both the "source" and the "outer limits" of personal jurisdiction "are defined exclusively by the Constitution." *Foster-Miller*, 46 F.3d at 143-44 (citing *Ins. Corp. of Ir. v. Compagnie des Bauxites de Guinee*, 456 U.S. 694, 702, 102 S.Ct. 2099, 72 L.Ed.2d 492 (1982)). Plaintiffs cannot use state law to overcome constitutional requirements. [11] *See Thomas v. Lazard Freres & Co.*, No. 3-01-CV-2160-R, 2002 U.S. Dist. LEXIS 9212 at *11 (N.D. Tex. May 21, 2002) (rejecting argument "that the exercise of specific jurisdiction is nevertheless proper under a joint enterprise theory" because "[t]his argument impermissibly confuses the concepts of liability and personal jurisdiction" (internal quotations omitted)).

***19** In summary, the Court determines that Plaintiffs have not put forward any facts establishing either general or specific personal jurisdiction over DISH Corp. Therefore, Plaintiffs have not met their burden of

demonstrating personal jurisdiction for Counts III through VI under Puerto Rico's long-arm statute. Accordingly, the Court grants DISH Corp.'s motion as to Counts III through VI of the Second Amended Complaint. [12]

C. Plaintiffs' RICO Claims

1. Personal Jurisdiction under RICO

Unlike Plaintiffs' other federal statutory claims, "there is general and widespread agreement that under at least some circumstances, the RICO statute permits courts to exercise personal jurisdiction over defendants lacking traditional minimum contacts with the forum." *Dispensa v. Nat'l Conf. of Catholic Bishops*, No. 19-cv-556-LM, 2020 U.S. Dist. LEXIS 89570 *22, 2020 WL 2573013 (D.N.H. May 21, 2020). This power comes from 18 U.S.C. § 1965, which provides:

> (a) Any civil action or proceeding under this chapter against any person may be instituted in the district court of the United States for any district in which such person resides, is found, has an agent, or transacts his affairs.
>
> (b) In any action under section 1964 of this chapter in any district court of the

United States in which it is shown that the ends of justice require that other parties residing in any other district be brought before the court, the court may cause such parties to be summoned, and process for that purpose may be served in any judicial district of the United States by the marshal thereof.

(c) In any civil or criminal action or proceeding instituted by the United States under this chapter in the district court of the United States for any judicial district, [subpoenas] issued by such court to compel the attendance of witnesses may be served in any other judicial district, except that in any civil action or proceeding no such [subpoena] shall be issued for service upon any individual who resides in another district at a place more than one hundred miles from the place at which such court is held without approval given by a judge of such court upon a showing of good cause.

(d) All other process in any action or proceeding under this chapter may be served on any person in any judicial district in which such person resides, is found, has an agent, or transacts his affairs.

Courts disagree on which subsection of 18 U.S.C. § 1965 authorizes nationwide service of process and therefore allows the exercise of personal jurisdiction over defendants lacking sufficient minimum contacts to the forum. The majority of circuits to consider the question have concluded that § 1965(b) is the controlling provision. These courts hold that "a federal court may exercise personal jurisdiction over a civil RICO defendant otherwise lacking traditional minimum contacts with the forum state," if 1) "personal jurisdiction over another civil RICO defendant otherwise exists in the forum," and 2) " 'the ends of justice require' that the court exercise personal jurisdiction over the civil RICO codefendant lacking the requisite contacts." *Dispensa*, 2020 U.S. Dist. LEXIS 89570, at *23, 2020 WL 2573013; *see also Butcher's Union Local No. 498 v. SDC Inv., Inc.*, 788 F.2d 535, 538-39 (9th Cir. 1986); *Lisak v. Mercantile Bancorp, Inc.*, 834 F.2d 668, 671-72 (7th Cir. 1987); *PT United Can Co. Ltd. v. Crown Cork & Seal Co., Inc.*, 138 F.3d 65, 70-72 (2d Cir. 1998); *Cory v. Aztec Steel Bldg., Inc.*, 468 F.3d 1226, 1229-33
(10th Cir. 2006).

***20** However, courts adhering to the majority approach are split on how to determine whether the "the ends of justice require" the exercise of personal jurisdiction over a defendant lacking sufficient minimum contacts. *Compare Butcher's Union*, 788 F.2d at 539 (requiring plaintiffs to "show that there is no other district in which

a court will have personal jurisdiction over all of the alleged co-conspirators"), *with Cory*, 468 F.3d at 1232 (concluding that "the 'ends of justice' analysis is not controlled by the fact that all defendants may be amenable to suit in one forum" and instead observing that "the 'ends of justice' is a flexible concept uniquely tailored to the facts of each case").

In contrast to the majority approach, two circuits—the Fourth Circuit and the Eleventh Circuit—have concluded that § 1965(d) is the controlling provision. *See Republic of Panama v. BCCI Holdings (Lux.) S.A.*, 119 F.3d 935, 942 (11th Cir. 1997); *ESAB Grp., Inc. v. Centricut, Inc.*, 126 F.3d 617, 626 (4th Cir. 1997). These circuits do not inquire into whether "the ends of justice require" the exercise of personal jurisdiction over defendants lacking sufficient minimum contacts. *See Republic of Panama*, 119 F.3d at 942; *ESAB Grp.*, 126 F.3d at 626.

The First Circuit has not decided whether § 1965(b) or § 1965(d) controls. At least three district courts in the First Circuit have sided with the majority. *See World Depot Corp.*, 2017 U.S. Dist. LEXIS 198814, at *14, 2017 WL 6003052; *Kalika, LLC v. Bos. & Me. Corp.*, No. 15-14043-GAO, 2018 U.S. Dist. LEXIS 45612 at *21, 2019 WL 1276099 (D. Mass. Feb. 28, 2018); *Dispensa*, 2020 U.S. Dist. LEXIS 89570, at *25, 2020 WL 2573013. On the other hand, at least one district court in the First Circuit

has adopted the approach of the Fourth and Eleventh Circuits. *See Bridge v. Invest Am., Inc.*, 748 F. Supp. 948, 950-51 (D.R.I. 1990). DISH Corp. urges the Court to adopt the majority approach, *Def.'s Reply* at 5-8, while Plaintiffs suggest the Court should follow the Fourth and Eleventh Circuits. *Pls.' Opp'n* at 22-23.

Ultimately, the Court determines that it need not decide whether § 1965(b) or § 1965(d) is controlling. Although "courts should ordinarily satisfy jurisdictional concerns before addressing the merits of a civil action," the First Circuit has advised that this "rule is not mechanically to be applied." *Feinstein v. Resol. Trust Corp.*, 942 F.2d 34, 40-41 (1st Cir. 1991), *abrogated on other grounds by Salinas v. United States*, 522 U.S. 52, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997). "Where, as here, the affected defendant does not insist that the jurisdictional issue be determined first, and no special circumstances exist," district courts may "eschew[ ] difficult jurisdiction and venue-related issues in favor of ordering dismissal on the merits." [13] *Id.*

Having thoroughly analyzed Plaintiffs' RICO claims in the context of the motions to dismiss filed by the Federal Defendants, the DISH/NagraStar Defendants, and the Toltec Defendants, the Court concludes that it is better to assess those claims on the merits than to break new ground on an unsettled jurisdictional issue. Accordingly, the Court bypasses DISH Corp.'s personal-jurisdiction

challenge as to Plaintiffs' RICO claims. *See Ogilvie v. Beale*, No. 93 C 2934, 1994 U.S. Dist. LEXIS 1123 at *1, *7, *15-24, 1994 WL 33972 (N.D. Ill. Feb. 3, 1994) (bypassing personal jurisdiction to dismiss civil RICO claim pursuant to Rule 12(b)(6)); *cf. World Depot Corp.*, 2017 U.S. Dist. LEXIS 198814, at *15, 2017 WL 6003052 (formally dismissing civil RICO claim for lack of personal jurisdiction but also "noting that the complaint appears to fail to state a claim under the RICO statute"). The Court opts to dismiss Plaintiffs' RICO claims on the merits, for the reasons explained below.

2. The Merits of Plaintiffs' RICO and RICO Conspiracy Claims

***21** Plaintiffs' RICO claim falls short because their allegations rely too heavily on conclusory statements, and the conduct they allege does not establish a colorable RICO claim. First, the allegations in the Second Amended Complaint are too threadbare to sufficiently plead DISH Corp.'s participation in a RICO enterprise. Second, even if the Court were to credit Plaintiffs' conclusory allegations, they nonetheless have failed to adequately plead predicate acts constituting a pattern of racketeering activity.

To state a civil RICO claim under 18 U.S.C. § 1962(c), a plaintiff must allege four elements: (1) conduct; (2) of an enterprise; (3) through a pattern; (4) of racketeering

activity. *Lerner v. Colman*, 26 F.4th 71, 77 (1st Cir. 2022) (citing *Sedima, S.P.R.L. v. Imrex Co.*, 472 U.S. 479, 496, 105 S.Ct. 2787, 86 L.Ed.2d 384 (1985)). "Racketeering activity" is defined to include a variety of predicate offenses, including mail fraud, wire fraud, and theft of trade secrets. 18 U.S.C. § 1961(1). The civil-suit provision of the RICO statute grants the right to sue to "[a]ny person injured in his business or property by reason of a violation of" the substantive provisions of the statute. *Id.* § 1964(c).

Civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron v. Embassy Suites (P.R.), Inc.*, 223 F.3d 12, 20 (1st Cir. 2000). "[I]n cases alleging civil RICO violations, particular care is required to balance the liberality of the Civil Rules with the necessity of preventing abusive or vexatious treatment of defendants." *Miranda v. Ponce Fed. Bank*, 948 F.2d 41, 44 (1st Cir. 1991), *abrogated on other grounds by Salinas v. United States*, 522 U.S. 52, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997). "Civil RICO is an unusually potent weapon—the litigation equivalent of a thermonuclear device. The very pendency of a RICO suit can be stigmatizing and its consummation can be costly." *Id.* Accordingly, "courts should strive to flush out frivolous RICO allegations at an early stage." *Figueroa Ruiz v. Alegria*, 896 F.2d 645, 650 (1st Cir. 1990).

a. RICO Enterprise

In interpreting the RICO "enterprise" requirement, the Supreme Court has explained that "there is no restriction upon the associations embraced by the definition: an enterprise includes any union or group of individuals associated in fact." *Turkette*, 452 U.S. at 580, 101 S.Ct. 2524. The enterprise concept is not unbounded, however, because an enterprise must be "an entity, for present purposes a group of persons associated together for a common purpose of engaging in a course of conduct." *Id.* at 583, 101 S.Ct. 2524. In cases "involving an alleged associated-in-fact RICO enterprise, the existence of the charged enterprise does not follow, ipso facto, from evidence that those named as the enterprise's associates engaged in crimes that collectively may be characterized as a pattern of racketeering activity." *United States v. Cianci*, 378 F.3d 71, 81 (1st Cir. 2004) (internal quotation omitted).

Put differently, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of 'racketeering activity' do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.* at 82. Ultimately, the First

Circuit has "read *Turkette* to impose a requirement that those associated in fact function as an ongoing unit and constitute an ongoing organization. Also important to such an enterprise is that its members share a common purpose." *Id.* at 82 (internal quotations omitted). Finally, the existence of an enterprise "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Turkette*, 452 U.S. at 583, 101 S.Ct. 2524.

***22** "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice," *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937, especially where "plaintiffs attempt to camouflage conclusory statements as allegations of fact." *A.G. ex rel. Maddox v. Elsevier, Inc.*, 732 F.3d 77, 81 (1st Cir. 2013). After sifting out Plaintiffs' conclusory statements, the RICO enterprise allegations as pleaded are wafer thin, and the well-pleaded facts remaining are insufficient to establish that the alleged association in fact "function[ed] as an ongoing unit" or constituted an "ongoing organization." *Cianci*, 378 F.3d at 82 (internal quotations omitted).

As to the enterprise requirement, the Second Amended Complaint merely offers that, starting in 2017, all Defendants conspired at the outset and together "formed an Association in Fact, [including] Legal Entity Enterprises that would help the Association in Fact

defendants advance the purpose and goals of the Racketeering Enterprises' conspiratorial objectives in misappropriating themselves from Plaintiff's DISME intellectual technology property, and trade secrets." *Second. Am. Compl.* ¶¶ 17-18; *see also id.* ¶¶ 126-28. The Second Amended Complaint later clarifies that DISH Corp., along with DISH LLC and NagraStar, "are the Racketeering Enterprises." *Id.* ¶¶ 58, 125. Further, it avers that the "Association-In-Fact defendants knowingly agreed, combined, and conspired to conduct the affairs of the Racketeering Enterprise in attempting and committing theft of trade secrets through a hoax criminal investigation operation." *Id.* ¶ 155.

With respect to the participation of DISH Corp., the Second Amended Complaint asserts that the "Racketeering Enterprise ... authorized the Dish/NagraStar defendants to form the Association in Fact, and use the Legal Entity Enterprises to advance its conspiratorial objective." *Id.* ¶ 95. It also alleges that "[o]n August 7, 2017, the Racketeering Enterprise contracted the Toltec defendants to purchase two (2) Naicom TV Set Top Box receivers so that the Association in Fact defendants could conduct reverse engineering on Plaintiffs' Intellectual Technology." *Id.* ¶ 87. However, besides alleging that Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel "supervised and approved" Mr. Jaczewski's payments to Naicom, the Second Amended Complaint fails to shed any additional light on the alleged

RICO enterprise. *Id.* ¶ 135.

Collectively, these allegations are almost entirely vague, conclusory, and devoid of factual development. At best, they describe the inner workings of the alleged RICO enterprise in a few isolated instances. But they fail to adequately describe how, apart from these isolated instances, the alleged RICO enterprise "function[ed] as an ongoing unit" or constituted an "ongoing organization" during the two-plus years it allegedly existed. *Cianci*, 378 F.3d at 82 (internal quotations omitted). In other words, Plaintiffs offer virtually no well-pleaded facts explaining how the Defendants functioned together as an ongoing unit or organization.

Plaintiffs attempt to compensate for this lack of well-pleaded facts by offering that "[t]he Association-In-Fact defendants had an ongoing organizational framework for carrying out the Racketeering Enterprises' criminal objectives" because "[t]he Association-In-Fact defendants could not have carried out the intricate task of robbing Plaintiffs' Intellectual Property and Trade Secrets ... unless it had some structure for making and communicating group decisions." *Second Am. Compl.* ¶ 130. The Court views this allegation as the epitome of a "[t]hreadbare recital[ ] of the elements of a cause of action, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937. The allegation merely restates the requirement that the enterprise have an organizational

framework, supported by nothing but the circular logic that the purported enterprise could not have succeeded unless it were truly an enterprise. The Court concludes that Plaintiffs' allegations do not adequately plead the existence of an "ongoing unit" or "ongoing organization" required for a RICO claim. *Cianci*, 378 F.3d at 82 (internal quotations omitted).

***23** Furthermore, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of 'racketeering activity' do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.*; *see also Bachman v. Bear Stearns & Co., Inc.*, 178 F.3d 930, 932 (7th Cir. 1999) (noting that a contrary rule would erroneously make "every conspiracy to commit fraud ... a RICO [enterprise] and consequently every fraud that requires more than one person to commit ... a RICO violation"). While Plaintiffs assert that DISH Corp. has previously been involved in trade secret misconduct, [14] they do not allege that this alleged association in fact as a whole has engaged or will engage in any misconduct unrelated to the one-off goal of stealing Plaintiffs' intellectual property. In its review of the Second Amended Complaint, the Court is unable to find the "[s]omething more" that "must be found ... that distinguishes RICO enterprises from ad hoc one-time

criminal ventures." *Cianci*, 378 F.3d at 82.

As noted earlier, Civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron*, 223 F.3d at 20. Ultimately, stripped of its conclusory allegations, the Second Amended Complaint does not assert sufficient facts to plead the existence of a RICO enterprise, and Plaintiffs' RICO claim must fail.

b. Pattern of Racketeering Activity: Mail and Wire Fraud

Plaintiffs must also plead a "pattern of racketeering activity," which "means the commission of at least two related acts of racketeering activity during a period of ten years." *Humana, Inc. v. Biogen, Inc.*, 666 F. Supp. 3d 135, 147 n.4 (D. Mass. 2023) (citing 18 U.S.C. § 1961(5)). "Racketeering activity" is defined to include a variety of predicate offenses, including mail fraud, wire fraud, and theft of trade secrets. 18 U.S.C. § 1961(1). The First Circuit has observed that the Supreme Court has found "that the civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements." *In re Neurontin Mktg. & Sales Pracs. Litig.*, 712 F.3d 21, 34 (1st Cir. 2013) (citing *Holmes v. Secs. Investor Prot. Corp.*, 503 U.S. 258, 268, 112 S.Ct.

1311, 117 L.Ed.2d 532 (1992)).

Plaintiffs allege that the purported RICO conspiracy's pattern of racketeering activity involved numerous criminal acts, including:

[A]cts indictable under Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy to Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.), while in addition, committing the possible underlying criminal offenses as prohibited under [the Computer] Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.), 18 U.S.C.A. § 2235-Search warrant procured maliciously; 18 U.S.C.A. § 1621-Perjury generally; 18 U.S.C.A. § 1001-Statements or entries generally, 18 U.S.C.A. § 912-Officer or employee of the United States; 18 U.S.C.A. § 2234-Authority exceeded in executing warrant; 18 U.S.C.A. § 2236-Searches without warrant, 18 U.S.C.A. § 1905-Disclosure of Confidential Information, while accomplishing their racketeering objectives. *Second Am. Compl.* ¶¶ 132; *see also id.* ¶ 155.

Most of these alleged offenses are not "predicate acts" under the RICO statute. Mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), and theft of trade secrets (18 U.S.C. §§ 1831-1832) [15] qualify; the rest do not. *See*

18 U.S.C. § 1961(1) (listing qualifying offenses).

***24** "Mail or wire fraud requires proof of (1) a scheme to defraud based on false pretenses; (2) the defendant's knowing and willing participation in the scheme with the specific intent to defraud; and (3) the use of interstate mail or wire communications in furtherance of the scheme." *Sanchez v. Triple-S Mgmt., Corp.*, 492 F.3d 1, 9-10 (1st Cir. 2007). "The 'in furtherance' requirement is to be read broadly." *United States v. Simon*, 12 F.4th 1, 33 (1st Cir. 2021). "[T]he mails need not be an essential element of the scheme. It is sufficient for the mailing to be incident to an essential part of the scheme, or a step in [the] plot." *Schmuck v. United States*, 489 U.S. 705, 710-11, 109 S.Ct. 1443, 103 L.Ed.2d 734 (1989) (internal citations and quotations omitted).

Federal Rule of Civil Procedure 9(b) requires that "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." FED. R. CIV. P. 9(b); *see also Humana*, 666 F. Supp. 3d at 154 ("Civil RICO claims based on the predicates of mail or wire fraud must meet the heightened pleading standard of Rule 9(b)"). A complaint must specify "the time, place, and content of an alleged false representation." *United States ex. rel. Kelly v. Novartis Pharms. Corp.*, 827 F.3d 5, 13 (1st Cir. 2016) (quoting *Doyle v. Hasbro, Inc.*, 103 F.3d 186, 194 (1st Cir. 1996)). Furthermore, "[t]he false or fraudulent

representation [in a mail or wire fraud claim] must be material." *United States v. Appolon*, 715 F.3d 362, 367 (1st Cir. 2013) (first alteration in original) (citation omitted).

Plaintiffs' mail and wire fraud claims are limited to allegations that Mr. Jaczewski—in an operation "instructed" by Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel and "supervised and approved" by the Federal Defendants—used an alias to purchase two Naicom set-top boxes and a monthly subscription he maintained for two years. *Second Am. Compl.* ¶¶ 132-37. In Plaintiffs' view, each purchase or payment "constitutes a wire fraud racketeering act since [Mr. Jaczewski, acting under the alias] Brian Parsons, posed as [a] legitimate client and used the interstate internet electronic services to access Naicom's website, and register online under the false pretenses of BRIAN PARSONS" and "made online payments through the use of interstate internet electronic services ... to defraud and deprive Naicom Corporation of its legitimate products, intellectual property and trade secrets." *Id.* ¶ 134. Between the initial purchases and monthly subscription payments, Plaintiffs tally 22 acts of wire fraud. *Id.* ¶ 135. They also consider the initial purchase to constitute mail fraud because Mr. Jaczewski "posed as a legitimate client and used the United States Postal Services to have Naicom mail him the IPTV Set Top Box to a fake address." *Id.* ¶ 133.

Accepting these allegations as true, the Court concludes that the facts are insufficient to support Plaintiffs' wire and mail fraud claims because the purportedly fraudulent representations (limited to Mr. Jaczewski's use of an alias for the set-top-box and subscription purchases) were not material. Nor could the mail and wire fraud allegations be predicate acts for Plaintiffs' RICO claims because the set-top-box operation was not causally connected to Plaintiffs' damages.

A material statement "has a natural tendency to influence, or [is] capable of influencing, the decision of the decision-making body to which it was addressed" but plaintiffs "need not prove that the decisionmaker actually relied on the falsehood or that the falsehood led to actual damages." *Appolon*, 715 F.3d at 368 (alteration in original) (citations and internal quotation omitted). In *Appolon*, the defendant provided untrue responses on a mortgage application, in response to questions "that specifically sought information regarding the purchaser's income, assets, and intent to reside in the property." *Id.* The First Circuit considered the false responses material because the questions "were designed to assess the borrower's creditworthiness" and thus the statements "were capable of influencing [the lender's] decision." *Id.*

***25** The purported false statements here are far afield

from providing false financial information on a mortgage application. Naicom's set-top boxes are commercial electronic products sold in retail stores like Sam's Club, and its subscription services are available on Apple's AppStore as the Naicom TV App. *Second Am. Compl.* ¶ 70 ("On February 16, 2017, Apple Corporation approved Naicom Corporation App for Apple's AppStore as Naicom TV App"); *id.* ¶ 71 ("On December 15, 2017, Sam's Club approved Naicom Corporation to officially launch and distribute in their retail stores [ ] Naicom's IPTV Set Top Box which offered the distribution of tv programming to customers in Puerto Rico"). Plaintiffs allege that Mr. Jaczewski committed wire and mail fraud by providing a false name "of BRIAN PARSONS, fake Phone (727) 409-9464, fake Email: parsons.brian716@outlook.com and Address: 9079 FOURTH STREET NORTH SAINT PETERS FL 33702 IP: 70.127.233.139, and made online payments through the use of interstate internet electronic services using the PM Visa ending in 2775." *Id.* ¶ 134. Plaintiffs also allege that Mr. Jaczewski used the alias of Brian Parsons when purchasing two Naicom set-top boxes. *Id.* ¶ 133.

The allegations confirm that Mr. Jaczewski used the false name of Brian Parsons. It is unclear, however, what Plaintiffs mean by a "fake Phone"—whether Mr. Jaczewski used a different phone as part of the alias or if the number provided was entirely made up. Plaintiffs have not adequately pleaded that the

remaining "false" statements are actually false. The Second Amended Complaint does not allege that email services require customers to use their real name in their email address. Thus, the Second Amended Complaint fails to allege that using an email with "parsons-brian" in the address is a false statement as there is no allegation that the address itself does not actually exist. It is unclear what Plaintiffs mean by a "fake" address, but the Second Amended Complaint does not allege that online retail customers are prohibited from having a product shipped to any address they desire, and Plaintiffs have offered nothing to suggest that this constitutes a false representation. [16] Likewise, nothing in the Second Amended Complaint suggests that the IP address or credit card involved false statements. [17]

The Court is thus left to consider whether Mr. Jaczewski's purchase of two commercially available products and an accompanying subscription using the name Brian Parsons can support Plaintiffs' alleged mail and wire fraud violations. The Court concludes that it cannot, because—absent allegations to the contrary—a customer providing a false name in such circumstances does not have "a natural tendency to influence, [nor is it] capable of influencing, the decision of the decision-making body to which it was addressed." *Appolon*, 715 F.3d at 368. Nothing in the Second Amended Complaint suggests that the use of this alias was material to

Plaintiffs' decision to sell Mr. Jaczewski their commercially available product. There is no allegation that Mr. Jaczewski was either known to Plaintiffs or prohibited from purchasing Plaintiffs' products. What is missing is an allegation that the alias could have reasonably affected the "decision of the decision-making body" (for example, Naicom's sales department's decision to process Mr. Jaczewski's payment or ship his order). Absent allegations regarding how Mr. Jaczewski's alias affected Naicom's decision to sell him their product, Plaintiffs have not pleaded material fraud with the requisite particularity. Plaintiffs' wire and mail fraud claims cannot stand and thus do not count as predicate acts in support of their RICO claim.

***26** Furthermore, even if the Court did find the alleged misrepresentations material, Plaintiffs' claims fall short of the causation standard required for a wire or mail fraud–based RICO claim. *Neurontin*, 712 F.3d at 34 ("[T]he civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements" (citing *Holmes*, 503 U.S. at 268, 112 S.Ct. 1311)). "The 'central question' in evaluating proximate causation in the RICO context 'is whether the alleged violation led directly to the plaintiff's injuries.' " *Sterling Suffolk Racecourse, LLC v. Wynn Resorts, Ltd.*, 990 F.3d 31, 35 (1st Cir. 2021) (quoting *Anza v. Ideal Steel Supply Corp.*, 547 U.S. 451, 461, 126 S.Ct. 1991, 164 L.Ed.2d 720 (2006)). Quoting the U.S. Supreme Court, the First

Circuit has noted that "[a] link [between the RICO predicate acts and plaintiff's injuries] that is too remote, purely contingent, or indirect is insufficient to show proximate cause." *Id.* (alterations in original) (quoting *Hemi Grp., LLC v. City of New York*, 559 U.S. 1, 9, 130 S.Ct. 983, 175 L.Ed.2d 943 (2010)). In addition, the First Circuit has identified "three functional factors with which to assess whether proximate cause exists under RICO." [18] *Id.* (quoting *Neurontin*, 712 F.3d at 35-36). The but-for causation question, in contrast, asks whether the plaintiff would have suffered the same injury absent the defendant's violation. *See Neurontin*, 712 F.3d at 34.

Here, the alleged violations fail both causation tests because Plaintiffs portray the set-top-box operation as an unmitigated failure that only provided further proof that Naicom was a legitimate company. Plaintiffs allege that "after testing Naicom TV several times to identify if it was providing DISH programming, on each case the test *revealed no DISH content*." *Second Am. Compl.* ¶ 90 (emphasis added). After attempting to use the boxes to penetrate Plaintiffs' network and steal their secrets, the "Dish/NagraStar defendants also informed the Racketeering Enterprises that the Association in Fact defendants couldn't penetrate Naicom's Data Center computers, servers, encoders electronic security system, and that a physical intrusion was necessary to extract the intellectual property from the computers, servers, and encoders by physical access." *Id.* ¶ 93. Plaintiffs further

allege that the operation did not yield evidence that would support a search warrant and thus the defendants had to provide "affidavits they knew contained material information known to be false and perjured to create probable cause to gain legal access into Plaintiffs' private business." *Id.* ¶ 20.

As the Court understands the Second Amended Complaint, Plaintiffs allege that all Defendants conspired from the outset to steal their intellectual property. The set-top-box operation was an attempt to steal Plaintiffs' secrets by reverse engineering the technology and/or penetrating Plaintiffs' networks. But the operation failed. All the Defendants gained was more proof that Naicom was a legitimate company, and they then had to resort to falsifying affidavits to justify physical access to Naicom's Data Center (through a search warrant) that would finally allow them access to the desired technology. Plaintiffs have not alleged any harm prior or unrelated to the execution of the warrants. Nor have Plaintiffs alleged that the Defendants would not have sought and executed the search warrants had they not undertaken the set-top-box operation.

The Court concludes that there is no connection—proximate or but-for—between the allegedly fraudulent set-top-box purchase and Defendants acquiring Plaintiffs' intellectual property during the execution of the warrants. The alleged mail and wire fraud is "too

remote" from Plaintiffs' alleged harms, *Hemi Grp.*, 559 U.S. at 9, 130 S.Ct. 983, and there is no indication that Plaintiffs would not have suffered their alleged harms absent the set-top-box operation. Plaintiffs' Second Amended Complaint thus falls short on both the materiality and causation standards for wire and mail fraud as predicate acts.

c. Pattern of Racketeering Activity: Theft of Trade Secrets

***27** RICO predicate offenses include any act indictable under 18 U.S.C. § 1832, relating to theft of trade secrets under the DTSA. 18 U.S.C. § 1961(1). 18 U.S.C. § 1832 provides that "[w]hoever, with intent to convert a trade secret ... to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information," or attempts to do so, shall be subject to criminal penalties. *Id.* § 1832(a)(1), (a)(4). "Trade secret" is defined broadly to include "all forms and types of financial, business, scientific, technical, economic, or engineering information," as long as "the owner thereof has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily

ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." *Id.* § 1839(3). Critically, however, the DTSA also provides that "[t]his chapter does not prohibit ... any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State." *Id.* § 1833(a)(1).

DISH Corp. argues that Plaintiffs fail to state a claim under the DTSA because the conduct alleged in the Second Amended Complaint was "supported by allegations of legitimate government action." *Def.'s Mot.* at 18 (quoting *Kahre v. Damm*, No. 2:07-CV-00231-DAE-RJJ, 2007 U.S. Dist. LEXIS 95978 at *26, 2007 WL 9728869 (D. Nev. Dec. 18, 2007)). DISH Corp. further submits that "all actions taken by DNC were performed under color of federal law, and at the direction and supervision of the Federal Defendants to assist them in discharging their governmental duties, including assisting with the investigation into Naicom's IPTV business operations and executing search warrants signed by a magistrate judge." *Id.* at 20.

Plaintiffs respond that the conduct alleged in the Second Amended Complaint was not legitimate law enforcement activity because "the procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Pls.' Opp'n* at 25.

Because the DTSA contains an exception for governmental activity, and the parties dispute whether the conduct alleged in the Second Amended Complaint constitutes governmental activity, the Court addresses this issue first. To do so, the Court examines the validity of the warrants.

The relevant standard for evaluating the validity of a warrant is the *Franks v. Delaware* framework, which requires Plaintiffs to adequately allege that both (1) "a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit" and (2) "the allegedly false statement is necessary to the finding of probable cause." *United States v. Reiner*, 500 F.3d 10, 14 (1st Cir. 2007) (quoting *Franks v. Delaware*, 438 U.S. 154, 155-56, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978)). Plaintiffs cite ten statements that the Defendants allegedly "falsely submitted to the Court" in an affidavit supporting their search warrant application. *Pls.' Opp'n* at 25. The Court has examined each and concludes that none supports Plaintiffs' claims.

The first purportedly false statement identified by Plaintiffs is the Defendants' statement that they believed there was probable cause that Plaintiffs were violating copyright and money laundering laws. *Id.* at 25-26. Plaintiffs allege that this statement is false because:

The execution of the search and seizure warrant in this case did not produce any criminal evidence whatsoever; there was no probable cause. That is why the United States never opposed Plaintiffs['] Motion for Return of Property under Rule 41(g) of the Fed.R.Crim.P. In fact, they didn't even contend the serious violations Plaintiffs imputed under *Franks* in the Rule 41(g) motion.

Id. at 26. This logic is unavailing. Plaintiffs cannot rely on the circular reasoning that the search's alleged failure to produce incriminating evidence thereby proves the Defendants could not have believed there was probable cause to search. *See Karamanoglu v. Town of Yarmouth*, 15 F.4th 82, 88 (1st Cir. 2021) (defining the probable cause inquiry as "whether, on balance, the facts *known to the officer at the time of the arrest* support probable cause" (emphasis in original)).

***28** Equally inadequate is Plaintiffs' claim that the Federal Defendants' failure to oppose Plaintiffs' motion to return the seized property proves not only that the seized property was not incriminating, but also that there was no probable cause to search in the first place. *See United States v. Pierre*, 484 F.3d 75, 87 (1st Cir. 2007) ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return"). The government's return of the seized hard drives and thumb drives, which—unlike drugs or illegal

firearms—are not inherently contraband and can easily be downloaded or duplicated, is consistent with *Pierre*.

Furthermore, Plaintiffs are simply incorrect that success on a Rule 41(g) motion conclusively establishes the invalidity of a search. Rule 41(g) allows motions for return of property from "[a] person aggrieved by an unlawful search and seizure of property *or* by the deprivation of property." FED. R. CRIM. P. 41(g) (emphasis supplied). Without more, the property's return alone cannot demonstrate an absence of probable cause to search and seize in the first place. Ultimately, Plaintiffs' first purportedly false statement offers nothing to undermine the validity of the warrants and searches.

Second, Plaintiffs offer that the Defendants "assured the Court they had evidence based on an investigation conducted by NagraStar of Naicom's unauthorized use of Direct TV signal to distribute its programming to its paid subscribers." *Pls.' Opp'n* at 26. Plaintiffs assert that this statement was false because "[t]he United States did not produce any evidence as to the above allegations," whereas "Naicom did produce all the documentary evidence establishing that they were authorized to distribute the copyright material and running a legitimate IPTV system." *Id.*

Again, Plaintiffs appear to be suggesting that

exculpatory evidence they produced during the warrants' execution proves that the underlying affidavit was false. These conclusory assertions tied together by circular logic do not adequately demonstrate the falsity of the affidavit. While Plaintiffs contend the affidavit did not "produce any evidence" supporting the suggestion that Naicom was distributing DirecTV content without authorization, the affidavit avers that Naicom's system displayed DirecTV error messages on at least 16 channels (and includes a photo of the message), that Naicom's satellite dishes were precisely oriented in a manner necessary to receive DirecTV satellite signals, that representatives of the companies offering some channels Naicom purported to provide confirmed that Naicom was not licensed to provide them, and other indicia of piracy. *See Pls.' Opp'n to DISH/NagraStar Mot.*, Attach. 1, *Aff. in Supp. of an Application for a Search Warrant* (*Warrant Aff.*). Simply put, Plaintiffs' argument that the affidavit contained no evidence of piracy is incorrect.

Third, Plaintiffs assert that, during a 2018 FBI site visit of Naicom's property, Mr. Vega "repeatedly told the agent that Naicom was a legal corporation and showed the agent a certificate from the National Cable Television Cooperative (NCTC) on the wall," yet the Federal Defendants still "filed the affidavit containing material false and perjured statements." *Pls.' Opp'n* at 26-27. It is not clear specifically which "materially false and

perjured statements" Plaintiffs are referring to, but the affidavit states that the FBI called NCTC's management group, which confirmed that Naicom was *not* a member. *Warrant Aff.* ¶ 15. Nothing in Plaintiffs' assertion that Mr. Vega told the FBI his company was legitimate and showed them a certificate on the wall establishes that the affidavit's claim—that NCTC management represented to the FBI that Naicom was not a member—was perjured.

***29** Fourth, Plaintiffs contend that the affidavit's claim that Naicom was using the NCTC certificate to create the appearance of legal access to channels was a "false and perjured statement" because an FBI agent took pictures of "Naicom's National Rural Telecommunications Cooperative 'NRCT' Certificate" and Naicom had licenses with other networks. *Pls.' Opp'n* at 27.

Fifth, Plaintiffs focus on the affidavit's claim that an FBI agent spoke with NCTC management, who confirmed that Naicom was not a member of their organization. *Id.* Plaintiffs allege that this "is a false and perjured statement" because Naicom provided evidence that it is a member of the NRTC. *Id.*

The distinction between NCTC and NRTC here is somewhat confusing. It appears that Plaintiffs are alleging the FBI took pictures of a NRTC certificate on the wall but incorrectly referred to it in the affidavit as a

NCTC certificate, or that the FBI mistook their NRTC certificate for an NCTC certificate. However, Plaintiffs also claim that the affidavit's assertion that they are not a member of the NCTC is a perjured statement because they provided evidence that they are a member of the NRTC. Plaintiffs offer no evidence that the latter statement was perjured because proving they are a NRTC member does not contradict the claim that they are not a NCTC member. To the extent the FBI may have misidentified a NRTC certificate as a NCTC certificate, the record does not suggest that this "allegedly false statement is necessary to the finding of probable cause," especially given the strength of the other supporting claims in the affidavit. *United States v. Patterson*, 877 F.3d 419, 424 (1st Cir. 2017) (quoting *Franks*, 438 U.S. at 156, 98 S.Ct. 2674).

Sixth, Plaintiffs turn to the affidavit's assertion that FBI agents contacted officials at HBO and DirecTV, who verified that Naicom did not have a relationship with their organizations despite offering HBO content. *Pls.' Opp'n* at 27. Plaintiffs claim that "[t]his is a false and perjured statement" because "Naicom provided evidence that it is licensed to distribute HBO and Cinemax programming." *Id.* at 27-28 (citing *Pls.' Opp'n to DISH/NagraStar Mot.*, Attach. 1 at 356) (HBO invoice dated August 31, 2019, for roughly $200 per month for "Cable — Private Home" services). Plaintiffs' claim is unpersuasive for two reasons: (1) this invoice for

inexpensive "Cable – Private Home" services does not appear to provide evidence of a licensing agreement; and (2) Plaintiffs have not directly contradicted the purportedly perjured claim, which was that HBO and DirecTV officials represented to the FBI that they did not have a relationship with Naicom.

Seventh, Plaintiffs focus on the affidavit's claim that the "external appearance of the Data Center offered indicia of piracy," calling it a "false and perjured statement" because "[a]t the conclusion of the search and seizure warrant execution the FBI agents found that [ ] Naicom's equipment (encoders) were provided by the networks authorizing the programming distribution and that the use of the satellite was in fact to download the codes provided by the networks." *Pls.' Opp'n* at 28. Plaintiffs again rely on circular logic, as the discovery of exculpatory evidence at the conclusion of a warrant's execution does not provide a "substantial preliminary showing" that the underlying affidavit was perjured. *Franks*, 438 U.S. at 155-56, 98 S.Ct. 2674.

***30** Plaintiffs' eighth point suffers from the same defect. They claim that the affidavit's statements that there were suspicious financial transactions between Naicom and other businesses owned by Mr. Quinones and Mr. Vega were false and perjured because "[d]uring the execution of the Search Warrant S/A Lange interviewed employees from the Business Office and was provided with financial

records," which established "that none of the Corporations were involved in any money laundering activities." *Pls.' Opp'n* at 28-29. Again, the fact that a search did not uncover incriminating evidence does not establish that it was predicated on a perjured affidavit.

Plaintiffs' ninth point takes issue with the affidavit's request to seize computers and data based on claimed probable cause that they contained evidence. *Id.* Plaintiffs contend that this statement was perjured because "the FBI agents were not looking for any criminal evidence" during the search and they did "not find[ ] any evidence whatsoever of the crimes described in the warrant, which also denied any probable cause." *Id.* at 29. The Court does not fully follow Plaintiffs' logic across these seemingly contradictory assertions, but they appear to utilize the same circular reasoning (the assertion of probable cause was perjured because the resulting search "denied any probable cause"), along with the conclusory contention that the FBI was not actually looking for evidence. These claims do not undermine the validity of the warrants.

Tenth, Plaintiffs claim that the affidavit's request to seize evidence of statutory violations was "false and perjured" because the FBI did not find any evidence at the conclusion of the search warrant execution. *Id.* Beyond the fact that this argument relies on the same circular logic, an affidavit's request to seize "things and ...

records" is not an assertion of fact and cannot be false or perjured. *Id.*

To summarize, none of these purportedly false statements, alone or in combination, satisfies Plaintiffs' burden under the *Franks* standard to overcome the presumed validity of the warrants. Moreover, Plaintiffs offer several additional, similarly unavailing, arguments that their DTSA allegations do not constitute legitimate law enforcement activity.

Plaintiffs submit that the August 29, 2019 search was "illegal" and "warrantless" because "[t]he Federal and Dish/NagraStar Defendants knew for a fact that the first search warrant execution had already denied any criminal wrongdoing, and that the initial alleged probable cause had dissipated." *Id.* at 36. This assertion—that the Defendants knew probable cause had dissipated—is wholly conclusory (especially in light of Plaintiffs' argument that the entire investigation was a hoax, and the agents knew probable cause never existed). Furthermore, the warrant did not expire until September 4, 2019 and courts generally recognize a "reasonable continuation rule" providing that a search may be reasonably continued if the warrant remains valid. [19] *See United States v. Keszthelyi*, 308 F.3d 557, 568-569 (6th Cir. 2002) (describing the rule and collecting cases). Plaintiffs have not offered any well-pleaded, nonconclusory allegations suggesting that the

continuance here was unreasonable. [20]

***31** Plaintiffs also contend that the searches were unlawful because the Federal Defendants did not follow the procedure to obtain a Stored Communications Act warrant (also known as a SCA order). *Pls.' Opp'n* at 31-33, 35. But this argument lacks merit because the Federal Defendants appropriately obtained traditional search warrants in lieu of a SCA order.

SCA orders are different from traditional search warrants. As one court has explained:

> SCA warrants "are not like the search warrants used in the physical world: they are 'executed' when a law enforcement agent delivers (sometimes by fax) the warrant to the [service provider]. The [service provider], not the agent, performs the 'search'; the [service provider] 'produces' the relevant material to the agent; the user associated with the inbox often never learns that his inbox has been 'searched.' In sum, these are not search warrants at all and to call them such confuses legal terminology."

In re Info. Associated with @gmail.com, No. 16-mj-00757 (BAH), 2017 U.S. Dist. LEXIS 130153, at *52-53, 2017 WL 3445634 (D.D.C. July 31, 2017) (quoting Paul K. Ohm,

Parallel–Effect Statutes and E–Mail "Warrants": Reframing the Internet Surveillance Debate, 72 GEO. WASH. L. REV. 1599, 1610-11 (2004)). Additionally, the standard for a SCA order is "less stringent than the probable cause standard generally required for a search warrant." *United States v. Taylor*, 54 F.4th 795, 804 (4th Cir. 2022). Finally, even if the Defendants were seeking information protected by the SCA, the statute gives law enforcement the option of seeking either a SCA order or a traditional search warrant. [21] *See* 18 U.S.C. § 2703(b) (the government may obtain "a court order for such disclosure under subsection (d) of this section" *or* "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"); *id.* § 2703(c) (same).

Plaintiffs' argument is groundless because the Federal Defendants were primarily—if not entirely—seeking information not protected by the SCA. Regardless, they obtained search warrants for the facility and computer systems, thereby satisfying the requirements of the SCA.

Plaintiffs also submit once again that "[t]he DNC Defendants can't raise at this time the defense that the execution of the search and seizure warrant was authorized, legal and constitutional, which was waived during the Rule 41(g) proceedings and abandoned forever." *Pls.' Opp'n* at 39.

However, as the Court has already explained, the government's decision not to oppose a motion to return property does not affect the validity of the warrant or seizure. *See Pierre*, 484 F.3d at 87 ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return").

Finally, although Plaintiffs contend that the search warrant executions were unlawful due to the involvement of the DISH/NagraStar Defendants, they acknowledge that "Congress has explicitly authorized" private parties to assist law enforcement in the execution of search warrants. *Pls.' Opp'n* at 33-34 (citing 18 U.S.C. § 3105). Further, although they contend that any civilian assisting with a search "must have been serving a legitimate investigative junction," *id.* at 34, Plaintiffs fail to make any well-pleaded, nonconclusory allegation that the DISH/NagraStar Defendants were not serving such a function. Indeed, Plaintiffs do not offer any persuasive argument that would permit the Court to find that the DISH/NagraStar Defendants' presence rendered the search illegal. [22]

***32** In sum, Plaintiffs have failed to adequately challenge the validity of the search warrants or establish that anything about the warrants' executions was unlawful. Plaintiffs have thus failed to plead a DTSA violation as a predicate act in support of their RICO claim because the allegations in the Second Amended

Complaint merely suggest that the Defendants were engaging in legitimate law enforcement activity. *See* 18 U.S.C. § 1833(a)(1) ("This chapter does not prohibit ... any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State"). Absent both an enterprise and any predicate acts, Plaintiffs' RICO claim (Count I) must be dismissed as to DISH Corp.

These same pleading shortfalls doom Plaintiffs' RICO conspiracy claim. *See Efron*, 223 F.3d at 21 (1st Cir. 2000) ("A conspiracy claim under section 1962(d) may survive a *factfinder's* conclusion that there is insufficient evidence to prove a RICO violation, but if the pleadings do not state a substantive RICO claim upon which relief may be granted, then the conspiracy claim also fails" (citations omitted) (emphasis in original)); *see also Salinas v. United States*, 522 U.S. 52, 64, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997) ("A conspirator must intend to further an endeavor which, if completed, *would satisfy all of the elements of a substantive criminal offense*, but it suffices that he adopt the goal of furthering or facilitating the criminal endeavor" (emphasis supplied)). As such, the Court also dismisses Plaintiffs' RICO conspiracy claim (Count II).

D. Plaintiffs' PTSA Claim

As noted above, the Second Amended Complaint states

that the Court has federal question jurisdiction over Counts I through VI and supplemental jurisdiction over Count VII. *Second Am. Compl.* ¶¶ 28-29. Having dismissed Counts I through VI, the Court also dismisses Count VII pursuant to 28 U.S.C. § 1367(c)(3). [23] *See* 28 U.S.C. § 1367(c) (3) (providing that "district courts may decline to exercise supplemental jurisdiction over a claim" if "the district court has dismissed all claims over which it has original jurisdiction").

VI. CONCLUSION

The Court GRANTS Defendant DISH Network Corporation's Motion to Dismiss (ECF No. 136). The Court DISMISSES Counts I though VII of Plaintiff's Second Amended Complaint as pleaded against DISH Network Corporation.

SO ORDERED.

All Citations

Not Reported in Fed. Supp., 2024 WL 1363755

Footnotes

1 This is the second lawsuit arising out of the underlying

events at issue. On August 25, 2020, a group of plaintiffs, including many of Plaintiffs here, filed a *Bivens* action against many of the same defendants. *See Quinones-Pimentel v. Cannon*, No. 3:20-cv-01443-JAW, 2022 U.S. Dist. LEXIS 48109 at *2-3, 2022 WL 826344 (D.P.R. Mar. 17, 2022). On March 17, 2022, the Court dismissed the plaintiffs' *Bivens* action. *Id.* At *88. The plaintiffs appealed, and the Court of Appeals for the First Circuit affirmed the Court's dismissal on October 27, 2023. *Quinones-Pimentel v. Cannon*, 85 F.4th 63, 66-68 (1st Cir. 2023).

2 In their Second Amended Complaint, Plaintiffs use the spelling, "Rinkle." *See, e.g.*, *Second Am. Compl.* ¶ 43. In her filings, however, Ms. Rinkel uses the spelling, "Rinkel." *See, e.g.*, *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Mot. to Dismiss* at 1 (ECF No. 134). No doubt, Ms. Rinkel knows how to spell her own name, and the Court uses "Rinkel" throughout this order.

3 Consistent with Federal Rule of Civil Procedure 12(b)(6), in describing the facts, the Court has relied upon the allegations in the Second Amended Complaint. *Foley v. Wells Fargo Bank, N.A.*, 772 F.3d 63, 68 (1st Cir. 2014); *Medina-Velázquez v. Hernández-Gregorat*, 767 F.3d 103, 108 (1st Cir. 2014) ("We examine whether the operative complaint states a claim for which relief can be granted when we construe the well-pleaded facts in the light most favorable to the plaintiffs, accepting their truth and drawing all reasonable inferences in plaintiffs' favor" (internal citation omitted)).

4 Presumably because Claro Puerto Rico is a well-known business in Puerto Rico, the Second Amended Complaint does not describe Claro Puerto Rico except by name. *See Second Am. Compl.* ¶ 68. According to Wikipedia, Claro Puerto Rico is the one of the largest telecommunications companies in Puerto Rico. *See Claro P.R.*, WIKIPEDIA (updated Oct. 14, 2023), *https://en.Wikipedia.org/wiki/Claro_Puerto_Rico*.

5 The Second Amended Complaint often refers to the

"Association in Fact defendants." *See, e.g., Second Am. Compl.* ¶ 87. As the Court understands the Second Amended Complaint, this term refers to all Defendants collectively. *See id.* ¶¶ 17, 62 (listing all the Defendants as together "form[ing] an Association in Fact").

6 Here, the Court quotes the language in the Second Amended Complaint. *Second Am. Compl.* ¶ 103. In the context of this sentence, the meaning of the verb, "counted," is unclear. It would make more sense if the sentence used "complied with," rather than "counted." Whichever verb is correct, however, makes no difference in this Court's ruling on the motion to dismiss.

7 The Plaintiffs variously spell NagraStar with a capital "S" and with a lower-case "s." *Compare Second Am. Compl.* ¶ 21, *with Pls.' Opp'n to DISH / NagraStar Mot.* at 1. NagraStar spells its name with a capital "S." *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel and Jordan Smith's Mot. to Dismiss* at 1. Again, on the assumption that NagraStar knows how to spell its own name, the Court has used NagraStar and insertedå this spelling in lower case references.

8 Plaintiffs also suggest that the Court should strike all the defenses raised by DISH Corp. pursuant to Federal Rule of Civil Procedure 12(f) because "there are no factual nor issues of law to be resolved before the validity of the defenses in the present context may be determined." *Pls.' Sur-Reply* at 9. The Court declines to do so.

9 The majority of Plaintiffs' claims about the alleged conspiracy do not even mention DISH Corp. specifically, but instead refer to the "Racketeering Enterprises." *See, e.g.*, *Second Am. Compl.* ¶¶ 92-93, 98-99, 130-31. According to Plaintiffs, the Racketeering Enterprises are DISH Corp., DISH LLC, and NagraStar. *Id.* ¶ 125. It is unclear which of the Racketeering Enterprises' contacts with Puerto Rico can be attributed to DISH Corp., as opposed to DISH LLC or NagraStar.

10 For their part, the DISH Corp. Defendants rely on the

Declaration of Jason Anguiano, which represents that DISH Corp: 1) "does not directly maintain any retail stores, warehouses, offices, mailing addresses, bank accounts, telephone listings, agents, or other personnel" in Puerto Rico; 2) "does not have any officers in Puerto Rico"; and 3) "does not directly own, manage, or lease any real or tangible property in Puerto Rico, conduct business in Puerto Rico, or maintain a registered agent for service of process in Puerto Rico." *Def.'s Mot.*, Attach. 1, *Decl. of Jason Anguiano* at 2. The only portion of the Anguiano Declaration directly disputed by Plaintiffs is the representation that DISH Corp. does not conduct business in Puerto Rico.

11 Plaintiffs also argue that they "are entitled to limited [jurisdictional] discovery to review the DNC and Nagrastar Joint Venture agreement to form Nagrastar LLC, by and between EchoStar Communications Corporation and Kudelski S.A." *Pls.' Opp'n* at 17. A "plaintiff who seeks jurisdictional discovery must make 'a colorable claim of jurisdiction' and must show that it 'has been diligent in preserving [its] rights to be entitled to jurisdictional discovery.' " *Motus, LLC v. Car Data Consultants, Inc.*, 23 F.4th 115, 128 (1st Cir. 2022) (quoting *Swiss Am. Bank, Ltd.*, 274 F.3d at 625-27). Because an examination of the agreements identified by Plaintiffs would only shed light on liability, not jurisdiction, the Court concludes that Plaintiffs' discovery request does not identify "a sufficient predicate for in personam jurisdiction." *Id.* (citing *Blair v. City of Worcester*, 522 F.3d 105, 111 (1st Cir. 2008)). Accordingly, the Court denies Plaintiffs' request for jurisdictional discovery.

12 Plaintiffs submit "that the DNC defendants failed to raise personal jurisdiction defenses" with respect to Counts IV, VI, and VII and "have therefore, waived any defense available under those claims pursuant to Rule 12(h)." *Pls.' Opp'n* at 20-21. This ignores that the basis for personal jurisdiction for these Counts IV and VI is the same as for Counts III and V. The Court rejects Plaintiffs' waiver argument as to Counts IV and VI and addresses Count VII below.

13 Here, DISH Corp. encourages the Court to bypass its

personal-jurisdiction defense and resolve Plaintiffs' RICO claims on the merits. *See Defs.' Reply* at 7-8 ("Notwithstanding the forgoing, if the Court dismisses Plaintiffs' RICO claims pursuant to the 12(b)(6) motions filed by the Federal Defendants, the DISH/NagraStar Defendants and the Toltec Defendants, it is unnecessary for the Court to reach DNC's jurisdictional challenge or the applicability of RICO's nationwide service of process provision").

14 These allegations are also conclusory. Plaintiffs claim that "the Racketeering Enterprise's ongoing regular way of business is to attempt to steal Intellectual Property, Patents, and Trade Secrets, from their owners every time they can do so." *Second Am. Compl.* ¶ 129. This allegation is supported only by references to other lawsuits involving DISH, and Plaintiffs do not attempt to connect the facts of these lawsuits to the present case. *Id.*

15 The statutory provision cited by Plaintiffs—18 U.S.C. § 1836—governs civil proceedings for misappropriation of trade secrets and is not listed as a predicate act in 18 U.S.C. § 1961(1). Since the Court assumes Plaintiffs' reference to 18 U.S.C. § 1836 was in error, the Court has recharacterized Plaintiffs' predicate-act allegations relating to theft of trade secrets as arising under 18 U.S.C. §§ 1831 and 1832.

16 In theory, Mr. Jaczewski could have provided an address that was entirely made up. This seems unlikely, however, because the Second Amended Complaint alleges that the Defendants used the set-top boxes to attempt remote attacks on Naicom's servers. Had the boxes been shipped to an address that didn't exist, they would have been returned to Naicom as undeliverable, meaning that the Defendants could not have used them to launch sniffing attacks. The Plaintiffs do not appear to allege that the mailing address is a fake address, and the Court doubts that they could do so, based on the information in this case.

17 To the contrary, the Second Amended Complaint includes a table listing all the payments made to Naicom by Mr. Jaczewski

posing as Brian Parsons. *Second Am. Compl.* ¶ 136. In the Court's view, these payments confirm that the credit card number provided by Mr. Jaczewski was valid.

18 These factors are: (1) "concerns about proof" because "the less direct an injury is, the more difficult it becomes to ascertain the amount of a plaintiff's damages attributable to the violation, as distinct from other, independent, factors," ... (2) "concerns about administrability and the avoidance of multiple recoveries," ... and (3) "the societal interest in deterring illegal conduct and whether that interest would be served in a particular case[.]" *Sterling Suffolk Racecourse*, 990 F.3d at 35-36 (quoting *Neurontin*, 712 F.3d at 35-36).

19 The "reasonable continuation rule" requires the satisfaction of two conditions: 1) "the subsequent entry must indeed be a continuation of the original search, and not a new and separate search"; and 2) "the decision to conduct a second entry to continue the search must be reasonable under the totality of the circumstances." *Keszthelyi*, 308 F.3d at 569.

20 The closest Plaintiffs come to a nonconclusory allegation is their assertion that U.S. Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned, after the execution of the first search warrant, that Naicom complied with "all the programming distribution contract and agreements." *Second Am. Compl.* ¶ 103. But this allegation is still conclusory, and it is undercut by the sentence immediately following it, which alleges that the USAO Defendants instructed S/A Pearson "to order Darwin Quinones and Victor Vega to report to the FBI Offices in San Juan with the licensing contracts for an interview regarding Naicom's company." *Id.* Clearly, whatever U.S Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned did not absolve Naicom of wrongdoing; otherwise, there would have been no need to conduct an interview.

21 Further, "the statute offers no express direction as to when

the government should seek a warrant versus" a SCA order. *Taylor*, 54 F.4th at 804.

22 Plaintiffs quote *Bellville v. Town of Northboro*, 375 F.3d 25 (1st Cir. 2004), for the proposition that "it might be a better practice, if circumstances permit, for law enforcement officers to disclose to the magistrate that civilians will be involved in the execution of the search and for the warrant to indicate that the magistrate permitted this involvement." *Pls.' Opp'n* at 21 (footnotes omitted) (quoting *Bellville*, 375 F.3d at 33-34). They fail to quote the preceding sentence, which states, "we will not improvise a rule that seems unnecessary in light of the overarching requirement that the use of civilians in the execution of a search must still meet the constitutional standard of reasonableness." *Bellville*, 375 F.3d at 33. The Court declines Plaintiffs' invitation to convert the best practice outlined by the First Circuit into a rule.

23 Plaintiffs also suggest that the Court has diversity jurisdiction pursuant to 28 U.S.C. § 1332 "because this suit is between a citizen of a domestic state (Naicom Corporation), (Kiaras, LLC), and (Paylink, LLC), and a citizen of a foreign state (Dish Network Corporation), (Dish Network, LLC) and (Nagrastar, LLC), and (Toltec Investigations, LLC)." *Second Am. Compl.* ¶ 30. The Supreme Court has "consistently interpreted § 1332 as requiring complete diversity: In a case with multiple plaintiffs and multiple defendants, the presence in the action of a single plaintiff from the same State as a single defendant deprives the district court of original diversity jurisdiction over the entire action." *Exxon Mobil Corp. v. Allapattah Servs., Inc.*, 545 U.S. 546, 553, 125 S.Ct. 2611, 162 L.Ed.2d 502 (2005). Here, all Plaintiffs and several Defendants are residents of Puerto Rico. *Second Am. Compl.* ¶¶ 33-36, 46-55. Because there is not complete diversity, and "[i]ncomplete diversity destroys original jurisdiction with respect to all claims," Plaintiffs' assertion that the Court has diversity jurisdiction is incorrect. *Allapattah*, 545 U.S. at 554, 125 S.Ct. 2611.

2024 WL 1363781

Only the Westlaw citation is currently available. United States District Court, D. Puerto Rico.

NAICOM CORPORATION, et al., Plaintiffs,

v.

DISH NETWORK CORPORATION, et al., Defendants.

No. 3:21-cv-01405-JAW

|

Signed March 29, 2024

Attorneys and Law Firms

Rafael F. Castro-Lang, Castro & Castro Law Office, San Juan, PR, for Plaintiffs.

Chad M. Hagan, Pro Hac Vice, Timothy Frank, Pro Hac Vice, Hagan Noll & Boyle LLC, Houston, TX, Jose L. Ramirez-Coll, Antonetti Montalvo & Ramirez-Coll, San Juan, PR, Carolina V. Cabrera-Bou, AMRC, LLC, San Juan, PR, for Defendants Dish Network Corporation, DISH Network L.L.C., NagraStar LLC, Bert Eichhorn, Emily Rinkle, Jordan Smith, Kevin Gedeon, Michael Thomas Jaczewski. Patrick B. Fenior, DOJ-Civ, Washington, DC, Priscila M. Acevedo-Roman, U.S. Attorney's Office for the District of Puerto Rico, San Juan, PR, for Defendants United States Attorney for the District of Puerto Rico, Rosa Emilia Rodriguez-Velez, Jose Capo,

Nicholas W. Cannon, Federal Bureau of Investigations San Juan Field in Puerto Rico, Douglas A. Leff, Bradely Rex, Lance Lange, Clay Rehrig, Juan Galarza, Jason Lopez, Kevin Pearson, United States Attorney's Office. Jose L. Ramirez-Coll, Antonetti Montalvo & Ramirez-Coll, San Juan, PR, Carolina V. Cabrera-Bou, AMRC, LLC, San Juan, PR, for Defendant Toltec Investigations, LLC.

ORDER ON FEDERAL DEFENDANTS' MOTION TO DISMISS

JOHN A. WOODCOCK, JR., UNITED STATES DISTRICT JUDGE

***1** A set of federal-employee defendants moves to dismiss plaintiffs' seven-count complaint, arising from federal agents searching plaintiffs' business and seizing their intellectual property. The Court grants the motion to dismiss, dismissing all seven counts. At the outset, based on the allegations in the complaint, the Court determines that the prosecutor defendants are entitled to absolute prosecutorial immunity on all counts. The Court dismisses the RICO claims (Counts I & II) because plaintiffs have not adequately pleaded an enterprise, a pattern of racketeering activity, or a conspiracy. The Court dismisses the Computer Fraud and Abuse Act claim (Count III), the Stored Communications Act claim (Count IV), the Digital Millennium Copyright Act claim (Count V), and the Defend Trade Secrets Act claim (Count VI)

because the alleged conduct falls within statutory exceptions for authorized law enforcement activity. Finally, the Court dismisses the Puerto Rico Uniform Trade Secrets Act claim because the defendants must be substituted pursuant to the Westfall Act and plaintiffs have not complied with the procedural requirements of the Federal Tort Claims Act.

I. PROCEDURAL HISTORY

On August 27, 2021, Naicom Corporation, D&V IP Holdings, LLC, Paylink, LLC, and Kiaras, LLC, filed a seven-count complaint against approximately twenty known Defendants and two dozen unknown Defendants. [1] *Compl.* (ECF No. 1). The Court has twice permitted Plaintiffs to amend their complaint, and the Second Amended Complaint is now the operative complaint. *Am. Compl.* (ECF No. 100); *Second Am. Compl.* (ECF No. 130).

The parties categorize the numerous Defendants into four groups: 1) DISH Network LLC, NagraStar LLC, Bert Eichhorn, Emily Rinkel, [2] Jordan Smith, and Kevin Gedeon (the DISH/NagraStar Defendants); 2) DISH Network Corporation (DISH Corp. or DNC); 3) Toltec Investigations, LLC and its President and CEO, Michael Thomas Jaczewski (the Toltec Defendants); and, 4) former U.S. Attorney Rosa E. Rodriguez-Velez, former Assistant U.S. Attorney Jose Capo-Iriarte, Assistant U.S. Attorney

Nicholas W. Cannon (the USAO Defendants) and Special Agents and employees of the Federal Bureau of Investigation Douglas Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, and Jason Lopez (the FBI Defendants) (collectively, the Federal Defendants).

***2** Plaintiffs allege: 1) violations of the Racketeer Influenced and Corrupt Organizations Act (RICO); 2) a RICO conspiracy; 3) violations of the Computer Fraud and Abuse Act (CFAA); 4) violations of the Stored Communications Act (SCA); 5) violations of the Digital Millennium Copyright Act (DMCA); 6) violations of the Defend Trade Secrets Act (DTSA) by misappropriation of trade secrets; and 7) violations of the Puerto Rico Industrial and Trade Secrets Protection Act (PTSA) under the Uniform Trade Secrets Act (Law No. 80). *Second Am. Compl.* ¶¶ 124-202.

On October 31, 2022 and November 1, 2022, each of the four groups of Defendants filed a motion to dismiss the complaint. *Fed. Defs.' Mot. to Dismiss* (ECF No. 138) (*Defs.' Mot.*); *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel and Jordan Smith's Mot. to Dismiss* (ECF No. 134); *Def. DISH Network Corp.'s Mot. to Dismiss* (ECF No. 136); *Defs.' Toltec Investigations L.L.C. and Mike Jaczewski's Mot. to Dismiss* (ECF No. 137).

On December 5, 2022, Plaintiffs filed a response to the DISH/NagraStar Defendants' motion to dismiss. *Mot. in Resp. to Dish/NagraStar Defs.' Mot. to Dismiss* (ECF No. 147) (*Pls.' Opp'n to DISH/NagraStar Mot.*). On January 18, 2023, Plaintiffs responded to the Federal Defendants' motion. *Mot. in Resp. to the Fed. Defs.' Mot. to Dismiss* (ECF No. 153) (*Pls.' Opp'n*). On February 21, 2023, the Toltec Defendants withdrew a section of their motion to dismiss, *Unopposed Notice of Partial Withdrawal of Toltec Investigations L.L.C. and Mike Jaczewski's 12(b)(2) Mot. to Dismiss* (ECF No. 163), and on February 27, 2023, Plaintiffs responded to the remainder of the Toltec Defendants' motion. *Mot. in Resp. to Toltec Investigations and Mike Jaczewski's Mot. to Dismiss* (ECF No. 167). On March 17, 2023, Plaintiffs responded to DISH Corp.'s motion. *Mot. in Resp. to Dish Network Corp.'s Mot. to Dismiss* (ECF No. 179).

Each group of Defendants filed a reply in support of its motion. *Fed. Defs.' Reply* (ECF No. 173) (*Defs.' Reply*); *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel and Jordan Smith's Reply* (ECF No. 164); *Defs. Toltec Investigations L.L.C. and Michael Jaczewski's Reply in Supp. of Rule 12(b)(6) Mot. to Dismiss* (ECF No. 185); *DISH Network Corp.'s Reply in Supp. of Its Mot. to Dismiss* (ECF No. 196).

Finally, Plaintiffs filed sur-replies opposing each motion. *Sur-Reply Mot. to Fed. Defs.' Reply Mot. to Pls.' Resp. to*

Fed. Defs.' Mot. to Dismiss, SAC (ECF No. 190) (*Pls.' Sur-Reply*); *Sur-Reply to the Dish Network, LLC and NagraStar, LLC Reply Mot. to Pls.' Resp. to Defs.' Mot. to Dismiss SAC* (ECF No. 182); *Sur-Reply Mot. to the Toltec Investigations L.L.C. and Michael Jaczewski's Reply Mot. to Pls.' Resp. to Their Mot. to Dismiss SAC* (ECF No. 195); *Sur-Reply Mot. to Dish Network Corp.'s Reply Mot. to Pls.' Resp. to Mot. to Dismiss SAC* (ECF No. 199).

II. FACTS [3]

a. The Parties

In 2015 and 2016, Darwin Quinones-Pimentel and Victor Vega-Encarnacion founded Naicom Corporation and D&V IP Holdings, LLC to offer Internet Protocol Television (IPTV) services. The companies are structured such that D&V holds the proprietary "intellectual technology" created by Mr. Quinones, and Naicom licenses the technology from D&V to distribute television programming. *Second Am. Compl.* ¶ 63. Kiaras, LLC and Paylink, LLC are also joint ventures operated by Mr. Quinones and Mr. Vega. *Id.* ¶ 14. Kiaras is a human resources and time-and-attendance management company, and PayLink is a payroll processing company. *Id.* Both Kiaras and PayLink operate on the "PAYLINK AND KIARAS Cloud Network," another proprietary intellectual technology creation of Mr. Quinones. *Id.* ¶¶ 5-6. All four companies are corporations existing under the laws of the

commonwealth of Puerto Rico with their places of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907. *Id.* ¶¶ 33-36.

***3** DISH Network Corporation (DISH Corp.) was organized in 1995 as a corporation under the laws of the State of Nevada, started offering the DISH® branded pay-tv service in March 1996, and is the nation's third largest pay-tv provider. *Id.* ¶ 37. DISH Network LLC (DISH LLC) was organized in 1987 as a Limited Liability Corporation under the laws of the state of Colorado. *Id.* ¶ 38.

NagraStar, LLC is a joint venture between DISH Corp. and Kudelski SA formed in 1998. *Id.* ¶ 39. NagraStar's focus is delivering and maintaining security solutions for satellite and Internet-based television systems and other connectivity initiatives in North America, and their mission also includes anti-piracy investigations and cooperation with law enforcement agencies. *Id.* Jordan Smith was at all relevant times a Manager of Field Security & Investigations and Senior Anti-Piracy Investigator for NagraStar. *Id.* ¶ 41. Bert Eichhorn and Emily Rinkel were Managers of Field Security & Investigations for NagraStar. *Id.* ¶¶ 42-43. Kevin Gedeon was a Manager of Fraud Investigations for NagraStar. *Id.* ¶ 44.

Toltec Investigations, LLC (Toltec) is a private investigative agency specializing in investigating the

technology and distribution involved in IPTV systems, copyrights, patents, and "Trademark and Brand's Intellectual Property." *Id.* ¶ 40. Michael Thomas Jaczewski, a.k.a. Brian Parsons, was at all relevant times President and Chief Executive Officer of Toltec. *Id.* ¶ 45. Rosa Emilia Rodriguez-Velez was at all relevant times the United States Attorney for the District of Puerto Rico. *Id.* ¶ 46. Jose Capo-Iriarte was an Assistant U.S. Attorney (AUSA) and head of the office's Criminal Division. *Id.* ¶ 47. Nicholas Cannon was an AUSA and Deputy Chief of the Cybercrimes Division. *Id.* ¶ 48.

Douglas Leff was at all relevant times Special Agent in Charge of the FBI's San Juan Division. *Id.* ¶ 49. Also in that division, Brad Rex was a Supervisory Special Agent; Lance Lange, Kevin Pearson, and Clay Rehrig were Special Agents; Juan Galarza was a Computer Science Officer; and Jason Lopez was an Evidence Technician. *Id.* ¶¶ 50-55.

b. Naicom's Origins

Between 2002 and 2012, Mr. Quinones developed the intellectual technology, including the source code, underpinning the Paylink and Kiaras Cloud Workforce Management system and Naicom's IPTV services. *Id.* ¶ 5. The proprietary IPTV system was characterized as a Dynamic Internet Semantic Multicast Environment (DISME), which "enabled for the first time the broadcast of media via private networks and the internet, a new

concept of IPTV service to distribute Live-Video Television Content (media) to residences, business, and primes customers." *Id.* ¶¶ 8-11.

By 2016, Mr. Quinones had completed all DISME technology alpha and beta tests and, alongside Mr. Vega, founded Naicom. *Id.* ¶ 12. Naicom is a network and internet communication platform that delivers live television, video on-demand content, internet, and wireless network services to subscribers worldwide. *Id.* Naicom also provides instant access to television shows, movies, and music/videos on-demand, and live sports and music events through Naicom's set-top box using IPTV and TV Everywhere (TVE) on any mobile device. *Id.*

Mr. Quinones and Mr. Vega registered Naicom as a closed corporation with the State Department of Puerto Rico and complied with all requirements as a legitimate IPTV business. *Id.* ¶ 66. Naicom also requested to manufacture its own brand of set-top boxes for end users through Informir LLC and acquired the programing licenses to distribute on-demand content in the United States, Puerto Rico, and the U.S. Virgin Islands through worldwide television network companies. *Id.* ¶¶ 67-68. In 2017, Naicom became a member of the National Rural Telecommunications Cooperative (NRTC). *Id.* ¶ 68.

***4** On January 6, 2017, Naicom submitted a request to the Apple Corporation to have its TV App added to Apple's

AppStore. *Id.* ¶ 69. Apple's legal department requested that Naicom produce all licenses authorizing the distribution of programming to Naicom's subscribers via Naicom's TV App. *Id.* On February 16, 2017, Apple approved Naicom's App for inclusion in the Apple AppStore. *Id.* ¶ 70. In December 2017, Sam's Club approved Naicom to launch and distribute Naicom's IPTV set-top box in their retail stores. *Id.* ¶ 71.

c. Naicom's Information Security

Naicom went to great lengths to protect its intellectual technology. *Id.* ¶¶ 64-65. D&V IP Holdings and Naicom developed significant amounts of confidential and proprietary information, including non-public information relating to the DISME's source codes, patterns, formulas, algorithms, methods, and techniques; the technological vision for Naicom's IPTV content, distribution, marketing, servicing, research and development efforts and strategies; business and marketing performance strategies; financial data and business plans; technical data; customer development management programs; and subcontractor and vendor relationships (collectively, with the DISME, the Confidential Information or Naicom's Confidential Information). *Id.* ¶ 64.

To protect this information, Plaintiffs only installed on their servers, located at Naicom's Data Center Facility, what is known as a compiled executable. *Id.* ¶ 65. The

entire system was installed with an operating system that allowed the hard drive to be encrypted and, to access the servers, an authorized employee would need to enter the secure data facility and provide a username and password. *Id.* The server is not exposed to the internet and could only be accessed from inside the facility. *Id.* The Confidential Information was also downloaded onto a hard disk and kept in a safe box. *Id.*

Plaintiffs took additional steps to safeguard their confidential information and proprietary data, including restricting employee access, requiring employees to execute non-disclosure agreements, imposing restrictions on remote access, and implementing encryption. *Id.* ¶¶ 72-76.

d. Negotiations with Claro Puerto Rico

In 2017, Naicom entered into negotiations with Claro Puerto Rico [4] to distribute Naicom set-top boxes to Claro customers. *Id.* ¶ 77. Claro represented to Naicom that it had approximately 320,000 internet subscribers who received only five megabytes and thus could not subscribe to Claro's IPTV services, which required sixty megabytes to upload programming. *Id.* ¶ 78. During negotiations, Naicom and Claro entered into a mutual non-disclosure agreement prior to discussing and analyzing business information and the contents of the resellers' agreement. *Id.* ¶ 79. Claro's Product Development Officer, Anibal Rios,

projected that the Claro-Naicom business alliance would bring in over $10,000,000 in monthly gross revenue for the first year and over $13,000,000 for the second year, only taking into account Claro's corporate and residential subscribers in Puerto Rico. *Id.* ¶ 80. Naicom projected that the Claro-Naicom alliance would add 100,000 new corporate subscribers, plus another 150,000 residential subscribers, bringing in projected monthly gross sales of $9,000,000 in the first year and $12,000,000 in the second year. *Id.* ¶ 81.

***5** Claro had an existing contract with DISH Network Satellite TV, whereby DISH Network provided TV programming to Claro's internet subscribers who could not subscribe to Claro's IPTV services. *Id.* ¶ 82. The Naicom deal represented a cancellation threat to DISH Network's contract with Claro. *Id.* Claro was also considering shutting down its IPTV business division due to loss of revenue. *Id.* During the negotiations for the Claro-Naicom deal, Carlos Garcia, Claro's IPTV business manager, became privy to information that the Claro-Naicom deal would leave him jobless if Claro opted to shut down its IPTV division, which he managed. *Id.* ¶. 83. Mr. Garcia alerted DISH Network that the Claro-Naicom IPTV deal would lead to cancellation of the DISH contract with Claro, which the Plaintiffs allege led to "great animosity" between DISH Network and Naicom. *Id.* ¶ 84. On August 14, 2018, after a year of meetings between Naicom and Claro, Claro pulled out of negotiations

without notice. *Id.* ¶ 85. Plaintiffs believe the DISH Network Defendants advised Claro to withdraw because the FBI was investigating Naicom and its founders. *Id.* ¶ 86.

e. The DISH Network Investigation

On August 7, 2017, the DISH/NagraStar Defendants and DISH Corp. instructed the Toltec Defendants to purchase two Naicom TV set-top box receivers so that the Defendants [5] could reverse engineer Plaintiffs' intellectual technology. *Id.* ¶ 87. The Defendants conducted "sniffing" to determine the direction of Naicom TV traffic and locate Naicom's facility. *Id.* The defendants also used sniffing to attack and penetrate Naicom's servers and computers, monitoring content and capturing information on the network under the supervision of the Federal Defendants. *Id.* One of the two set-top box receivers was maintained by the DISH/NagraStar Defendants, the other by the Toltec Defendants. *Id.* ¶ 88. Both receivers were used for the attacks on Naicom's data center servers. *Id.*

Mr. Jaczewski purchased the two set-top boxes from Naicom under the false name of "Brian Parsons," and he provided false contact information. *Id.* ¶ 89. According to the Defendants, their investigation revealed that the receiver provided access to approximately forty-three channels, including Disney, TBS, ESPN, CNN, HBO,

Showtime, and Cinemax. *Id.* ¶ 90. The Defendants downloaded the Naicom TV App through the Apple AppStore, which provided access to approximately forty-two channels, and tested Naicom TV several times to determine whether it was providing DISH programming. *Id.* The tests revealed no DISH content. *Id.*

The Defendants also contacted several media companies to inquire into whether Naicom had the appropriate licensing contracts to distribute its programming. *Id.* ¶ 91. On each occasion, the investigators were informed that Naicom was authorized to distribute the network's content. *Id.* The investigators also discovered that Naicom's TV distribution technology was a threat to DISH Network and Sling TV, representing future competition for subscribers in Puerto Rico and the United States. *Id.* ¶ 92.

The DISH/NagraStar Defendants informed the other Defendants that they could not penetrate Naicom's Data Center computers and servers remotely, and thus direct, physical access would be required to extract Naicom's intellectual property. *Id.* ¶ 93. They knew that by entering the data center and shutting down the computers and servers, they would be able to bypass Naicom's security measures and access the internal hard drive. *Id.* ¶ 94.

According to Naicom, the Defendants knew that the intellectual property was extremely valuable and worth

obtaining by any means necessary to advance their own television programming distribution system, and the Defendants conspired to misappropriate the technology for economic advantage. *Id.* ¶ 95.

***6** The DISH/NagraStar Defendants thereafter filed a complaint with the Federal Defendants alleging that Naicom was running an IPTV pirate operation. *Id.* ¶ 98. Plaintiffs allege that the motive behind the complaint was to secure NagraStar and DISH Network's participation in a search of Naicom's Data Center and the seizure of Naicom's computers, servers, and other hardware containing Naicom's intellectual property and trade secrets, under the ruse of assisting the Federal Defendants in discovering incriminating evidence. *Id.* Acquiring this information has given the DISH/NagraStar Defendants a competitive advantage over Naicom. *Id.* ¶ 99.

f. Execution of the Search Warrants

1. The First Search of Naicom's Data Center

On August 27, 2019, the Federal Defendants applied for two search warrants: one for Naicom Corporation located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907, and the other for Naicom's Data Center located at Villa Fontana, 4SS N2 Via Josefina, Carolina, Puerto Rico. *Id.* ¶¶ 19, 33, 105.

Plaintiffs allege that the search warrants were "issued under illegal and unlawful means" because the Federal Defendants provided affidavits they knew to contain false and perjured information. *Id.* ¶ 20.

On August 27, 2019, the Federal and DISH/NagraStar Defendants executed the warrants, with the DISH/NagraStar Defendants "acting as federal agents." *Id.* ¶ 21. They seized documents, hard drives, and thumb drives, and downloaded data from the computers and servers containing Plaintiffs' Confidential Information. *Id.* Plaintiffs allege that the Defendants knew from their investigation prior to the searches that Naicom was authorized to distribute its programming and was not pirating content. *Id.* ¶ 101. The Defendants also allegedly knew that the evidence collected in the Federal Defendants' investigative files "negated any criminal wrongdoing that Naicom's founders were committing the crimes charged in the search and seizure warrant affidavit and application." *Id.* ¶ 102.

At the conclusion of the August 27, 2019 search, the Federal Defendants "learned that Naicom TV counted with all the programming distribution contract and agreements" [6] and instructed Mr. Quinones and Mr. Vega to report to the FBI offices with their licensing contracts for an interview. *Id.* ¶ 103. This interview took place with the Federal Defendants sitting at one table and the DISH/NagraStar Defendants sitting at another table,

allegedly posing as federal agents. *Id.* ¶ 104. The Defendants questioned Mr. Quinones about how Naicom acquired the IPTV distribution contracts and the technology used to distribute the programing. *Id.* They also inspected Naicom's contracts with content providers, which contained trade/business secrets and confidential information regarding DISME technology. *Id.*

2. The Second Search of Naicom's Data Center

On August 29, 2019, U.S. Attorney Rodriguez-Velez and AUSAs Capo-Iriarte and Cannon instructed FBI Agents Lange and Pearson to return to Naicom's data center with DISH/NagraStar Defendants Smith, Gedeon, and Eichhorn. *Id.* ¶ 105. Naicom alleges that the USAO Defendants ordered this search despite knowing beforehand that Naicom was a legitimate business and there was no probable cause for continued investigation. *Id.* Without obtaining new warrants, the Defendants again entered Naicom's Data Center, performed password resets, and installed "pen drives and other electronic instruments" to bypass security measures and download and seize Naicom's Confidential Information. *Id.* ¶¶ 22, 106. The agents used keys taken from Naicom's offices to enter Naicom's Data Center. *Id.* ¶ 105.

***7** During the search, Agent Pearson contacted Naicom employee Jaime Echevarria and ordered him to come to the Data Center, as Agent Pearson wanted to speak with

him, Mr. Quinones, and Mr. Vega. *Id.* ¶ 107. Upon arriving at the Data Center, Mr. Quinones observed Agents Lange and Pearson allowing Mr. Smith, Mr. Gedeon,and Mr. Eichhorn to access Naicom's Data Center computers, servers, and other hardware equipment without authorization from Naicom. *Id.* ¶ 108.

During the search, Agents Pearson and Lange pressured Mr. Quinones to sign a hold-harmless document accepting that he had run a pirate operation in the past so that they could close the case. *Id.* ¶ 109. Otherwise, they threatened that they would shut down the Data Center operation. *Id.* Mr. Quinones refused, despite Agents Pearson and Lange imploring him to sign the document. *Id.* ¶ 110.

Sometime thereafter, Mr. Vega arrived and, upon entering the Data Center, asked Agents Pearson and Lange if they had another search warrant to enter and search the Data Center. *Id.* ¶ 111. Agent Lange represented to Mr. Vega that the search warrants gave him ten days to come in and out and search the Data Center. *Id.* Mr. Vega told Agent Lange that Agent Lange was violating the United States Constitution and federal law. *Id.*

Mr. Vega thereafter informed Agents Pearson and Lange that he had discovered via LinkedIn that the alleged FBI experts who executed the search and interrogated Mr. Quinones and him at the FBI offices were Kevin Gedeon,

investigator for DISH Network, and Jordan Smith, Bert Eichhorn, and Emily Rinkel, investigators for NagraStar. *Id.* ¶ 112. Mr. Vega questioned Agents Lange and Pearson as to why the FBI brought in his competition to search, inspect, and photograph private documents and allowed them access to computers and servers containing trade secrets, code sources, and business and intellectual property belonging to Naicom. *Id.* ¶ 113. Mr. Vega called his attorney and told him about the second search. *Id.* ¶ 114. After speaking with Agent Lange, the FBI agents and DISH/NagraStar investigators shut down Naicom's business operation and left the premises. *Id.*

g. The Demand for the Return of Property Under Rule 41(g)

On September 6, 2019, Plaintiffs filed a motion to demand the return of seized property under Rule 41(g) of the Federal Rules of Criminal Procedure. *Id.* ¶ 115. The District Court granted Plaintiffs' Rule 41(g) motion on November 5, 2019, noting that the Government had waived objections to the court's Report & Recommendation. *Id.* ¶¶ 116-17.

h. Plaintiffs' Alleged Harms

Plaintiffs allege that the criminal investigation caused significant damage to their business reputation and unfairly enriched their competitors. *Id.* ¶¶ 118-19. They

allege that prior to the execution of the search warrants, they had a great reputation and were about to close on a $15,000,000 investment deal, but investors pulled out upon learning Naicom was under criminal investigation. *Id.* ¶¶ 120-21. Plaintiffs also allege that Naicom was about to close a multimillion-dollar deal with Claro when Claro learned of the FBI's investigation and pulled out of negotiations. *Id.* ¶ 122. Plaintiffs say they have lost subscribers because of negative publicity resulting from the investigation and that the Defendants' intrusion into Naicom's Data Center computers, servers, and equipment caused damage leaving subscribers without TV programming services for several weeks and costing more than
$500,000 to repair. *Id.* ¶ 123.

i. Plaintiffs' Causes of Action

***8** Plaintiffs bring seven counts. Count One alleges that the Defendants violated RICO by forming an association in fact to advance the criminal objective of stealing Plaintiffs' intellectual property and trade secrets by committing mail and wire fraud, among other crimes. *Id.* ¶¶ 124-53.

Count Two alleges that the Defendants engaged in a RICO conspiracy by conspiring to plan and execute the scheme outlined in Count One. *Id.* ¶¶ 154-57.

Count Three alleges that the Defendants violated the

CFAA by accessing Naicom's computer systems without authorization or in excess of authorization and obtaining and using valuable information from those computers. *Id.* ¶¶ 158-68.

Count Four alleges that the Defendants violated the SCA by "willfully and intentionally access[ing] without authorization a facility which operates servers, encoders, computers, and telecommunications systems and technology, by electronically transmitting communications involved in Webservers, Email-Servers, Carrier Grade Routers which interconnected with local ISP providers through Border Gateway Protocols (BGP) in exchanging routing information between autonomous systems." *Id.* ¶¶ 169-75.

Count Five alleges that the Defendants violated the DMCA by illegally obtaining Plaintiffs' copyright-protected software programs, documents, confidential information, and research. *Id.* ¶¶ 176-84.

Count Six alleges that the Defendants violated the DTSA by stealing Plaintiffs' trade secrets, including DISME technology, intellectual property, and other confidential information. *Id.* ¶¶ 185-94.

Finally, Count Seven alleges that the Defendants misappropriated Plaintiffs' trade secrets in violation of the PTSA. *Id.* ¶¶ 195-202.

III. THE PARTIES' POSITIONS

a. The Federal Defendants' Motion to Dismiss

The Federal Defendants move to dismiss all counts of the Second Amended Complaint. *Defs.' Mot.* at 1-39.

The Federal Defendants begin by arguing that the individual capacity statutory claims should be dismissed for failure to state a claim on which relief may be granted because qualified immunity shields federal employees from individual capacity damages suits unless they violate clearly established constitutional or statutory rights. *Id.* at 8. They contend that because, in their view, Plaintiffs fail to allege any statutory violations, qualified immunity bars suit. *Id.* The Federal Defendants submit that "[o]nce the conclusory and speculative allegations and threadbare recital of elements of a cause of action are set aside, it is apparent that the plaintiffs' lengthy complaint cannot support any of the claims it advances against the Federal Defendants." *Id.* at 9. They add that "[t]he plaintiffs similarly fail to specify the particular conduct of each Federal Defendant that supposedly forms the basis for liability. Instead, the complaint alleges collective legal wrongs," which "is especially improper when the defendants are public officials." *Id.* at 10.

Turning to the statutory claims, the Federal Defendants

assert that "plaintiffs rely on broad, conclusory, allegations of wrongdoing that fail to establish any of the four requisite elements of a civil RICO claim." *Id.* at 11. In their view, Plaintiffs do not plausibly allege that the Federal Defendants joined with other Defendants to form an enterprise and directed the operations of the purported enterprise, the alleged pattern of racketeering activity is deficient, and the limited breadth, duration, and purpose of the supposed racketeering activity do not establish the pattern required to sustain a RICO claim. *Id.*

***9** The Federal Defendants submit that the Second Amended Complaint "lacks well-pleaded allegations showing that the Federal Defendants participated in any association-in-fact 'enterprise.' " *Id.* at 13. Furthermore, they contend that "plaintiffs also do not distinguish the alleged enterprise from their allegations of racketeering activity as RICO requires." *Id.* at 14. Specifically, the complaint "supposes an enterprise that exists exclusively to obtain the plaintiffs' confidential information" and "[b]y conceiving an enterprise in such narrow terms, the plaintiffs fail to plausibly allege a RICO enterprise." *Id.*

The Federal Defendants also assert that "[t]he plaintiffs make no allegations sufficient to connect the Federal Defendants to the conduct of the supposed enterprise's affairs" and thus "the complaint does not plausibly allege that the Federal Defendants were conducting the affairs of some association-in-fact enterprise with the other

defendants instead of their own federal agencies' official business." *Id.* at 14-15. They add that "[t]he plaintiffs' allegations are all the more implausible given an obvious alternative explanation for the searches, namely that the Federal Defendants pursued a lawful criminal investigation." *Id.* at 15 (citation and internal quotation marks omitted). Ultimately, they offer that "the RICO claims against each Federal Defendant fail both for want of an 'enterprise' and lack of plausible allegations that any particular Federal Defendant participated in the posited enterprise." *Id.* at 16.

Next, the Federal Defendants argue that "Plaintiffs fail to plausibly allege that the Federal Defendants engaged in a pattern of racketeering activity." *Id.* at 17. They submit that "[t]he plaintiffs' RICO theory here relies for its predicate acts on supposed mail and wire fraud, and allegations of misappropriation of trade secrets" but "the plaintiffs cannot plausibly allege the Federal Defendants committed the supposed predicate offenses based on the FBI's execution of a search warrant at Naicom's San Juan office and its data center." *Id.* at 17-18. Additionally, they offer that "[b]eyond failing to coherently allege the minimum predicate acts, the plaintiffs fail to 'allege facts linking each [Federal] defendant to the grounds on which that particular defendant is potentially liable' for the supposed pattern of racketeering activity." *Id.* at 19 (alteration in original) (quoting *Redondo Waste Sys. v. López-Freytes*, 659 F.3d 136, 140 (1st Cir. 2011)).

The Federal Defendants' final argument against the RICO claim is that the alleged scheme lacks the requisite continuity because Plaintiffs "allege a narrow scheme directed exclusively at the acquisition of their intellectual property and trade secrets" and "[t]he allegations here describe no risk of the alleged activity continuing." *Id.* at 20.

Briefly addressing the RICO conspiracy claim, the Federal Defendants claim that the Plaintiffs' failure to plead a substantive RICO claim inherently defeats the conspiracy claim. *Id.* at 20-21.

Next, the Federal Defendants address the CFAA claim, contending that it fails as a matter of law "because the CFAA does not prohibit lawfully-authorized investigative activity of federal law enforcement agencies" and "the government had a warrant to search the plaintiffs' computers." *Id.* at 21. Moreover, they submit that "[t]he Federal Defendants also did not 'access' the plaintiffs' computers, and the plaintiffs do not allege a compensable loss or damage caused by the Federal Defendant's actions." *Id.*

Regarding the SCA claim, the Federal Defendants argue that electronic materials accessed during the raids were not "electronic communications" as defined and protected by the Act. *Id.* at 26-28. They submit further that none of

the Federal Defendants accessed Plaintiffs' computers, the Federal Defendants lacked the requisite state of mind for liability under the SCA and, in any event, the SCA provides that good faith reliance on a warrant is a complete defense. *Id.* at 28-30.

***10** The Federal Defendants stake out similar positions on the DMCA claim, contending that if anyone engaged in copyright circumvention it was the DISH/NagraStar Defendants alone and, regardless, the statute protects authorized law enforcement activity. *Id.* at 30-32.

Regarding the DTSA claim, the Federal Defendants assert that Plaintiffs have failed to adequately plead the existence of a trade secret and—again—the statute protects authorized law enforcement activity. *Id.* at 32-35.

The Federal Defendants then pivot back to immunity, contending that the Westfall Act provides for absolute immunity for all Federal Defendants on the PTSA claim, and absolute prosecutorial immunity shields the USAO Defendants for their prosecutorial acts. *Id.* at 35. They submit that the Westfall Act provides that tort claims against federal employees acting in the scope of their employment must be brought under the Federal Tort Claims Act (FTCA), which mandates the immediate substitution of the United States as the defendant. *Id.* at 35-36. The Federal Defendants argue that the United States must be substituted as defendant and the claim

must then be dismissed because Plaintiffs have not complied with the FTCA's procedural requirements. *Id.* at 36.

Finally, regarding prosecutorial immunity, the Federal Defendants submit that the USAO Defendants are absolutely immune from suit because their conduct was "intimately associated with the judicial phase of the criminal process." *Id.* at 37 (quoting *Imbler v. Pachtman*, 424 U.S. 409, 430, 96 S.Ct. 984, 47 L.Ed.2d 128 (1976)).

b. Plaintiffs' Opposition

Plaintiffs oppose the Federal Defendants' motion by first insisting that the "individual capacity statutory claims state a claim upon which relief could be granted, therefore, the Federal Defendants are not entitled to qualified immunity from Plaintiffs' RICO claims." *Pls.' Opp'n* at 10. They submit that the Second Amended Complaint alleges against the Federal Defendants "criminal and civil violations [that] were clearly established and prohibited at the time they committed the crime" and thus they are not entitled to qualified immunity. *Id.* at 12-13.

Plaintiffs further acknowledge that the Attorney General's designee has certified, pursuant to the Westfall Act, that the Federal Defendants were acting within the scope of their employments. *Id.* They assert, however, that

the Federal Defendants did not act within the scope of their official duties and that if the Court agrees it must re-substitute the Federal Defendants. *Id.* at 68-69. Similarly, Plaintiffs contend that the USAO Defendants are not entitled to absolute prosecutorial immunity because their conduct "violated clear and established criminal and civil laws" and was not in furtherance of their protected prosecutorial duties. [7] *Id.* at 71-73.

***11** Turning to the RICO counts, Plaintiffs submit that they have pleaded "a colorable RICO claim on the facts" because "they have plead[ed] enough facts in the [Second Amended Complaint] giving defendants a fair notice of what there is, and the grounds upon which they rest." *Id.* at 16-17. They add that they also "have pleaded a colorable RICO enterprise on the facts." *Id.* at 18-20.

Plaintiffs further contend that they have sufficiently pleaded "conduct of a criminal enterprise that is separate and apart from the conduct of defendants' own affairs." *Id.* at 20. In their view, the three required elements for establishing a RICO enterprise are: (1) "an ongoing organization, formal or informal," (2) that "the various associate[s] function as a continuing unit," and (3) that the enterprise exists "separate and apart from the pattern of activity in which it engages." *Id.* at 21 (quoting *United States v. Turkette*, 452 U.S. 576, 583, 101 S.Ct. 2524, 69 L.Ed.2d 246 (1981)). Plaintiffs assert, however, that while they "will ultimately need to establish each of these

factors, at this early juncture it is sufficient to merely [ ] allege the existence of an association-in-fact enterprise." *Id.* (citing *Pappa v. Unum Life Ins. Co. of Am.*, No. 3:07-cv-0708, 2008 WL 744820, at *——— – ———, 2008 U.S. Dist. LEXIS 21500 at *29-30 (M.D. Pa. Mar. 18, 2008)). They add that it is reasonable to infer from the complaint that "the Association in Fact defendants comprised by the Federal and Dish/Nagrastar defendants, functioned as a continuing unit and had an ascertainable structure distinct from that inherent in the conduct of a pattern of racketeering activity." *Id.* at 22.

Plaintiffs argue that they have established a pattern of racketeering activity because they have "pleaded that the Association in Fact defendants committed over 30 racketeering acts ranging from Mail and Wire fraud to theft of trade secrets, in a period of two years which began in July 2017 and ended in August 2019." *Id.* at 25. In their view, "[t]hese facts satisfied the closed period of repeated conduct" and there are also "allegations of a threat of continued activity, in reference to the Dish Network and Nagrastar corporation joint venture." *Id.* at 25-26. Plaintiffs submit further that they have pleaded a viable RICO conspiracy claim and that—contrary to the Federal Defendants' assertions—pleading an actionable substantive RICO claim is not a prerequisite for a RICO conspiracy claim. *Id.* at 27-29.

Plaintiffs next turn to their CFAA claim, beginning by

addressing the Federal Defendants' position that any computer intrusions were protected lawfully authorized investigative activity. *Id.* at 30. Plaintiffs rejoin that the Defendants' conduct is not covered by this exception because "the procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Id.* They contend that the "search warrant contained materially false representations and perjured testimony" and ultimately lacked probable cause. *Id.* at 31. Plaintiffs submit further that the "alleged initial probable cause dissipated with the first search warrant execution" and thus the second search was "illegal and warrantless." *Id.* at 35.

Plaintiffs go on to argue that the "affidavit in support of the search warrant was defective on its face." *Id.* at 36. They contend that their computer systems were protected under the SCA, the Federal Defendants' "conclusory" statements were insufficient to justify a search, and the search ultimately did not comply with the SCA. *Id.* at 37-38. According to Plaintiffs, the Federal Defendants did not "seek authorization from the Magistrate to bring Plaintiffs' competitors, the Dish/Nagrastar defendants, to execute the search warrant," and although Plaintiffs concede that 18 U.S.C. § 3105 "allowed the aid of private parties," they rejoin that "the statute clearly prohibited the executing officer from bringing to the search a party which had another interest, profit, or other marketplace

incentive." *Id.* at 41. Plaintiffs submit further that "the Federal defendants cannot raise at this stage a legal defense which the Federal defendants abandoned when they did not oppose the Motion for Return of Property under Rule 41(g) proceedings." *Id.* at 43.

***12** After concluding that the searches were generally unlawful, Plaintiffs return to the specifics of their CFAA claim. They offer that they have established each element of a CFAA violation and—contrary to the Federal Defendants' assertions—the fact that only the DISH/NagraStar Defendants actually intruded on Plaintiffs' computer systems is irrelevant because the Federal Defendants are responsible "under a conspiratorial theory of liability." *Id.* at 45-51.

Plaintiffs make similar arguments in support of their remaining claims. For the SCA claim, they submit that they have established each element of a SCA violation and reiterate that the search was not legally authorized. *Id.* at 52-60. In support of their DMCA claim, they "submit that for the same factual and legal reasons argued above, the Federal defendants also violated the Digital Millennium Copyright Act." *Id.* at 61. Plaintiffs again assert that the searches were not legally authorized and the Federal Defendants are liable for the DISH/NagraStar Defendants' conduct during the searches. *Id.* at 60-61.

Finally, turning to their trade secrets claims, Plaintiffs

reiterate once more that the searches were not legally authorized and submit that the complaint adequately describes the trade secrets allegedly misappropriated by the Defendants. *Id.* at 62-66. Plaintiffs conclude by asking the Court to deny the Federal Defendants' Motion to Dismiss in its entirety. *Id.* at 74.

c. The Federal Defendants' Reply

In reply, the Federal Defendants offer that "plaintiffs base their claims on allegations that are conclusory, collective, and speculative" and "[f]or that reason, and because the Federal Defendants are shielded by both absolute and qualified immunity, the Second Amended Complaint fails to state claims on which relief may be granted." *Defs.' Reply* at 1.

The Federal Defendants begin by comparing Plaintiffs' suit to *Ashcroft v. Iqbal*, 556 U.S. 662, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009), and *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007), and asserting that the "complaint relies on conclusory allegations to support the claims of wrongdoing, and none of its allegations plausibly support the inferences needed to sustain the plaintiffs' various statutory claims." *Id.* at 2-4.

They next contend that "[t]he plaintiffs are also incorrect that 'at this early juncture it is sufficient to merely allege

the existence of an association-in-fact enterprise' to support their RICO claim." *Id.* at 5 (quoting *Pls.' Opp'n* at 21). The Federal Defendants add further that Plaintiffs have not plausibly alleged the existence of an association in fact, "that any of the Federal Defendants adopted and acted with the purpose of stealing their intellectual property," or "what benefit they gained from doing so." *Id.* at 5-6. Nor, in their view, do Plaintiffs "explain how the supposed association-in-fact enterprise functioned as a continuous unit." *Id.* at 7. Moreover, the Federal Defendants contend that "[t]he plaintiffs also fail to address the Federal Defendants' lack of control over the alleged enterprise or participation in either its operation or management." *Id.*

Turning to the alleged pattern of racketeering activity, the Federal Defendants assert that Plaintiffs' response "is silent as to the predicate act allegations not complying with Rule 8 or Rule 9 pleading standards or describing adequately the Federal Defendants' involvement in Dish Network's supposed trade secret theft scheme." *Id.* at 8-9. In response to Plaintiffs' contention that an actionable substantive RICO claim is not a prerequisite for a RICO conspiracy claim, they rejoin that "First Circuit precedent clearly holds otherwise." *Id.* at 10 (citing *Efron v. Embassy Suites (P.R.), Inc.*, 223 F.3d 12, 21 (1st Cir. 2000)).

***13** The Federal Defendants go on to argue that "Plaintiffs fail to overcome the search warrants' validity,"

characterizing Plaintiffs' allegations of perjury as conclusory and contending that they have failed to rebut key evidence supporting the search warrants. *Id.* at 10-14. The Federal Defendants add that their willingness to later return the seized property does not imply the invalidity of the search warrants or any other Fourth Amendment violation. *Id.* at 14-16.

For the remainder of Plaintiffs' claims, the Federal Defendants reject Plaintiffs' contentions that the searches were not legally authorized. *Id.* at 16-21. Regarding the CFAA claim, they submit that "plaintiffs' CFAA conspiracy claim suffers from the same pleading deficiencies as does the RICO conspiracy claim." *Id.* at 16. For the SCA claim, they offer that Plaintiffs' opposition "confuse[s] an SCA disclosure order with the traditional search warrant under the Federal Rules of Criminal Procedure that the government, in fact, used to search the plaintiffs' offices and that was the subject of the plaintiffs' Rule 41(g) proceedings." *Id.* at 18. Furthermore, they assert that "the government appropriately opted for a traditional search warrant in this case because it sought to seize evidence of the plaintiffs' piracy operation rather than to require the plaintiffs to disclose certain electronic communications." *Id.*

On the DMCA claim, the Federal Defendants reiterate that it must fail because "[t]he Second Amended Complaint's allegations do not attribute circumvention

conduct directly to any Federal Defendant. Nor do the Plaintiffs' allegations overcome the statute's broad law enforcement exception." *Id.* at 19. Similarly, they contend that the DTSA claim should be dismissed because "the plaintiffs rely on broad assertions that simply recite the elements of a DTSA claim, and because they do not address the statutory exemption applicable to the Federal Defendants' law enforcement actions in this matter." *Id.* at 20-21.

Finally, the Federal Defendants reject Plaintiffs' Westfall Act argument, asserting that they are protected because they acted within the scope of their employment and "[w]hether an employee acted in the scope of office or employment does not depend on whether his or her alleged actions can be characterized as tortious or even criminal." *Id.* at 21-23. Likewise, they reiterate that the USAO defendants are entitled to absolute prosecutorial immunity. *Id.* at 23-24.

d. Plaintiffs' Sur-Reply

In their sur-reply, Plaintiffs contend that: the Federal Defendants' Reply did not contribute anything not already discussed in their motion to dismiss; Plaintiffs have met or exceeded the required pleading standard for each claim; and, the Federal Defendants have forfeited any "Fourth Amendment issue" relating to the search warrants or searches. *Pls. Sur-Reply* at 1-13.

IV. LEGAL STANDARD

Federal Rule of Civil Procedure 12(b)(6) requires dismissal of a complaint that "fail[s] to state a claim upon which relief can be granted." FED. R. CIV. P. 12(b)(6). To state a claim, a complaint must contain, among other things, "a short and plain statement of the claim showing that the pleader is entitled to relief." FED. R. CIV. P. 8(a)(2). In other words, a complaint must contain "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937 (quoting *Twombly*, 550 U.S. at 570, 127 S.Ct. 1955). A claim is facially plausible when "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly*, 550 U.S. at 556, 127 S.Ct. 1955). Plausible means " 'something more than merely possible' or 'merely consistent with a defendant's liability.' " *Germanowski v. Harris*, 854 F.3d 68, 71-72 (1st Cir. 2017) (internal citation omitted) (quoting *Schatz v. Republican State Leadership Comm.*, 669 F.3d 50, 55 (1st Cir. 2012)); *Ocasio-Hernández v. Fortuño-Burset*, 640 F.3d 1, 11 (1st Cir. 2011). This is a " 'context-specific' job that compels [judges] 'to draw on' [their] 'judicial experience and common sense.' " *Schatz*, 669 F.3d at 55 (quoting *Iqbal*, 556 U.S. at 679, 129 S.Ct. 1937).

***14** This is a "two-step analysis." *Cardigan Mountain Sch. v. N.H. Ins. Co.*, 787 F.3d 82, 84 (1st Cir. 2015). "First,

the court must distinguish 'the complaint's factual allegations (which must be accepted as true) from its conclusory legal allegations (which need not be credited).' " *García-Catalán v. United States*, 734 F.3d 100, 103 (1st Cir. 2013) (quoting *Morales-Cruz v. Univ. of P.R.*, 676 F.3d 220, 224 (1st Cir. 2012)); *see also Schatz*, 669 F.3d at 55 (stating that a court may "isolate and ignore statements in the complaint that simply offer legal labels and conclusions or merely rehash cause-of-action elements"). "Second, the court must determine whether the factual allegations are sufficient to support 'the reasonable inference that the defendant is liable for the misconduct alleged.' " *García-Catalán*, 734 F.3d at 103 (quoting *Haley v. City of Boston*, 657 F.3d 39, 46 (1st Cir. 2011)).

In ruling on a motion to dismiss, a court may properly take into account four types of documents outside the complaint without converting the motion into one for summary judgment: (1) documents of undisputed authenticity; (2) documents that are "official public records"; (3) documents that are "central" to a plaintiff's claim; and (4) documents that are sufficiently referenced in the complaint. *Watterson v. Page*, 987 F.2d 1, 3 (1st Cir. 1993). Here, the Second Amended Complaint refers to applications for search warrants. *See, e.g.*, *Second Am. Compl.* ¶¶ 18-21. The parties have not placed before the Court the search warrants themselves or the orders approving the warrants, but in ruling on this motion to dismiss, the Court has considered the parties'

unchallenged characterizations of the timing and content of those warrants.

V. DISCUSSION

a. Absolute Prosecutorial Immunity

As a threshold matter, the Court evaluates the Federal Defendants' claim that the USAO Defendants are entitled to absolute prosecutorial immunity.

1. Caselaw

Immunity is "defined by the functions it protects and serves, not by the person to whom it attaches." *Acevedo-Garcia v. Vera-Monroig*, 204 F.3d 1, 8 (1st Cir. 2000) (internal quotation omitted). "[T]he official seeking absolute immunity bears the burden of showing that such immunity is justified for the function in question." *Burns v. Reed*, 500 U.S. 478, 486, 111 S.Ct. 1934, 114 L.Ed.2d 547 (1991). There is a "presumption ... that qualified rather than absolute immunity is sufficient to protect government officials in the exercise of their duties." *Id.* at 486-87, 111 S.Ct. 1934. Prosecutors are absolutely immune from suit for monetary damages under § 1983 for conduct that is "intimately associated with the judicial phase of the criminal process." *Imbler v. Pachtman*, 424 U.S. 409, 430-31, 96 S.Ct. 984, 47 L.Ed.2d 128 (1976).

In *Buckley v. Fitzsimmons,* the Supreme Court reiterated the view expressed in *Burns* that absolute immunity does not extend to all actions by a prosecutor. 509 U.S. 259, 273, 113 S.Ct. 2606, 125 L.Ed.2d 209 (1993) (citing *Burns*, 500 U.S. at 494-96, 111 S.Ct. 1934). The *Buckley* Court refused to accord absolute immunity to "[a] prosecutor's administrative duties and those investigatory functions that do not relate to an advocate's preparation for the initiation of a prosecution or for judicial proceedings." *Id.* The Supreme Court further observed that in *Imbler* it "did not attempt to describe the line between a prosecutor's acts in preparing for those functions, some of which would be absolutely immune, and his acts of investigation or 'administration,' which would not." *Id.* at 270, 113 S.Ct. 2606.

The caselaw provides examples of conduct that is and is not absolutely immune. In *Burns*, the Supreme Court concluded that prosecutors are not entitled to absolute immunity for the advice they give to the police, but they are entitled to absolute immunity for participating in a probable cause hearing. 500 U.S. at 489-96, 111 S.Ct. 1934. In *Buckley*, the Supreme Court rejected the petitioner's argument that absolute immunity extended "only to the act of initiation itself and to conduct occurring in the courtroom." 509 U.S. at 272, 113 S.Ct. 2606. It restated *Imbler*'s conclusion that absolute immunity includes "actions preliminary to the initiation of a prosecution and actions apart from the courtroom." *Id.*

(quoting *Imbler*, 424 U.S. at 431 n.33, 96 S.Ct. 984). The *Buckley* Court distinguished between actions a prosecutor takes as an advocate, ranging from evaluating evidence for prosecution to the prosecution itself, and actions a prosecutor takes as an investigator, such as "searching for the clues and corroboration" or planning and executing "a raid on a suspected weapons cache." *Id.* at 273-74, 113 S.Ct. 2606. Summarizing its prior caselaw, the *Buckley* Court also clarified that "appearing before a judge and presenting evidence in support of a motion for a search warrant involved the prosecutor's 'role as advocate for the State,' " *id.* at 271, 113 S.Ct. 2606 (quoting *Burns*, 500 U.S. at 491, 111 S.Ct. 1934), and that "issuance of a search warrant is a judicial act ... 'intimately associated with the judicial phase of the criminal process.' " *Id.* at 271, 113 S.Ct. 2606 (quoting *Burns*, 500 U.S. at 492, 111 S.Ct. 1934).

2. Analysis

***15** The Federal Defendants submit that the USAO Defendants are entitled to absolute immunity because they were acting as advocates when they submitted the search warrant applications, and Plaintiffs have not alleged that they acted as affiants in support of the warrants or participated in their executions. *Defs.' Mot.* at 37. Plaintiffs respond that the USAO Defendants' role in facilitating the searches was limited to administrative duties or other investigative functions not entitled to

immunity. *Pls.' Opp'n* at 71-73. The Federal Defendants have the better argument.

Plaintiffs' response focuses on the USAO Defendants' role in using their authority to obtain purportedly unlawful search warrants as part of a "hoax criminal investigation" despite being aware that the applications "contained information known to be false and perjured." *Id.* at 71-72 (quoting *Second Am. Compl.* ¶¶ 18, 20). First, Plaintiffs' allegations of prosecutorial misconduct are wholly conclusory. Regarding the search warrants, they allege broadly that "[t]he search warrant order was issued under illegal and unlawful means in that the Federal defendants used the Legal Entity Enterprises' power to have the judiciary authorize the search and seizure warrants through the use of affidavits they knew contained material information known to be false and perjured to create probable cause to gain legal access into Plaintiffs' private business in violation [of] the United States criminal laws." *Second Am Compl.* ¶ 20. Aside from their general claims that every defendant was involved from the beginning in virtually every aspect of a conspiracy to defraud them despite knowing that Naicom was a legitimate business, Plaintiffs do not allege which of the USAO Defendants—U.S. Attorney Rodriguez-Velez, AUSA Capo-Iriarte, and AUSA Cannon—were involved in the preparation and submission of the search warrant application, or how they falsified it.

There is no suggestion of why the USAO Defendants would agree to lead a criminal conspiracy to defraud Plaintiffs or how they came together with the numerous other defendants to organize the conspiracy. The possibility that the federal prosecutors believed that Naicom may have been engaged in illegal piracy presents an "obvious alternative explanation" for the USAO Defendants' conduct. *Iqbal*, 556 U.S. at 682, 129 S.Ct. 1937. Moreover, even if the warrant applications contained false or perjured information, Plaintiffs do not allege that the USAO Defendants acted as affiants providing this information, and it would be equally plausible that the USAO Defendants were relying in good faith on bad information submitted by the private companies and/or FBI Defendants. [8]

Regardless, even if the Court were to find that Plaintiffs had sufficiently pleaded the USAO Defendants' involvement in submitting search warrant applications containing false information, the USAO Defendants would still be entitled to prosecutorial immunity. The *Buckley* Court outlined how absolute immunity attaches to actions taken in a prosecutor's role as an advocate, including "actions preliminary to the initiation of a prosecution and actions apart from the courtroom." 509 U.S. at 272, 113 S.Ct. 2606 (quoting *Imbler*, 424 U.S. at 431 n.33, 96 S.Ct. 984). In doing so, it noted that "appearing before a judge and presenting evidence in support of a motion for a search warrant involved the prosecutor's 'role as advocate for the

State,' " *id.* at 271, 113 S.Ct. 2606 (quoting *Burns*, 500 U.S. at 491, 111 S.Ct. 1934), and that "issuance of a search warrant is a judicial act ... 'intimately associated with the judicial phase of the criminal process.' " *Id.* at 271, 113 S.Ct. 2606 (quoting *Burns*, 500 U.S. at 492, 111 S.Ct. 1934). The First Circuit has since further clarified that protected functions include:

***16** "appearing before a judge and presenting evidence in support of a motion for a search warrant," *Burns*, 500 U.S. at 491, 111 S.Ct. 1934, and "prepar[ing] and filing ... [a criminal] information and [a] motion for an arrest warrant," *Kalina v. Fletcher*, 522 U.S. 118, 129, 118 S.Ct. 502, 139 L.Ed.2d 471 (1997). The basic "principle" of these cases is "that acts undertaken by a prosecutor in preparing for the initiation of judicial proceedings or for trial, and which occur in the course of his role as an advocate for the State, are entitled to the protections of absolute immunity." *Buckley*, 509 U.S. at 273, 113 S.Ct. 2606. *Penate v. Kaczmarek*, 928 F.3d 128, 136 (1st Cir. 2019) (alterations in original).

Plaintiffs have not alleged that the USAO Defendants falsified the affidavits themselves, served as supporting witnesses, or participated in the execution of the search warrants. Thus, even if Plaintiffs had properly pleaded that each USAO Defendant participated in the warrant application process, the USAO Defendants would still be entitled to absolute prosecutorial immunity for conduct

undertaken in their roles as advocates. *See Omran v. United States*, No. 1:14-cv-00505-DBH, 2014 U.S. Dist. LEXIS 179017, at *15 (D.N.H. Dec. 30, 2014) ("[P]rosecutors are entitled to absolute immunity for their actions in procuring a warrant, so long as they do not act as attesting witnesses" (alteration in original) (quoting *Orth v. Balaam*, 528 F. App'x 723, 725-26 (9th Cir. 2013))); *Chan v. Cirilli*, No. 1:21-cv-11135-IT, 2022 WL 17156089, at *——, 2022 U.S. Dist. LEXIS 211287 at *6 (D. Mass. Nov. 22, 2022) (prosecutors who allegedly fabricated criminal complaint affidavits and provided perjured testimony to grand jury were entitled to absolute immunity). This immunity necessitates the dismissal of all counts as pleaded against the USAO Defendants.

b. The Plaintiffs' RICO and RICO Conspiracy Claims

Plaintiffs' RICO claim falls short because their allegations rely too heavily on conclusory statements, and the conduct they allege does not establish a colorable RICO claim. First, the allegations in the Second Amended Complaint are too threadbare to sufficiently plead the Federal Defendants' participation in a RICO enterprise and a pattern of racketeering activity. Second, even if the Court were to credit Plaintiffs' conclusory allegations, they nonetheless have failed to adequately plead predicate acts constituting a pattern of racketeering activity.

To state a civil RICO claim under 18 U.S.C. § 1962(c), a plaintiff must allege four elements: (1) conduct; (2) of an enterprise; (3) through a pattern; (4) of racketeering activity. *Lerner v. Colman*, 26 F.4th 71, 77 (1st Cir. 2022) (citing *Sedima, S.P.R.L. v. Imrex Co.*, 472 U.S. 479, 496, 105 S.Ct. 2787, 86 L.Ed.2d 384 (1985)). "Racketeering activity" is defined to include a variety of predicate offenses, including, among other things, mail fraud, wire fraud, and theft of trade secrets. *Id.* § 1961(1). The civil-suit provision of the RICO statute grants the right to sue to "[a]ny person injured in his business or property by reason of a violation of" the substantive provisions of the statute. *Id.* § 1964(c).

Civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron*, 223 F.3d at 20 (1st Cir. 2000). "[I]n cases alleging civil RICO violations, particular care is required to balance the liberality of the Civil Rules with the necessity of preventing abusive or vexatious treatment of defendants." *Miranda v. Ponce Fed. Bank*, 948 F.2d 41, 44 (1st Cir. 1991), *abrogated on other grounds by Salinas v. United States*, 522 U.S. 52, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997). "Civil RICO is an unusually potent weapon—the litigation equivalent of a thermonuclear device. The very pendency of a RICO suit can be stigmatizing and its consummation can be costly." *Id.* Accordingly, "courts

should strive to flush out frivolous RICO allegations at an early stage of the litigation." *Figueroa Ruiz v. Alegria*, 896 F.2d 645, 650 (1st Cir. 1990).

1. RICO Enterprise

a. Caselaw

***17** In interpreting the RICO "enterprise" requirement, the Supreme Court has explained that "there is no restriction upon the associations embraced by the definition: an enterprise includes any union or group of individuals associated in fact." *Turkette*, 452 U.S. at 580, 101 S.Ct. 2524. The enterprise concept is not unbounded, however, because an enterprise must be "an entity, for present purposes a group of persons associated together for a common purpose of engaging in a course of conduct." *Id.* at 583, 101 S.Ct. 2524. In cases "involving an alleged associated-in-fact RICO enterprise, the existence of the charged enterprise does not follow, ipso facto, from evidence that those named as the enterprise's associates engaged in crimes that collectively may be characterized as a 'pattern of racketeering activity.' " *United States v. Cianci*, 378 F.3d 71, 81 (1st Cir. 2004).

Put differently, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of racketeering activity do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of

having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.* at 82. Ultimately, the First Circuit has "read *Turkette* to impose a requirement that those associated in fact function as an ongoing unit and constitute an ongoing organization. Also important to such an enterprise is that its members share a common purpose." *Id.* at 82 (internal quotations omitted). Finally, the existence of an enterprise "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Turkette*, 452 U.S. at 583, 101 S.Ct. 2524.

b. Analysis

"Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice," *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937, especially where "plaintiffs attempt to camouflage conclusory statements as allegations of fact." *A.G. ex rel. Maddox v. Elsevier, Inc.*, 732 F.3d 77, 81 (1st Cir. 2013). After sifting out Plaintiffs' conclusory statements, the RICO allegations as pleaded against the Federal Defendants are wafer thin, and the well-pleaded facts remaining are insufficient to establish that the alleged association in fact "function[ed] as an ongoing unit" or constituted an "ongoing organization." *Cianci*, 378 F.3d at 82 (internal quotations omitted).

The Second Amended Complaint pleads clearly and plausibly that the Federal Defendants investigated Plaintiffs for digital piracy, obtained and executed (on two occasions) search warrants for Plaintiffs' facilities, and coordinated with the DISH/NagraStar Defendants in the investigation, including permitting them to assist with the execution of the search warrants. Beyond these broad allegations, however, Plaintiffs' specific allegations are scant and conclusory. They assert that the "investigation" was really a pretextual hoax concocted to steal their intellectual property. But the Second Amended Complaint is silent as to why or how at least ten employees of a U.S. Attorney's Office and the FBI—ranging from the U.S. Attorney herself to an FBI evidence technician and a computer scientist—came together to orchestrate and execute this scheme.

The Second Amended Complaint offers that, starting in 2017, all Defendants conspired at the outset and together "formed an Association In Fact, [including] Legal Entity Enterprises that would help the Association in Fact defendants advance the purpose and goals of the Racketeering Enterprises' conspiratorial objectives in misappropriating themselves from Plaintiffs' DISME intellectual technology property, and trade secrets and favor the Racketeering Enterprises' economic and market growth, at the expense of the Plaintiffs' financial and business detriment." *Second Am. Compl.* ¶¶ 17-18. It adds that the "Association-In-Fact defendants knowingly

agreed, combined, and conspired to conduct the affairs of the Racketeering Enterprise in attempting and committing theft of trade secrets through a hoax criminal investigation operation." *Id.* ¶ 155.

***18** Plaintiffs also assert that all DISH/NagraStar and Federal Defendants allegedly "supervised and approved" the set-top-box operation that involved a vast majority of the purported predicate acts. *Id.* ¶¶ 133-35. However, beyond pleading that each Federal Defendant and each DISH/NagraStar Defendant "supervised and approved" that operation, Plaintiffs do not elaborate on the role of any Federal Defendant, and instead assert that the operation involved the DISH/NagraStar Defendants instructing the Toltec Defendants to purchase the set-top boxes for testing and provide one to the "Racketeering Enterprises." *Id.* ¶ 134.

These assertions are almost entirely vague, conclusory, and devoid of factual development that could explain how the alleged association in fact "function[ed] as an ongoing unit" or constituted an "ongoing organization." *Cianci*, 378 F.3d at 82 (internal quotations omitted). Aside from baldly asserting that each Federal Defendant individually agreed—for reasons unclear—to join the DISH/NagraStar conspiracy to steal Plaintiffs' property, Plaintiffs offer virtually no well-pleaded facts explaining how the conspirators functioned together as an ongoing unit or organization.

On that point, Plaintiffs offer only that "[t]he Association-In-Fact defendants had an ongoing organizational framework for carrying out the Racketeering Enterprises' criminal objectives. The Association-In-Fact defendants could not have carried out the intricate task of robbing Plaintiffs' Intellectual Property and Trade Secrets confidential information for the Racketeering Enterprises, unless it had some structure for making and communicating group decisions." *Second Am. Compl.* ¶ 130. The Court views this allegation as the epitome of a "[t]hreadbare recital[ ] of the elements of a cause of action, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937. It merely restates the requirement that the enterprise have an organizational framework, supported by nothing but the circular logic that the purported enterprise could not have succeeded unless it were truly an enterprise. There is, however, an obvious alternative explanation: that the information was seized pursuant to a legitimate law enforcement investigation, not stolen as part of an elaborate conspiracy. These allegations do not adequately plead the existence of an "ongoing unit" or "ongoing organization" required for a RICO claim. *Cianci*, 378 F.3d at 82 (internal quotations omitted).

Furthermore, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of racketeering activity do not automatically thereby

constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.*; *see also Bachman v. Bear Stearns & Co., Inc.*, 178 F.3d 930, 932 (7th Cir. 1999) (noting that a contrary rule would erroneously make "every conspiracy to commit fraud ... a RICO [enterprise] and consequently every fraud that requires more than one person to commit ... a RICO violation"). Plaintiffs allege that the Federal Defendants joined together with the other Defendants solely for the purpose of stealing Plaintiffs' "DISME intellectual technology property, and trade secrets," which they allegedly accomplished through executing the search warrants. *Second Am. Compl.* ¶¶ 18-21. While Plaintiffs assert that the DISH/NagraStar Defendants and DISH Corp. have been previously involved in trade secret misconduct, they do not allege that the Federal Defendants—or this association in fact as a whole—engaged or will engage in any misconduct unrelated to the one-off goal of stealing Plaintiffs' intellectual property. In its review of the Second Amended Complaint, the Court is unable to find the "[s]omething more" that "must be found ... that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Cianci*, 378 F.3d at 82.

***19** As noted earlier, civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO

pattern from allegations that, upon closer scrutiny, do not support it." *Efron*, 223 F.3d at 20. Ultimately, stripped of its conclusory allegations, the Court concludes that the Second Amended Complaint has not asserted sufficient facts to plead the Federal Defendants' involvement in a RICO enterprise, and Plaintiffs' RICO claim must fail.

2. Pattern of Racketeering Activity

Plaintiffs must also plead a "pattern of racketeering activity," which "means the commission of at least two related acts of racketeering activity during a period of ten years." *Humana, Inc. v. Biogen, Inc.*, 666 F. Supp. 3d 135, 147 n.4 (D. Mass. 2023) (citing 18 U.S.C. § 1961(5)). "Racketeering activity" is defined to include a variety of predicate offenses, including mail fraud, wire fraud, and theft of trade secrets. 18 U.S.C. § 1961(1). The First Circuit has observed that the Supreme Court has found "that the civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements." *In re Neurontin Mktg. & Sales Pracs. Litig.*, 712 F.3d 21, 34 (1st Cir. 2013) (citing *Holmes v. Secs. Investor Prot. Corp.,* 503 U.S. 258, 268, 112 S.Ct. 1311, 117 L.Ed.2d 532 (1992)).

Plaintiffs allege that the purported RICO conspiracy's pattern of racketeering involved numerous predicate acts, including:

> [A]cts indictable under Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy to Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.), while in addition, committing the possible underlying criminal offenses as prohibited under [the Computer] Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.), 18 U.S.C.A. § 2235-Search warrant procured maliciously; 18 U.S.C.A. § 1621-Perjury generally; 18 U.S.C.A. § 1001-Statements or entries generally, 18 U.S.C.A. § 912-Officer or employee of the United States; 18 U.S.C.A. § 2234-Authority exceeded in executing warrant; 18 U.S.C.A. § 2236-Searches without warrant, 18 U.S.C.A. § 1905-Disclosure of Confidential Information, while accomplishing their racketeering objectives. *Second Am. Compl.* ¶ 132.

Most of these alleged offenses are not "predicate acts" under the RICO statute. Mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), and theft of trade secrets (18 U.S.C. §§ 1831 and 1832) [9] qualify; the rest do not. *See* 18 U.S.C. § 1961(1) (listing qualifying offenses); *Pls.'*

Opp'n at 13 ("The Federal defendants violated three predicate acts indictable under RICO: mail fraud; wire fraud; and misappropriation or theft of trade secrets"). The Court turns to the allegations concerning these three predicate acts.

a. Wire and Mail Fraud

"Mail or wire fraud requires proof of (1) a scheme to defraud based on false pretenses; (2) the defendant's knowing and willing participation in the scheme with the specific intent to defraud; and (3) the use of interstate mail or wire communications in furtherance of the scheme." *Sanchez v. Triple-S Mgmt., Corp.*, 492 F.3d 1, 9-10 (1st Cir. 2007). "The 'in furtherance' requirement is to be read broadly." *United States v. Simon*, 12 F.4th 1, 33 (1st Cir. 2021). "[T]he mails need not be an essential element of the scheme. It is sufficient for the mailing to be incident to an essential part of the scheme, or a step in [the] plot." *Schmuck v. United States*, 489 U.S. 705, 710-11, 109 S.Ct. 1443, 103 L.Ed.2d 734 (1989) (internal citations and quotations omitted).

***20** Federal Rule of Civil Procedure 9(b) requires that "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." FED. R. CIV. P. 9(b); *see also Humana*, 666 F. Supp. 3d at 154 ("Civil RICO claims based on the predicates of mail or wire fraud must meet the heightened

pleading standard of Rule 9(b)"). A complaint must specify "the time, place, and content of an alleged false representation." *United States ex rel. Kelly v. Novartis Pharms. Corp.*, 827 F.3d 5, 13 (1st Cir. 2016) (quoting *Doyle v. Hasbro, Inc.*, 103 F.3d 186, 194 (1st Cir. 1996)). Furthermore, "[t]he false or fraudulent representation [in a mail or wire fraud claim] must be material." *United States v. Appolon*, 715 F.3d 362, 367 (1st Cir. 2013) (first alteration in original) (citation omitted).

Plaintiffs' mail and wire fraud claims are limited to allegations that Mr. Jaczewski—in an operation "instructed" by Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel and "supervised and approved" by the Federal Defendants—used an alias to purchase two Naicom set-top boxes and a monthly subscription he maintained for two years. *Second Am. Compl.* ¶¶ 132-37. In Plaintiffs' view, each purchase or payment "constitutes a wire fraud racketeering act since [Mr. Jaczewski, acting under the alias] Brian Parsons, posed as [a] legitimate client and used the interstate internet electronic services to access Naicom's website, and register online under the false pretenses of BRIAN PARSONS" and "made online payments through the use of interstate internet electronic services ... to defraud and deprive Naicom Corporation of its legitimate products, intellectual property and trade secrets." *Id.* ¶ 134. Between the initial purchases and monthly subscription payments, Plaintiffs tally 22 acts of wire fraud. *Id.* ¶ 135.

Finally, they also consider the initial purchase to constitute mail fraud because Mr. Jaczewski "posed as a legitimate client and used the United States Postal Services to have Naicom mail him the IPTV Set Top Box to a fake address." *Id.* ¶ 133. Accepting these allegations as true, the Court concludes that the facts are insufficient to support Plaintiffs' wire and mail fraud claims because the purportedly fraudulent representations (limited to Mr. Jaczewski's use of an alias for the set-top-box purchase and subscription) were not material. Nor could the mail and wire fraud allegations be predicate acts for Plaintiffs' RICO claim because the set-top-box operation was not causally connected to Plaintiffs' damages.

A material statement "has a natural tendency to influence, or [is] capable of influencing, the decision of the decisionmaking body to which it was addressed" but plaintiffs "need not prove that the decisionmaker actually relied on the falsehood or that the falsehood led to actual damages." *Appolon*, 715 F.3d at 368 (alteration in original) (internal quotation omitted). In *Appolon*, the defendant provided untrue responses on a mortgage application, in response to questions "that specifically sought information regarding the purchaser's income, assets, and intent to reside in the property." *Id.* The First Circuit considered the false responses material because the questions "were designed to assess the borrower's creditworthiness" and thus the statements "were capable of influencing [the

lender's] decision." *Id.*

The purported false statements here are far afield from providing false financial information on a mortgage application. Naicom's set-top boxes are commercial electronic products sold in retail stores like Sam's Club, and its subscription services are available on Apple's AppStore as the Naicom TV App. *Second Am. Compl.* ¶ 70 ("On February 16, 2017, Apple Corporation approved Naicom Corporation App for Apple's AppStore as Naicom TV App"); *id.* ¶ 71 ("On December 15, 2017, Sam's Club approved Naicom Corporation to officially launch and distribute in their retail stores [ ] Naicom's IPTV Set Top Box which offered the distribution of tv programming to customers in Puerto Rico"). Parsing Plaintiffs' allegations, they allege that Mr. Jaczewski committed wire and mail fraud by providing a false name "of BRIAN PARSONS, fake Phone (727) 409-9464, fake Email: parsons.brian716@outlook.com and Address: 9079 FOURTH STREET NORTH SAINT PETERS FL 33702 IP: 70.127.233.139, and made online payments through the use of interstate internet electronic services using the PM Visa ending in 2775." *Id.* ¶ 134. Plaintiffs also allege Mr. Jaczewski used the alias of Brian Parsons when purchasing two Naicom set-top boxes. *Id.* ¶ 133.

***21** The allegations confirm that Mr. Jaczewski used the false name of Brian Parsons. It is unclear, however, what Plaintiffs mean by a "fake Phone"—whether Mr.

Jaczewski used a different phone as part of the alias or if the number provided was entirely made up. Plaintiffs have not adequately pleaded that the remainder of the "false" statements are actually false. The Second Amended Complaint does not allege that email services require customers to use their real name in their email address. Thus, the Second Amended Complaint fails to allege that using an email with "parsons.brian" in the address is a false statement as there is no allegation that the address itself does not actually exist. It is unclear what Plaintiffs mean by a "fake" address, but again, the Second Amended Complaint also does not allege that online retail customers are prohibited from having a product shipped to any address they desire, and Plaintiffs have offered nothing to suggest that this constitutes a false representation. [10] Likewise, nothing in the Second Amended Complaint suggests that the IP address or credit card involved false statements. [11]

The Court is thus left to consider whether Mr. Jaczewski's purchase of two commercially available products and an accompanying subscription using the name Brian Parsons can support Plaintiffs' alleged mail and wire fraud violations. The Court concludes that it cannot, because—absent allegations to the contrary—a customer providing a false name in such circumstances does not have "a natural tendency to influence, [nor is it] capable of influencing, the decision of the decisionmaking body to which it was

addressed." *Appolon*, 715 F.3d at 368. Nothing in the Second Amended Complaint suggests that the use of this alias was material to Plaintiffs' decision to sell Mr. Jaczewski their commercially available product. There is no allegation that Mr. Jaczewski was either known to Plaintiffs or prohibited from purchasing Plaintiffs' products. What is missing is an allegation that the alias could have reasonably affected the "decision of the decisionmaking body" (for example, Naicom's sales department) to process Mr. Jaczewski's payment or ship his order. Absent allegations regarding how Mr. Jaczewski's alias affected Naicom's decision to sell him their product, Plaintiffs have not pleaded material fraud with the requisite particularity. Plaintiffs' wire and mail fraud claims cannot stand and thus do not count as predicate acts in support of their RICO claim.

Furthermore, even if the Court did find the alleged representations material, Plaintiffs' claims fall short of the causation standard required for a wire or mail fraud-based RICO claim. *Neurontin*, 712 F.3d at 34 ("[T]he civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements" (citing *Holmes,* 503 U.S. at 268, 112 S.Ct. 1311)). "The 'central question' in evaluating proximate causation in the RICO context 'is whether the alleged violation led directly to the plaintiff's injuries.' " *Sterling Suffolk Racecourse, LLC v. Wynn Resorts, Ltd.*, 990 F.3d 31, 35 (1st Cir. 2021) (quoting *Anza v. Ideal Steel Supply*

Corp., 547 U.S. 451, 461, 126 S.Ct. 1991, 164 L.Ed.2d 720 (2006)). Quoting the U.S. Supreme Court, the First Circuit has noted that "[a] link [between the RICO predicate acts and plaintiff's injuries] that is too remote, purely contingent, or indirect is insufficient to show proximate cause." *Id.* (alterations in original) (quoting *Hemi Grp., LLC v. City of New York*, 559 U.S. 1, 9, 130 S.Ct. 983, 175 L.Ed.2d 943 (2010)). In addition, the First Circuit has identified "three functional factors with which to assess whether proximate cause exists under RICO." [12] *Id.* (quoting *Neurontin*, 712 F.3d at 35-36). The but-for causation question, in contrast, asks whether, absent the defendant's violation, the plaintiff would have suffered the same injury. *See Neurontin*, 712 F.3d at 34.

***22** Here, the alleged violations fail both causation tests because Plaintiffs portray the set-top-box operation as an unmitigated failure that only provided further proof that Naicom was a legitimate company. They allege that "after testing Naicom TV several times to identify if it was providing DISH programming, on each case the test *revealed no DISH content*." *Second Am. Compl.* ¶ 90 (emphasis added). After attempting to use the boxes to penetrate Plaintiffs' network and steal their secrets, the "Dish/Nagrastar defendants also informed the Racketeering Enterprises that the Association in Fact defendants couldn't penetrate Naicom's Data Center computers, servers, encoders electronic security system, and that a physical intrusion was necessary to extract the

intellectual property from the computers, servers, and encoders by physical access." *Id.* ¶ 93. They allege further that the operation did not yield evidence that would support a search warrant and thus the defendants had to provide "affidavits they knew contained material information known to be false and perjured to create probable cause to gain legal access into Plaintiffs['] private business." *Id.* ¶ 20.

As the Court understands the Second Amended Complaint, Plaintiffs allege that the Defendants conspired from the outset to steal their intellectual property. The set-top-box operation was an attempt to steal Plaintiffs' secrets by reverse engineering the technology and/or penetrating Plaintiffs' networks. But the operation failed. All the Defendants gained was more proof that Naicom was a legitimate company, and they then had to resort to falsifying affidavits to justify physical access to Naicom's Data Center (through search warrants) that would finally allow them access to the desired technology. Plaintiffs have not alleged any harm prior or unrelated to the execution of the warrants. Nor have Plaintiffs alleged that Defendants would not have sought and executed the search warrants had they not undertaken the set-top-box operation.

The Court concludes that there is no connection—proximate or but-for—between the allegedly fraudulent set-top-box purchase and the Defendants acquiring

Plaintiffs' intellectual property during the execution of the warrants. The alleged mail and wire fraud is "too remote" from Plaintiffs' alleged harms, *Hemi Grp.*, 559 U.S. at 9, 130 S.Ct. 983, and there is no indication that Plaintiffs would not have suffered their alleged harms absent the set-top-box operation. Plaintiffs' Second Amended Complaint thus falls short on both the materiality and causation standards for wire and mail fraud as predicate acts.

b. Theft of Trade Secrets

Plaintiffs also plead that the Federal Defendants committed RICO predicate acts by misappropriating their trade secrets. *See Second Am. Compl.* ¶¶ 138-41; *Pls.' Opp'n* at 13 ("The Federal defendants violated three predicate acts indictable under RICO: mail fraud; wire fraud; and misappropriation or theft of trade secrets"). As noted above, RICO predicate offenses include any act indictable under 18 U.S.C. § 1832, relating to theft of trade secrets under the DTSA. 18 U.S.C. § 1961(1). 18 U.S.C. § 1832 provides that "[w]hoever, with intent to convert a trade secret ... to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information," or attempts to do so, shall be subject to criminal penalties. *Id.* § 1832(a)(1),

(a)(4). "Trade secret" is defined broadly to include "all forms and types of financial, business, scientific, technical, economic, or engineering information," as long as "the owner thereof has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." *Id.* § 1839(3). Critically, however, the DTSA also provides that "[t]his chapter does not prohibit ... any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State." *Id.* § 1833(a)(1).

***23** The scope of Plaintiffs' DTSA theories is unclear. They allege clearly that the Federal Defendants violated the DTSA on August 27 and 29, 2019 (the dates of the searches) by "facilitating and assisting" the DISH/NagraStar Defendants' entry into Naicom's facility to steal Naicom's trade secrets. *Second Am. Compl.* ¶ 141. Their other theories are far more ambiguous, alleging generally that "[b]eginning on or before August 7, 2017," Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel, along with the Federal Defendants: "stole, and without authorization misappropriated, took, carried away, or by fraud, artifice, or deception obtained trade secrets," *id.* ¶ 138; "did without authorization, spy, reverse engineered, copied, duplicated, downloaded, uploaded, altered,

destroyed, replicated, transmitted, delivered, sent, communicated, and/or conveyed intellectual property and trade secrets," *id.* ¶ 139; and "misappropriated, obtained, or converted without authorization [the trade secrets] to the economic benefit of [the] Racketeering Enterprises and other defendant coconspirators." *Id.* ¶ 140. This section of the Second Amended Complaint, however, offers no additional details as to when or how any specific Federal Defendant violated the DTSA.

The only clarity in Plaintiffs' 75-page opposition is their contention that "[t]he record ... supports the finding that the Dish/Nagrastar defendants' misapprop[riation of] Plaintiffs' trade secrets by illegal means is unlawful, given the way [the] Dish/Nagrastar defendants obtained the same through the illegal search warrant, warrantless executions, and trespass, orchestrated and facilitated by the Federal defendants." *Pls.' Opp'n* at 66. Based on the content of Plaintiffs' Second Amended Complaint and their statements in opposition to the Federal Defendants' motion to dismiss, the Court narrows the scope of the DTSA inquiry to the Federal Defendants' actions related to obtaining and executing the search warrants—discarding any other DTSA allegations as pleaded with insufficient particularity against any Federal Defendant. 13

The Federal Defendants argue that Plaintiffs' misappropriation of trade secrets claims should be

dismissed because "the plaintiffs have not adequately alleged the existence of any trade secrets" and because "Congress specifically exempted from the statute's criminal and civil provisions 'any otherwise lawful activity conducted by a governmental entity of the United States.' " *Defs.' Mot.* at 32-33 (quoting 18 U.S.C. § 1833(a)(1)). The Court concludes that Plaintiffs have not adequately impugned the validity of the warrants and the Federal Defendants' conduct is thus exempt from DTSA liability as authorized law enforcement activity.

The Federal Defendants submit that "the plaintiffs here acknowledge that the government obtained and searched under the authority of a warrant," which "makes the Federal Defendants' actions here presumptively lawful." *Id.* at 33. They add that the Supreme Court has observed that "[t]he fact that a neutral magistrate has issued a warrant is the clearest indication that the officers acted in an objectively reasonable manner or, as we have sometimes put it, in 'objective good faith.' " *Id.* at 23, 130 S.Ct. 983 (quoting *Messerschmidt v. Millender*, 565 U.S. 535, 546, 132 S.Ct. 1235, 182 L.Ed.2d 47 (2012)). The Federal Defendants assert further that "[t]he plaintiffs' conclusory allegations that the warrant was 'unlawful,' or secured using an affidavit in support of probable cause containing 'material information known to be false and perjured' are insufficient to [impugn the presumptive validity of the warrant]." *Id.* at 33 (citations omitted).

Plaintiffs respond that "the procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Pls.' Opp'n* at 30. Because Plaintiffs dispute the validity of the warrants, the Court addresses this issue first.

***24** The parties agree that the relevant standard for evaluating the validity of a warrant is the *Franks v. Delaware* framework, which requires Plaintiffs to adequately allege that both (1) "a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit" and (2) "the allegedly false statement is necessary to the finding of probable cause." *United States v. Reiner*, 500 F.3d 10, 14 (1st Cir. 2007) (quoting *Franks v. Delaware,* 438 U.S. 154, 155-56, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978)).

Plaintiffs cite ten statements that they allege Defendants "falsely submitted to the Court." *Id.* at 31. The Court has examined each and concludes that none supports Plaintiffs' claims.

Plaintiffs' first purportedly false statement is the Federal Defendants' statement that they believed there was probable cause that Plaintiffs violated copyright and money laundering laws. *Id.* Plaintiffs allege that this statement is false because:

The execution of the search and seizure warrant in this case did not produce any criminal evidence whatsoever; there was no probable cause. That is why the United States never opposed Plaintiffs' Motion for Return of Property under Rule 41(g) of the Fed.R.Crim.P. In fact, they didn't even contend the serious violations Plaintiffs imputed under *Franks* in the Rule 41(g) motion. *Id.* This logic is unavailing. Plaintiffs cannot rely on the circular reasoning that the search's alleged failure to produce incriminating evidence thereby proves that the Defendants could not have believed there was probable cause to search. *See Karamanoglu v. Town of Yarmouth*, 15 F.4th 82, 88 (1st Cir. 2021) (defining the probable cause inquiry as "whether, on balance, the facts *known to the officer at the time of the arrest* support probable cause").

Equally inadequate is Plaintiffs' claim that the Federal Defendants' failure to oppose Plaintiffs' motion to return the seized property proves not only that the seized property was not incriminating, but also that there was no probable cause to search in the first place. *See United States v. Pierre*, 484 F.3d 75, 87 (1st Cir. 2007) ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return"). The government's return of the seized hard drives and thumb drives, which—unlike drugs or illegal firearms—are not inherently contraband and can easily be downloaded or duplicated, is consistent with *Pierre*.

Furthermore, Plaintiffs are simply incorrect that success on a Rule 41(g) motion conclusively establishes the invalidity of a search. Rule 41(g) allows motions for return of property from "[a] person aggrieved by an unlawful search and seizure of property *or* by the deprivation of property." FED. R. CRIM. P. 41(g) (emphasis supplied).

Without more, the property's return alone cannot demonstrate an absence of probable cause to search and seize in the first place. Ultimately, Plaintiffs' first purportedly false statement offers nothing to undermine the validity of the warrants and searches.

Second, Plaintiffs offer that the Federal Defendants "assured the Court they had evidence based on an investigation conducted by Nagrastar of Naicom's unauthorized use of Direct TV signal to distribute its programing to its paid subscribers." *Pls.' Opp'n* at 32. Plaintiffs assert that this statement was false because "[t]he United States did not produce any evidence as to the above allegations ... [i]n contrast, Naicom did produce all the documentary evidence establishing that they were authorized to distribute the copyright material." *Id.*

***25** Again, Plaintiffs appear to be suggesting that exculpatory evidence they produced during the search proves that the affidavit was false. These conclusory assertions tied together by circular logic do not adequately

demonstrate the falsity of the affidavit. While Plaintiffs contend that the affidavit did not "produce any evidence" supporting the suggestion that Naicom was distributing DirecTV content without authorization, the affidavit avers that Naicom's system displayed DirecTV error messages on at least 16 channels (and includes a photo of the message), that Naicom's satellite dishes were precisely oriented in a manner necessary to receive DirecTV satellite signals, that representatives of the companies offering some channels Naicom purported to provide confirmed that Naicom was not licensed to provide them, and other indicia of piracy. *See Pls.' Opp'n to DISH/NagraStar Mot.*, Attach. 1 at 272-94, *Aff. in Supp. of an Application for a Search Warrant* (*Warrant Aff.*). Simply put, Plaintiffs' argument that the affidavit contained no evidence of piracy is incorrect.

Third, Plaintiffs assert that, during a 2018 FBI site visit of Naicom's property, Mr. Vega "repeatedly told the agent that Naicom was a legal corporation and showed the agent a certificate from the National Cable Television Cooperative (NCTC) on the wall," yet the Federal Defendants still "filed the affidavit containing materially false and perjured statements." *Pls.' Opp'n* at 32. It is not clear specifically which "materially false and perjured statements" Plaintiffs are referring to, but the affidavit states that the FBI called NCTC's management group, which confirmed that Naicom was *not* a member. *Warrant Aff.* ¶ 15. Nothing in Plaintiffs' assertion that Mr. Vega

told the FBI his company was legitimate and showed them a certificate on the wall establishes that the affidavit's claim—that NCTC management represented to the FBI that Naicom was not a member—was perjured.

Fourth, Plaintiffs contend that the affidavit's claim that Naicom was using the NCTC certificate to create the appearance of legal access to channels was "a false and perjured statement" because an FBI agent took pictures of "Naicom's National Rural Telecommunications Cooperative 'NRCT' Certificate" and Naicom had licenses with other networks. *Pls.' Opp'n* at 32-33.

Fifth, Plaintiffs focus on the affidavit's claim that FBI agents spoke with NCTC management, who confirmed that Naicom was not a member of their organization. *Id.* at 33. They allege that this "is a false and perjured statement" because Naicom provided evidence that it is a member of the NRTC. *Id.*

The distinction between NCTC and NRTC here is somewhat confusing. It appears Plaintiffs are alleging that the FBI took pictures of a NRTC certificate on the wall but incorrectly referred to it in the affidavit as a NCTC certificate, or that the FBI mistook their NRTC certificate for an NCTC certificate. However, Plaintiffs also claim that the affidavit's assertion that they are not a member of the NCTC is a perjured statement because they provided evidence that they are a member of the NRTC.

Plaintiffs offer no evidence that the latter statement was perjured because proving they are a NRTC member does not contradict the claim that they are not a NCTC member. To the extent that the FBI may have misidentified a NRTC certificate as a NCTC certificate, the record does not suggest that this "allegedly false statement is necessary to the finding of probable cause," especially given the strength of the other supporting claims in the affidavit. *United States v. Patterson*, 877 F.3d 419, 424 (1st Cir. 2017) (quoting *Franks*, 438 U.S. at 156, 98 S.Ct. 2674).

Sixth, Plaintiffs turn to the affidavit's assertion that FBI agents contacted officials at HBO and DirecTV, who verified that Naicom did not have a relationship with their organizations despite offering HBO content. *Pls.' Opp'n* at 33. Plaintiffs claim that "[t]his is a false and perjured statement" because "Naicom provided evidence that it is licensed to distribute HBO and Cinemax programming." *Id.* (citing *Pls.' Opp'n to DISH/NagraStar Mot.*, Attach. 1 at 356) (HBO invoice dated August 31, 2019, for roughly $200 per month for "Cable – Private Home" services). Plaintiffs' claim is unpersuasive for two reasons: (1) this invoice for inexpensive "Cable – Private Home" services does not appear to provide evidence of a licensing agreement; and (2) Plaintiffs have not directly contradicted the purportedly perjured claim, which was that HBO and DirecTV officials represented to the FBI that they did not have a relationship with Naicom.

***26** Seventh, Plaintiffs focus on the affidavit's claim that the "external appearance of the Data Center offered indicia of piracy," calling it a "false and perjured statement" because "[a]t the conclusion of the search and seizure warrant execution the FBI agents found that [ ] Naicom's equipment (encoders) were provided by the networks authorizing the programming distribution and that the use of the satellite was in fact to download the codes provided by the networks." *Id.* at 33-34. Plaintiffs again rely on circular logic, as the discovery of exculpatory evidence at the conclusion of a warrant's execution does not provide a "substantial preliminary showing" that the underlying affidavit was perjured. *Franks*, 438 U.S. at 155-56, 98 S.Ct. 2674.

Plaintiffs' eighth point suffers from the same defect. They claim that the affidavit's statements that there were suspicious financial transactions between Naicom and other businesses owned by Mr. Quinones and Mr. Vega were false and perjured because "[d]uring the execution of the Search Warrant S/A Lange interviewed employees from the Business Office and was provided with financial records" which established "that none of the Corporations were involved in any money laundering activities." *Pls.' Opp'n* at 34. Again, the fact that a search did not uncover incriminating evidence does not establish that it was predicated on a perjured affidavit.

Plaintiffs' ninth point takes issue with the affidavit's

request to seize computers and data based on claimed probable cause that they contained evidence. *Id.* at 34-35. Plaintiffs contend that this statement was perjured because the "FBI agents were not looking for any criminal evidence" during the search and they did "not find[ ] any evidence whatsoever of the crimes described in the warrant, which also denied any probable cause." *Id.* at 34. The Court does not fully follow Plaintiffs' logic across these seemingly contradictory assertions, but they appear to utilize the same circular reasoning (the assertion of probable cause was perjured because the resulting search "denied any probable cause"), along with the conclusory contention that the FBI was not actually looking for evidence. [14] These claims do not undermine the validity of the warrants.

Tenth, Plaintiffs claim that the affidavit's request to seize evidence relating to statutory violations was "false and perjured" because the FBI did not find any evidence at the conclusion of the search. *Id.* at 35. Beyond the fact that this argument relies on the same circular logic, an affidavit's request to seize "things and ... records" is not an assertion of fact and cannot be false or perjured. *Id.*

To summarize, none of these purportedly false statements, alone or in combination, satisfies Plaintiffs' burden under the *Franks* standard to overcome the presumed validity of the warrants. Moreover, Plaintiffs offer several additional arguments that are similarly

unavailing.

Plaintiffs submit that the August 29, 2019 search was "illegal" and "warrantless" because "[t]he Federal and Dish/Nagrastar defendants knew for a fact that the first search warrant execution had already denied any criminal wrongdoing, and that the initial alleged probable cause had dissipated." *Id.* at 42. This assertion—that the Federal Defendants knew probable cause had dissipated—is wholly conclusory (especially in light of Plaintiffs' argument that the entire investigation was a hoax, and the agents knew probable cause never existed). Furthermore, the warrants did not expire until September 4, 2019 and courts generally recognize a "reasonable continuantion rule" providing that a search may be reasonably continued if the warrant remains valid. [15] *See United States v. Keszthelyi*, 308 F.3d 557, 568-69 (6th Cir. 2002) (describing the rule and collecting cases). Plaintiffs have not offered any well-pleaded, nonconclusory allegations suggesting that the continuance here was unreasonable. [16]

***27** Plaintiffs also contend that the searches were unlawful because the Federal Defendants did not follow the procedure to obtain a Stored Communications Act warrant (also known as a disclosure order or a SCA order). *Pls.' Opp'n* at 37-38. However, as the Federal Defendants observe, "the government appropriately opted for a

traditional search warrant in this case because it sought to seize evidence of the plaintiffs' piracy operation rather than to require the plaintiffs to disclose certain electronic communications." *Defs.' Reply* at 18.

While SCA warrants and traditional search warrants are not the same thing, the Court has no trouble concluding that the Federal Defendants' decision to proceed via search warrant was proper. As one court has explained:

> SCA warrants "are not like the search warrants used in the physical world: they are 'executed' when a law enforcement agent delivers (sometimes by fax) the warrant to the [service provider]. The [service provider], not the agent, performs the 'search'; the [service provider] 'produces' the relevant material to the agent; the user associated with the inbox often never learns that his inbox has been 'searched.' In sum, these are not search warrants at all and to call them such confuses legal terminology."

In re Info. Associated with @gmail.com, No. 16-mj-00757 (BAH), 2017 WL 3445634, at *———–———, 2017 U.S. Dist. LEXIS 130153, at *52-53 (D.D.C. July 31, 2017) (quoting Paul K. Ohm, *Parallel–Effect Statutes and E–Mail "Warrants": Reframing the Internet Surveillance Debate*,

72 GEO. WASH. L. REV. 1599, 1610-11 (2004)). Additionally, the standard for an SCA order is "less stringent than the probable cause standard generally required for a search warrant." *United States v. Taylor*, 54 F.4th 795, 804 (4th Cir. 2022). Finally, even if the Federal Defendants were seeking information protected by the SCA, the statute gives them the option of seeking either an SCA order or a traditional search warrant. [17] *See* 18 U.S.C. § 2703(b) (the government may obtain "a court order for such disclosure under subsection (d) of this section" *or* "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"); *id.* § 2703(c) (same).

Plaintiffs' argument is groundless because the Federal Defendants were primarily—if not entirely—seeking information not protected by the SCA. Regardless, they obtained a search warrant for the facility and computer systems, thereby satisfying the requirements of the SCA.

Plaintiffs also argue again that "the Federal defendants cannot raise at this stage a legal defense which the Federal defendants abandoned when they did not oppose the Motion for Return of Property under Rule 41(g) proceedings." *Pls.' Opp'n* at 43. However, as the Court has already explained, the government's decision not to oppose a motion to return property does not affect the validity of the warrants or seizure. *See Pierre*, 484 F.3d at 87 ("Once seized property is no longer needed as evidence, a criminal

defendant is presumed to have the right to its return").

Finally, while Plaintiffs contend that permitting the DISH/NagraStar Defendants to assist with the search was unlawful, they acknowledge that "Congress has explicitly authorized the practice." *Pls.' Opp'n* at 39 (citing 18 U.S.C. § 3105). Further, although they contend that any civilian assisting with a search "must have been serving a legitimate investigative function," *id.*, Plaintiffs fail to make any well-pleaded, nonconclusory allegation that the DISH/NagraStar Defendants were not serving such a function. Indeed, Plaintiffs do not offer any persuasive argument that would permit the Court to find that the DISH/NagraStar Defendants' presence rendered the search illegal. [18]

***28** In sum, Plaintiffs have failed to adequately challenge the validity of the search warrants or to establish that any Federal Defendant exceeded the bounds of his or her lawful authority. Plaintiffs have thus failed to plead a DTSA violation as a predicate act in support of their RICO claim. *See* 18 U.S.C. § 1833(a)(1) ("This chapter does not prohibit ... any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State"). Absent both an enterprise and a pattern of racketeering activity, Plaintiffs' RICO (Count I) claim must be dismissed as to the Federal Defendants.

These same pleading shortfalls doom Plaintiffs' RICO conspiracy claim as to the Federal Defendants. *See Efron*, 223 F.3d at 21 ("A conspiracy claim under section 1962(d) may survive a *factfinder's* conclusion that there is insufficient evidence to prove a RICO violation, but if the pleadings do not state a substantive RICO claim upon which relief may be granted, then the conspiracy claim also fails" (citations omitted) (emphasis in original)); *see also Salinas v. United States*, 522 U.S. 52, 64, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997) ("A conspirator must intend to further an endeavor which, if completed, *would satisfy all of the elements of a substantive criminal offense*, but it suffices that he adopt the goal of furthering or facilitating the criminal endeavor" (emphasis supplied)). As such, the Court also dismisses Plaintiffs' RICO conspiracy claim (Count II) as to the Federal Defendants.

c. Plaintiffs' DTSA, CFAA, SCA, and DMCA Claims

The Court's determination that the Federal Defendants' conduct during the execution of the search warrants did not exceed the bounds of a lawful warrant is ultimately also fatal to Plaintiffs' DTSA, CFAA, SCA, and DMCA claims, because each statute has a similar exemption for law enforcement activity.

i. The DTSA Claim

Plaintiffs' freestanding DTSA claim alleges the same violation as the DTSA claims offered as predicate acts for the RICO claim, and thus fails for the reasons previously described. While the DTSA does provide a private right of action for owners "of a trade secret that is misappropriated ... if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce," 18 U.S.C. § 1836, this right of action cannot be used to challenge "otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State." *Id.* § 1833(a)(1). The Court dismisses Plaintiffs' DTSA claim (Count VI) as to the Federal Defendants.

ii. The CFAA Claim

The CFAA contains virtually the same exception for law enforcement activity. *Compare* 18 U.S.C. § 1833(a)(1) (the DTSA "does not prohibit or create a private right of action for any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State"), *with id.* § 1030(f) (the CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States"). In *Smith v. Aldridge*, the plaintiff "allege[d] that Defendant stole his smartphone, which is legally protected under CFAA" but also admitted "that

Defendant had a warrant when she accessed his phone." No. 3:17-cv-01485-HZ, 2018 WL 1434813, at *6, 2018 U.S. Dist. LEXIS 47021, at *18 (D. Or. Mar. 22, 2018). The district judge observed that "Defendant, therefore, had legal authority to access Plaintiff's phone at the time that she did" and because "Plaintiff admits that Defendant had a warrant, Plaintiff would have to show that the warrant was invalid in order to show that the access was unauthorized [For the plaintiff] to prevail on this CFAA claim, the Court would have to determine that Plaintiff's Fourth Amendment Rights were violated." *Id.* at *18 & n.4.

***29** Because the Federal Defendants' challenged conduct was "lawfully authorized investigative ... activity" under the search warrants, Plaintiffs have not pleaded a viable CFAA claim.

iii. The SCA Claim

Turning to the SCA claim, "courts in the First Circuit have consistently applied CFAA caselaw in analyzing the SCA Thus, the Court's analysis under this statute is the same as under the CFAA." *Sun West Mortg. Co. v. Flores*, No. 15-1082 (GAG), 2016 WL 1030074, at *4, 2016 U.S. Dist. LEXIS 31149 at *11 (D.P.R. Mar. 10, 2016) (citation omitted); *see also Cheng v. Romo*, No. 11-10007-DJC, 2012 WL 6021369, at *4, 2012 U.S. Dist. LEXIS 169535 at *10 (D. Mass. Nov. 28, 2012) ("Other district courts within this

Circuit have addressed 'access without authorization' and 'exceeding authorization' in considering the analogous provision of the CFAA"). As the Court noted previously, even if the Federal Defendants were seeking information protected by the SCA, the statute gives them an option of seeking either an SCA order or a traditional search warrant. *See* 18 U.S.C. § 2703(b) (the government may obtain "a court order for such disclosure under subsection (d) of this section" *or* "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"); *id.* § 2703(c) (same). Furthermore, even if the warrants were not valid, the SCA still provides that "[a] good faith reliance on a court warrant or order is a complete defense to any civil or criminal action brought under this chapter or any other law." *Id.* § 2707(e).

Even if the Court were to assume that the Federal Defendants seized electronic communications protected by the SCA, they did so pursuant to valid warrants and thus did not violate the statute. Furthermore, even if the warrants were not valid, Plaintiffs' allegations of bad faith by the Federal Defendants are conclusory and the Federal Defendants would thus still be protected by the good faith defense. *See John K. MacIver Inst. for Pub. Pol'y, Inc. v. Schmitz*, 243 F. Supp. 3d 1028, 1035 (W.D. Wis. 2017), *aff'd*, 885 F.3d 1004 (7th Cir. 2018) ("Given the absence of any case law even suggesting that a state search warrant issued under similar circumstances may be invalid under

the SCA, plaintiff's conclusory allegation of a lack of good faith is also wholly insufficient to support a claim that defendants 'actually knew that the [warrant] was invalid [under the SCA]' " (emphasis omitted) (alterations in original) (quoting *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1181 (9th Cir. 2013))). Plaintiffs' SCA claim will not lie against the Federal Defendants for essentially the same reasons as their CFAA claim.

iv. The DMCA Claim

Similarly, the DMCA explicitly provides that it "does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State." 17 U.S.C. § 1201(e). This language is virtually identical to the CFAA's law enforcement exception. *Cf.* 18 U.S.C. § 1030(f) (the CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State"). This provision of the DMCA has been interpreted as "broadly exempting official law enforcement activity." *Green v. U.S. Dep't of Just.*, 392 F. Supp. 3d 68, 77 (D.D.C. 2019).

***30** As with the DTSA, CFAA, and SCA claims, even assuming Plaintiffs had established all the other elements of a DMCA claim, their claim would still be stymied by the

statute's law enforcement exception. Plaintiffs' DTSA, CFAA, SCA, and DMCA claims all fail as pleaded against the Federal Defendants because the challenged searches were conducted pursuant to lawfully authorized warrants.

d. The Plaintiffs' PTSA Claim

The Federal Defendants contend that Plaintiffs' Puerto Rico Uniform Trade Secrets Act claim is barred by the Westfall Act. *Defs.' Mot.* at 35-36. The Court agrees.

"Under the Westfall Act, the Attorney General can certify that a federal employee named as a defendant in a civil case was 'acting within the scope of his office or employment at the time of the incident' that serves as the basis for a tort claim against that employee." *Lyons v. Brown*, 158 F.3d 605, 606 (1st Cir. 1998) (quoting 28 U.S.C. § 2679(d)(1)). The Act provides that "[u]pon certification ... any civil action or proceeding commenced upon such claim in a United States district court shall be deemed an action against the United States ... and the United States shall be substituted as the party defendant." *Vélez-Díaz v. Vega-Irizarry*, 421 F.3d 71, 75 (1st Cir. 2005) (alterations in original) (quoting 28 U.S.C. § 2679(d)(1)). While certification is sufficient to substitute the United States as defendant and dismiss the federal employees from the case, the certification is "provisional and subject to judicial review." *Davric Me. Corp. v. U.S. Postal Serv.*, 238 F.3d 58, 65 (1st Cir. 2001) (citing

Gutiérrez de Martínez v. Lamagno, 515 U.S. 417, 434, 115 S.Ct. 2227, 132 L.Ed.2d 375 (1995)). If plaintiffs are able to show that the employees acted outside the scope of their employment, the employees may be re-substituted as the party defendants. *Davric*, 238 F.3d at 65; *Aversa v. United States*, 99 F.3d 1200, 1208 (1st Cir. 1996).

The Federal Defendants submit that Plaintiffs' PTSA claim "is barred because Congress provided in the Westfall Act that the exclusive remedy for claims for negligent or wrongful acts or omissions of federal employees acting in the scope of office or employment is a suit against the United States under the Federal Tort Claims Act" and "the Attorney General's designee has certified scope of office or employment" for the Federal Defendants. *Defs.' Mot.* at 35-36. This is sufficient to substitute the United States as a defendant: "Upon certification ... any civil action or proceeding ... *shall* be deemed an action against the United States ... and the United States *shall* be substituted as the party defendant." 28 U.S.C. § 2679(d)(1) (emphasis supplied).

The Federal Defendants argue further that once the United States has been substituted, the PTSA claim "must be dismissed as to the government as well" because " '[u]pon certification, any action or proceeding subject to' the Act 'shall proceed in the same manner as any action against the United States filed pursuant to' the FTCA 'and shall be subject to the limitations and exceptions applicable

to those actions.' " *Defs.' Mot.* at 36 (quoting 28 U.S.C. § 2679(d)(4)). According to the Federal Defendants, Plaintiffs have not complied with the FTCA's requirement that the Plaintiffs must first present their claim in writing to the appropriate federal agency "and so their claim should be dismissed as to the United States for lack of subject matter jurisdiction." *Id.* (citing 28 U.S.C. § 2675(a)).

***31** Plaintiffs do not dispute that the Attorney General's designee has certified the Federal Defendants or that they have not complied with the FTCA's procedural requirements. *Pls.' Opp'n* at 67-71. Instead, their singular point of opposition is that "the Federal Defendants violated a host of criminal and civil laws that disqualify them for a certification under the Westfall Act" and thus "this Court should reject the certification outright." *Id.* at 69-71. While Plaintiffs are correct that the Court may review the certification, the proper inquiry is not whether the Federal Defendants' conduct broke the law, but whether they were acting within the scope of their employment. *See Davric*, 238 F.3d at 66 ("In order to strike the substitution of the United States, plaintiffs here must show that ... [the defendant] was acting outside the scope of his employment at the time of the incident out of which the claims arose").

"Where a plaintiff asserts that a defendant acted outside the scope of his or her employment despite the Attorney General's certification to the contrary, the burden of proof

is on the plaintiff" and "State law controls the determination of whether a federal employee was acting within the scope of employment." *Id.* (citations omitted). Under Puerto Rico law, courts:

> [M]ust consider the following three elements in deciding whether to impose liability under the doctrine of respondeat superior consistent with Puerto Rico law: an employee's a) [d]esire to serve, benefit, or further his employer's business or interest[;] b) [whether] the act is reasonably related to the scope of the employment[; and] c) [whether] the agent has not been prompted by purely personal motives. Among these elements, [t]he fundamental consideration for determination of an employer's liability is whether or not the employee's acts fall within the scope of his employment in the sense that they furthered a desire to serve and benefit the employer's interest, resulting in an economic benefit to the employer. *Vernet v. Serrano-Torres*, 566 F.3d 254, 261 (1st Cir. 2009) (alterations in original) (citations and internal quotation marks omitted).

Plaintiffs allege that the Federal Defendants should not be certified because they lied on the search warrant applications, shared seized information with the DISH/NagraStar Defendants, allowed the DISH/NagraStar Defendants to accompany them during the search, and their entire criminal investigation was

"nothing more than a ruse" to steal Plaintiffs' intellectual property. *Pls.' Opp'n* at 69-71 (quoting *Second Am. Compl.* ¶ 4). The Federal Defendants counter that "[t]he allegations in this case involve actions the Federal Defendants took in furtherance of their investigative or prosecutorial duties on the United States' behalf" and that the "criminal investigation, including the execution of search warrants and the seizure of evidence at the plaintiffs' business properties ... furthered the employer's business interest, which includes the investigation and prosecution of federal crimes." *Defs.' Reply* at 22 (citations and internal quotations omitted).

The Court agrees with the Federal Defendants. For Plaintiffs to establish conduct outside the scope of employment, they would need to offer well-pleaded facts alleging that the entire investigation was truly a ruse created for the purpose of stealing their intellectual property (or, at least primarily motivated by that improper purpose). Such allegations would establish that the Federal Defendants were not acting in their employer's interest of investigating possible criminal activity. As the Court has explained, however, Plaintiffs' allegations on this point—which offer little detail and no motive for the Federal Defendants to conspire with one private company against another—are too conclusory to support their claims.

Plaintiffs have not met their burden to show that, despite

the Attorney General's certification, the Federal Defendants acted outside the scope of their employment. The Court will thus not reverse the substitution and the United States now stands in their shoes.

***32** "Section 2675 [of the FTCA] requires that the potential plaintiff give notice to the government of the nature of the claim and the damages requested" and "[f]ailure to timely file an administrative claim with the appropriate federal agency results in dismissal of the plaintiff's claim, since the filing of an administrative claim is a non-waivable jurisdictional requirement." *Santiago-Ramirez v. Sec'y of Dep't of Def.*, 984 F.2d 16, 18 (1st Cir. 1993) (citations omitted). Plaintiffs do not allege that they have provided notice, nor do they dispute the Federal Defendants' contention that—assuming the substation holds—this defect requires dismissal. For the reasons stated in *Santiago-Ramirez*, Plaintiffs' PTSA claim must be dismissed for lack of subject matter jurisdiction.

VI. CONCLUSION

The Court GRANTS the Federal Defendants' Motion to Dismiss (ECF No. 138). The Court DISMISSES Counts I-VII of Plaintiffs' Second Amended Complaint (ECF No. 130) as pleaded against the Federal Defendants.

SO ORDERED.

All Citations

Not Reported in Fed. Supp., 2024 WL 1363781

Footnotes

1 This is the second lawsuit arising out of the underlying events at issue. On August 25, 2020, a group of plaintiffs, including many of Plaintiffs here, filed a *Bivens* action against many of the same defendants. *See Quinones-Pimentel v. Cannon*, No. 3:20-cv-01443-JAW, 2022 WL 826344, at *——— – ———, 2022 U.S. Dist. LEXIS 48109 at *2-3 (D.P.R. Mar. 17, 2022). On March 17, 2022, the Court dismissed the *Bivens* action. *Id.* at *88. The plaintiffs appealed, and the Court of Appeals for the First Circuit affirmed the Court's dismissal on October 27, 2023. *Quinones-Pimentel v. Cannon*, 85 F.4th 63, 66-68 (1st Cir. 2023).

2 In their Second Amended Complaint, Plaintiffs use the spelling, "Rinkle." *See, e.g.*, *Second Am. Compl.* ¶

43. In their filings, however, the DISH/NagraStar Defendants use the spelling, "Rinkel." *See, e.g.*, *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Mot. to Dismiss* at 1 (ECF No. 134). No doubt, Ms. Rinkel knows how to spell her own name, and the Court uses "Rinkel" throughout this order.

3 Consistent with Federal Rule of Civil Procedure 12(b)(6), in describing the facts, the Court has relied upon the allegations in the Second Amended Complaint. *Foley v. Wells Fargo Bank, N.A.*, 772 F.3d 63, 68 (1st Cir. 2014); *Medina-Velázquez v. Hernández-Gregorat*, 767 F.3d 103, 108 (1st Cir. 2014) ("We examine whether the operative

complaint states a claim for which relief can be granted when we construe the well-pleaded facts in the light most favorable to the plaintiffs, accepting their truth and drawing all reasonable inferences in plaintiffs' favor" (internal citation omitted)).

4 Presumably because Claro Puerto Rico is a well-known business in Puerto Rico, the Second Amended Complaint does not describe Claro Puerto Rico except by name. *See Second Am. Compl.* ¶ 68. According to Wikipedia, Claro Puerto Rico is the one of the largest telecommunications companies in Puerto Rico. *See Claro P.R.*, WIKIPEDIA (updated Oct. 14, 2023), *https://en.Wikipedia.org/wiki/Claro_Puerto_Rico.*

5 Plaintiffs often refer in the Second Amended Complaint to the "Association in Fact defendants." *See, e.g., Second Am. Compl.* ¶ 87. As the Court interprets Plaintiffs' complaint, this term refers to all Defendants collectively. *See id.* ¶¶ 17, 62 (listing all the Defendants as together "form[ing] an Association in Fact").

6 Here, the Court quotes the text in the Second Amended Complaint. *Second Am. Compl.* ¶ 103. In the context of this sentence, the meaning of the verb, "counted," is unclear. It would make more sense if the sentence used "complied with," rather than "counted." Whichever verb is correct, however, makes no difference in the Court's ruling on the motion to dismiss.

7 Plaintiffs also argue that sovereign immunity does not apply to their RICO claims, although the Federal Defendants did not invoke sovereign immunity in their motion to dismiss. *Pls.' Opp'n* at 15-16. They submit that their claims "were not brought against the United States, but against specific federal official/agent[ ] defendants, in their individual and personal capacities, for criminal actions indictable under RICO, falling outside their scope of employment, and beyond their statutory authority," and thus Plaintiffs "are allowed to prosecute under equitable civil remedies of the United States laws." *Id.* at 16.

8 It is also not clear from the Second Amended Complaint how the

USAO Defendants would have learned that the information in the affidavits was false. Merely alleging that the USAO Defendants had this knowledge due to their participation in the conspiracy, as Plaintiffs appear to have done, is conclusory.

9 The statutory provision cited by Plaintiffs—18 U.S.C. § 1836—discusses civil proceedings for misappropriation of trade secrets and is not listed as a predicate act in 18 U.S.C. § 1961(1). Since the Court assumes Plaintiffs' reference to 18 U.S.C. § 1836 was in error, the Court has recharacterized their predicate-act allegations relating to theft of trade secrets as arising under 18 U.S.C. §§ 1831 and 1832.

10 In theory, Mr. Jaczewski could have provided an address that was entirely made up. This seems unlikely, however, in light of the Second Amended Complaint's allegations that the Defendants used the set-top boxes to attempt remote attacks on Naicom's servers. Had the boxes been shipped to an address that didn't exist, they would have been returned to Naicom as undeliverable, meaning that the Defendants could not have used them to launch sniffing attacks.

11 To the contrary, in the Second Amended Complaint, Plaintiffs include a table listing all the payments made to Naicom by Mr. Jaczewski posing as Brian Parsons. *Second Am. Compl.* ¶ 136. In the Court's view, these payments confirm that the credit card number provided by Mr. Jaczewski was valid.

12 These factors are:

(1) "concerns about proof" because "the less direct an injury is, the more difficult it becomes to ascertain the amount of a plaintiff's damages attributable to the violation, as distinct from other, independent, factors," ... (2) "concerns about administrability and the avoidance of multiple recoveries," ... and (3) "the societal interest in deterring illegal conduct and whether that interest would be served in a particular case[.]"

Sterling Suffolk Racecourse, 990 F.3d at 35-36 (quoting *Neurontin*,

712 F.3d at 35-36).

13 Regardless, most of these allegations appear to be incorporated in the allegations related to the search warrants. For example, it is unclear what Plaintiffs are referring to in alleging that the Federal Defendants "copied, duplicated, [and] downloaded" their confidential information aside from the allegations relating to the search warrant execution. *Second Am. Compl.* ¶ 139.

14 Apart from their general contention that the investigation was a hoax invented to steal their intellectual property, Plaintiffs have provided no support for this latter assertion. As noted above, it is equally plausible

—if not more so—that the FBI was looking for evidence as part of a legitimate criminal investigation.

15 The "reasonable continuation rule" requires the satisfaction of two conditions: 1) "the subsequent entry must indeed be a continuation of the original search, and not a new and separate search"; and 2) "the decision to conduct a second entry to continue the search must be reasonable under the totality of the circumstances." *Keszthelyi*, 308 F.3d at 569.

16 The closest Plaintiffs come to a nonconclusory allegation is their assertion that U.S. Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned, after the execution of the first search warrant, that Naicom complied with "all the programming distribution contract and agreements." *Second Am. Compl.* ¶

103. But this allegation is still conclusory, and it is undercut by the sentence immediately following it, which alleges that the USAO Defendants instructed S/A Pearson "to order Darwin Quinones and Victor Vega to report to the FBI Offices in San Juan with the

licensing contracts for an interview regarding Naicom's company." *Id.* Clearly, whatever U.S Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned did not absolve Naicom of wrongdoing; otherwise, there would have been no need to conduct an interview.

17 Further, "the statute offers no express direction as to when the government should seek a warrant versus" a SCA order." *Taylor*, 54 F.4th at 804.

18 Plaintiffs quote *Bellville v. Town of Northboro*, 375 F.3d 25 (1st Cir. 2004), for the proposition that "it might be a better practice, if circumstances permit, for law enforcement officers to disclose to the magistrate that civilians will be involved in the execution of the search and for the warrant to indicate that the magistrate permitted this involvement." *Pls.' Opp'n* at 40 (footnotes omitted) (quoting *Bellville*, 375 F.3d at 33-34). They fail to quote the preceding sentence, which states, "we will not improvise a rule that seems unnecessary in light of the overarching requirement that the use of civilians in the execution of a search must still meet the constitutional standard of reasonableness." *Bellville*, 375 F.3d at 33. The Court declines to accept Plaintiffs' invitation to convert the best practice outlined by the First Circuit into a rule.

2024 WL 1363772
Only the Westlaw citation is currently available. United States District Court, D. Puerto Rico.

NAICOM CORPORATION, et al., Plaintiffs,

v.

DISH NETWORK CORPORATION, et al., Defendants.

No. 3:21-cv-01405-JAW
|
Signed March 29, 2024

Attorneys and Law Firms

Rafael F. Castro-Lang, Castro & Castro Law Office, San Juan, PR, for Plaintiffs.

Chad M. Hagan, Pro Hac Vice, Timothy Frank, Pro Hac Vice, Hagan Noll & Boyle LLC, Houston, TX, Jose L. Ramirez-Coll, Antonetti Montalvo & Ramirez-Coll, San Juan, PR, Carolina V. Cabrera-Bou, Amrc, LLC, San Juan, PR, for Defendants Dish Network Corporation, DISH Network L.L.C., NagraStar LLC, Bert Eichhorn, Emily Rinkle, Jordan Smith, Kevin Gedeon, Michael Thomas Jaczewski.

Patrick B. Fenior, DOJ-Civ, Washington, DC, Priscila M. Acevedo-Roman, U.S. Attorney's Office for the District of Puerto Rico, San Juan, PR, for Defendants United States Attorney for the District of Puerto Rico, Rosa Emilia Rodriguez-Velez, Jose Capo, Nicholas W. Cannon, Federal Bureau of Investigations San Juan Field in Puerto Rico, Douglas A. Leff, Bradely Rex, Lance Lange, Clay Rehrig,

Juan Galarza, Jason Lopez, Kevin Pearson, United States Attorney's Office.
Jose L. Ramirez-Coll, Antonetti Montalvo & Ramirez-Coll, San Juan, PR, Carolina V. Cabrera-Bou, Amrc, LLC, San Juan, PR, for Defendant Toltec Investigations, LLC.

ORDER ON THE TOLTEC DEFENDANTS' MOTION TO DISMISS

JOHN A. WOODCOCK, JR., UNITED STATES DISTRICT JUDGE

***1** A limited liability company and its chief executive officer file a motion to dismiss plaintiffs' seven-count complaint, arising out of a criminal investigation wherein the defendants assisted federal law enforcement. The Court grants the motion to dismiss, dismissing all seven counts. The Court dismisses plaintiffs' RICO claims because plaintiffs have not adequately pleaded the existence of an enterprise, a pattern of racketeering activity, or a conspiracy. The Court dismisses plaintiffs' Defend Trade Secrets Act claim because, taking plaintiffs' allegations as true, the private parties' assistance to law enforcement fell within the statutory exception for authorized law enforcement activity. Finally, the Court dismisses plaintiffs' Computer Fraud and Abuse Act claim, Stored Communications Act claim, Digital Millennium Copyright Act claim, and Puerto Rico Uniform Trade Secrets Act claim because plaintiffs have not adequately

alleged that these particular defendants are liable for the alleged statutory violations.

I. PROCEDURAL HISTORY

On August 27, 2021, Naicom Corporation, D&V IP Holdings, LLC, Paylink, LLC, and Kiaras, LLC, filed a seven-count complaint against approximately twenty known Defendants and two dozen unknown Defendants. [1] *Compl.* (ECF No. 1). The Court has twice permitted Plaintiffs to amend their complaint, and the Second Amended Complaint is now the operative complaint. *Am. Compl.* (ECF No. 100); *Second Am. Compl.* (ECF No. 130).

The parties categorize the numerous Defendants into four groups: 1) DISH Network LLC, NagraStar LLC, Bert Eichhorn, Emily Rinkel, [2] Jordan Smith, and Kevin Gedeon (the DISH/NagraStar Defendants); 2) DISH Network Corporation (DISH Corp. or DNC); 3) Toltec Investigations, LLC and its President and CEO, Michael Thomas Jaczewski (the Toltec Defendants); and, 4) former U.S. Attorney Rosa E. Rodriguez-Velez, former Assistant U.S. Attorney Jose Capo-Iriarte, Assistant U.S. Attorney Nicholas W. Cannon (the USAO Defendants) and Special Agents and employees of the Federal Bureau of Investigation Douglas Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, and Jason Lopez (the FBI Defendants)

(collectively, the Federal Defendants).

***2** Plaintiffs allege: (1) violations of the Racketeer Influenced and Corrupt Organizations Act (RICO); (2) a RICO conspiracy; (3) violations of the Computer Fraud and Abuse Act (CFAA); (4) violations of the Stored Communications Act (SCA); (5) violations of the Digital Millennium Copyright Act (DMCA); (6) violations of the Defend Trade Secrets Act (DTSA) by misappropriation of trade secrets; and (7) violations of the Puerto Rico Industrial and Trade Secrets Protection Act (PTSA) under the Uniform Trade Secrets Act (Law No. 80). *Second Am. Compl.* ¶¶ 124-202.

On October 31 and November 1, 2022, each of the four groups of Defendants filed a motion to dismiss the complaint. *Defs.' Toltec Investigations, L.L.C. and Mike Jaczewski's Mot. to Dismiss* (ECF No. 137) (*Defs.' Mot.*); *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Mot. to Dismiss* (ECF No. 134) (*DISH/NagraStar Mot.*)*; Def. DISH Network Corp.'s Mot. to Dismiss* (ECF No. 136); *Fed. Defs.' Mot. to Dismiss* (ECF No. 138).

On December 5, 2022, Plaintiffs filed a response to the DISH/NagraStar Defendants' motion to dismiss. *Mot. in Resp. to Dish/NagraStar Defs.' Mot. to Dismiss* (ECF No. 147) (*Pls.' Opp'n to DISH/NagraStar Mot.*). On January 18, 2023, Plaintiffs responded to the Federal Defendants'

motion. *Mot. in Resp. to the Fed. Defs.' Mot. to Dismiss* (ECF No. 153). On February 21, 2023, the Toltec Defendants withdrew a section of their motion to dismiss, *Unopposed Notice of Partial Withdrawal of Toltec Investigations L.L.C. and Mike Jaczewski's 12(b)(2) Mot. to Dismiss* (ECF No. 163), and on February 27, 2023, Plaintiffs responded to the remainder of the Toltec Defendants' motion. *Mot. in Resp. to Toltec Investigations and Mike Jaczewski's Mot. to Dismiss* (ECF No. 167) (*Pls.' Opp'n*). On March 17, 2023, Plaintiffs responded to DISH Corp.'s motion. *Mot. in Resp. to Dish Network Corp.'s Mot. to Dismiss* (ECF No. 179).

Each group of Defendants filed a reply in support of its motion. *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Reply* (ECF No. 164); *Fed. Defs.' Reply* (ECF No. 173); *Defs. Toltec Investigations L.L.C. and Michael Jaczewski's Reply in Supp. of Rule 12(b)(6) Mot. to Dismiss* (ECF No. 185) (*Defs.' Reply*); *DISH Network Corp.'s Reply in Supp. of Its Mot. to Dismiss* (ECF No. 196).

Finally, Plaintiffs filed sur-replies opposing each motion. *Sur-Reply to the Dish Network, LLC and NagraStar, LLC Reply Mot. to Pls.' Resp. to Defs.' Mot. to Dismiss SAC* (ECF No. 182); *Sur-Reply Mot. to Fed. Defs.' Reply Mot. to Pls.' Resp. to Fed. Defs.' Mot. to Dismiss, SAC* (ECF

No. 190); *Sur-Reply Mot. to the Toltec Investigations L.L.C. and Michael Jaczewski's Reply Mot. to Pls.' Resp. to Their Mot. to Dismiss SAC* (ECF No. 195) (*Pls.' Sur-Reply*); *Sur-Reply Mot. to Dish Network Corp.'s Reply Mot. to Pls.' Resp. to Mot. to Dismiss SAC* (ECF No. 199).

II. FACTS [3]

A. The Parties

***3** In 2015 and 2016, Darwin Quinones-Pimentel and Victor Vega-Encarnacion founded Naicom Corporation (Naicom) and D&V IP Holdings, LLC (D&V) to offer Internet Protocol Television (IPTV) services. The companies are structured such that D&V holds the proprietary "intellectual technology" created by Mr. Quinones, and Naicom licenses the technology from D&V to distribute television programming. *Second Am. Compl.* ¶ 63. Kiaras, LLC (Kiaras) and Paylink, LLC (Paylink) are also joint ventures operated by Mr. Quinones and Mr. Vega. *Id.* ¶ 14. Kiaras is a human resources and time-and-attendance management company, and Paylink is a payroll processing company. *Id.* Both Kiaras and Paylink operate on the "PAYLINK AND KIARAS Cloud Network," another proprietary intellectual technology creation of Mr. Quinones. *Id.* ¶¶ 5-6. All four companies are corporations existing under the laws of the commonwealth of Puerto Rico with their places of business located at Building Centro de Seguros,

701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907. *Id.* ¶¶ 33-36.

DISH Network Corporation (DISH Corp.) was organized in 1995 as a corporation under the laws of the State of Nevada, started offering the DISH® branded pay-tv service in March 1996, and is the nation's third largest pay-tv provider. *Id.* ¶ 37. DISH Network LLC (DISH LLC) was organized in 1987 as a Limited Liability Corporation under the laws of the state of Colorado. *Id.* ¶ 38.

NagraStar, LLC (NagraStar) is a joint venture between DISH Corp. and Kudelski SA formed in 1998. *Id.* ¶ 39. NagraStar's focus is delivering and maintaining security solutions for satellite and Internet-based television systems and other connectivity initiatives in North America, and their mission also includes anti-piracy investigations and cooperation with law enforcement agencies. *Id.* Jordan Smith was at all relevant times a Manager of Field Security & Investigations and Senior Anti-Piracy Investigator for NagraStar. *Id.* ¶ 41. Bert Eichhorn and Emily Rinkel were Managers of Field Security & Investigations for NagraStar. *Id.* ¶¶ 42-43. Kevin Gedeon was a Manager of Fraud Investigations for NagraStar. *Id.* ¶ 44.

Toltec Investigations, LLC (Toltec) is a private investigative agency specializing in investigating the technology and distribution involved in IPTV systems, copyrights, patents, and "Trademark and Brand's Intellectual Property." *Id.* ¶ 40. Michael Thomas

Jaczewski, a.k.a. Brian Parsons, was at all relevant times President and Chief Executive Officer of Toltec. *Id.* ¶ 45.

Rosa Emilia Rodriguez-Velez was at all relevant times the United States Attorney for the District of Puerto Rico. *Id.* ¶ 46.

Jose Capo-Iriarte was an Assistant U.S Attorney (AUSA) and head of the office's Criminal Division. *Id.* ¶ 47. Nicholas Cannon was an AUSA and Deputy Chief of the Cybercrimes Division. *Id.* ¶ 48.

Douglas Leff was at all relevant times Special Agent in Charge of the FBI's San Juan Division. *Id.* ¶ 49. Also in that division, Brad Rex was a Supervisory Special Agent, Lance Lange, Kevin Pearson, and Clay Rehrig were Special Agents, Juan Galarza a Computer Science Officer, and Jason Lopez an Evidence Technician. *Id.* ¶¶ 50-55.

B. Naicom's Origins

Between 2002 and 2012, Mr. Quinones developed the intellectual technology, including the source code, underpinning the Paylink and Kiaras Cloud Workforce Management system and Naicom's IPTV services. *Id.* ¶ 5. The proprietary IPTV system was characterized as a Dynamic Internet Semantic Multicast Environment (DISME), which "enabled for the first time the broadcast of media via private networks and the internet, a new

concept of IPTV service to distribute Live-Video Television Content (media) to residences, business, and primes customers." *Id.* ¶¶ 8-11.

By 2016, Mr. Quinones had completed all DISME technology alpha and beta tests and, alongside Mr. Vega, founded Naicom. *Id.* ¶ 12. Naicom is a network and internet communication platform that delivers live television, video on-demand content, internet, and wireless network services to subscribers worldwide. *Id.* Naicom also provides instant access to television shows, movies, and music/videos on-demand, and live sports and music events through Naicom's set-top box using IPTV and TV Everywhere (TVE) on any mobile device. *Id.*

***4** Mr. Quinones and Mr. Vega registered Naicom as a closed corporation with the State Department of Puerto Rico and complied with all requirements as a legitimate IPTV business. *Id.* ¶ 66. Naicom also requested to manufacture its own brand of set-top boxes for end users through Informir LLC and acquired the programing licenses to distribute on-demand content in the United States, Puerto Rico, and the U.S. Virgin Islands through worldwide television network companies. *Id.* ¶¶ 67-68. In 2017, Naicom became a member of the National Rural Telecommunications Cooperative (NRTC). *Id.* ¶ 68.

On January 6, 2017, Naicom submitted a request to the Apple Corporation to have its TV App added to

Apple's AppStore. *Id.* ¶ 69. Apple's legal department requested that Naicom produce all licenses authorizing the distribution of programming to Naicom's subscribers via Naicom's TV App. *Id.* On February 16, 2017, Apple approved Naicom's App for inclusion in the Apple AppStore. *Id.* ¶ 70. In December 2017, Sam's Club approved Naicom to launch and distribute Naicom's IPTV set-top box in their retail stores. *Id.* ¶ 71.

C. Naicom's Information Security

Naicom went to great lengths to protect its intellectual technology. *Id.* ¶¶ 64-65. D&V and Naicom developed significant amounts of confidential and proprietary information, including non-public information relating to the DISME's source codes, patterns, formulas, algorithms, methods, and techniques; the technological vision for Naicom's IPTV content, distribution, marketing, servicing, research and development efforts and strategies; business and marketing performance strategies; financial data and business plans; technical data; customer development management programs; and subcontractor and vendor relationships (collectively, with the DISME, the Confidential Information or Naicom's Confidential Information). *Id.* ¶ 64.

To protect this information, Plaintiffs only installed on their servers, located at the Naicom's Data Center Facility, what is known as a compiled executable. *Id.* ¶

65. The entire system was installed with an operating system that allowed the hard drive to be encrypted and, to access the servers, an authorized employee would need to enter the secure data facility and provide a username and password. *Id.* The server is not exposed to the internet and could only be accessed from inside the facility. *Id.* The Confidential Information was also downloaded onto a hard disk and kept in a safe box. *Id.*

Plaintiff companies took additional steps to safeguard their confidential information and proprietary data, including restricting employee access, requiring employees to execute non-disclosure agreements, imposing restrictions on remote access, and implementing encryption. *Id.* ¶¶ 72-76.

D. Negotiations with Claro Puerto Rico

In 2017, Naicom entered into negotiations with Claro Puerto Rico [4] (Claro) to distribute Naicom set-top boxes to Claro customers. *Id.* ¶ 77. Claro represented to Naicom that it had approximately 320,000 internet subscribers who received only five megabytes and thus could not subscribe to Claro's IPTV services, which required sixty megabytes to upload programming. *Id.* ¶ 78. During negotiations, Naicom and Claro entered into a mutual non-disclosure agreement prior to discussing and analyzing business information and the contents of the resellers' agreement. *Id.* ¶ 79. Claro's Product

Development Officer, Anibal Rios, projected that the Claro-Naicom business alliance would bring in over $10,000,000 in monthly gross revenue for the first year and over $13,000,000 for the second year only taking into account Claro's corporate and residential subscribers in Puerto Rico. *Id.* ¶ 80. Naicom projected that the Claro-Naicom alliance would add 100,000 new corporate subscribers, plus another 150,000 residential subscribers, bringing in projected monthly gross sales of $9,000,000 in the first year and $12,000,000 in the second year. *Id.* ¶ 81.

***5** Claro had an existing contract with DISH Network Satellite TV, whereby DISH Network provided TV programming to Claro's internet subscribers who could not subscribe to Claro's IPTV services. *Id.* ¶ 82. The Naicom deal represented a cancellation threat to DISH Network's contract with Claro. *Id.* Claro was also considering shutting down its IPTV business division due to loss of revenue. *Id.* During the negotiations for the Claro-Naicom deal, Carlos Garcia, Claro's IPTV business manager, became privy to information that the Claro-Naicom deal would leave him jobless if Claro opted to shut down its IPTV division, which he managed. *Id.* ¶ 83. Mr. Garcia alerted DISH Network that the Claro-Naicom IPTV deal would lead to cancellation of the DISH contract with Claro, which the Plaintiffs allege led to "great animosity" between DISH Network and Naicom. *Id.*

¶ 84. On August 14, 2018, after a year of meetings between Naicom and Claro, Claro pulled out of negotiations without notice. *Id.* ¶ 85. Plaintiffs believe the DISH Network Defendants advised Claro to withdraw because the FBI was investigating Naicom and its founders. *Id.* ¶ 86.

E. The DISH Network Investigation

On August 7, 2017, the DISH/NagraStar and DISH Corp. Defendants instructed the Toltec Defendants to purchase two Naicom TV set-top-box receivers so that the Defendants [5] could reverse engineer Plaintiffs' intellectual technology. *Id.* ¶ 87. The Defendants conducted "sniffing" to determine the direction of Naicom TV traffic and locate Naicom's facility. *Id.* The Defendants also used sniffing to attack and penetrate Naicom's servers and computers, monitoring content and capturing information on the network under the supervision of the Federal Defendants. *Id.* One of the two set-top-box receivers was maintained by the DISH/NagraStar Defendants, the other by the Toltec Defendants. *Id.* ¶ 88. Both receivers were used for the attacks on Naicom's data center servers. *Id.*

Mr. Jaczewski purchased the two set-top boxes from Naicom under the false name of "Brian Parsons," and he provided false contact information. *Id.* ¶ 89. According to the Defendants, their investigation revealed that the

receiver provided access to approximately forty-three channels, including Disney, TBS, ESPN, CNN, HBO, Showtime, and Cinemax. *Id.* ¶ 90. The Defendants downloaded the Naicom TV App through the Apple AppStore, which provided access to approximately forty-two channels, and tested Naicom TV several times to determine whether it was providing DISH programming. *Id.* The tests revealed no DISH content. *Id.*

The Defendants also contacted several media companies to inquire into whether Naicom had the appropriate licensing contracts to distribute its programming. *Id.* ¶ 91. On each occasion, the investigators were informed that Naicom was authorized to distribute the network's content. *Id.* The investigators also discovered that Naicom's TV distribution technology was a threat to DISH Network and Sling TV, representing future competition for subscribers in Puerto Rico and the United States. *Id.* ¶ 92.

The DISH/NagraStar Defendants informed the other Defendants that they could not penetrate Naicom's Data Center computers and servers remotely, and thus direct, physical access would be required to extract Naicom's intellectual property. *Id.* ¶ 93. They knew that by entering the data center and shutting down the computers and servers, they would be able to bypass Naicom's security measures and access the internal hard drive. *Id.* ¶ 94.

According to Naicom, the Defendants knew that the intellectual property was extremely valuable and worth obtaining by any means necessary to advance their own television programming distribution system, and the Defendants conspired to misappropriate the technology for economic advantage. *Id.* ¶ 95.

***6** The DISH/NagraStar Defendants thereafter filed a complaint with the Federal Defendants alleging that Naicom was running an IPTV pirate operation. *Id.* ¶ 98. Plaintiffs allege that the motive behind the complaint was to secure NagraStar and DISH Network's participation in a search of Naicom's Data Center and the seizure of Naicom's computers, servers, and other hardware containing Naicom's intellectual property and trade secrets, under the ruse of assisting the Federal Defendants in discovering incriminating evidence. *Id.* Acquiring this information has given the DISH/NagraStar Defendants a competitive advantage over Naicom. *Id.* ¶ 99.

F. Execution of the Search Warrants

1. The First Search of Naicom's Data Center

On August 27, 2019, the Federal Defendants applied for two search warrants: one for Naicom Corporation located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907, and the other for

Naicom's Data Center located at Villa Fontana, 4SS N2 Via Josefina, Carolina, Puerto Rico. *Id.* ¶¶ 19, 33, 105. Plaintiffs allege that the search warrants were "issued under illegal and unlawful means" because the Federal Defendants provided affidavits they knew to contain false and perjured information. *Id.* ¶ 20.

On August 27, 2019, the Federal and DISH/NagraStar Defendants executed the warrants, with the DISH/NagraStar Defendants "acting as federal agents." *Id.* ¶ 21. They seized documents, hard drives, and thumb drives, and downloaded data from the computers and servers containing Plaintiffs' Confidential Information. *Id.* Plaintiffs allege that the Defendants knew from their investigation prior to the searches that Naicom was authorized to distribute its programming and was not pirating content. *Id.* ¶ 101. The Defendants also allegedly knew that the evidence collected in the Federal Defendants' investigative files "negated any criminal wrongdoing that Naicom's founders were committing the crimes charged in the search and seizure warrant affidavit and application." *Id.* ¶ 102.

At the conclusion of the August 27, 2019 search, the Federal Defendants "learned that Naicom TV counted with all the programming distribution contract and agreements" [6] and instructed Mr. Quinones and Mr. Vega to report to the FBI offices with their licensing contracts for an interview. *Id.* ¶ 103. This interview took

place with the Federal Defendants sitting at one table and the DISH/NagraStar Defendants sitting at another table, allegedly posing as federal agents. *Id.* ¶ 104. The Defendants questioned Mr. Quinones about how Naicom acquired the IPTV distribution contracts and the technology used to distribute the programing. *Id.* They also inspected Naicom's contracts with content providers, which contained trade/business secrets and confidential information regarding DISME technology. *Id.*

2. The Second Search of Naicom's Data Center

On August 29, 2019, U.S. Attorney Rodriguez-Velez and AUSAs Capo-Iriarte and Cannon instructed FBI Agents Lange and Pearson to return to Naicom's data center with DISH/NagraStar Defendants Smith, Gedeon, and Eichhorn. *Id.* ¶ 105. Naicom alleges that the USAO Defendants ordered this search despite knowing beforehand that Naicom was a legitimate business and there was no probable cause for continued investigation. *Id.* Without obtaining new warrants, Defendants again entered Naicom's data center facility, performed password resets, and installed "pen drives and other electronic instruments" to bypass security measures and download and seize Naicom's Confidential Information. *Id.* ¶¶ 22, 106. The agents used keys taken from Naicom's offices to enter Naicom's data center. *Id.* ¶ 105.

***7** During the search, Agent Pearson contacted Naicom employee Jaime Echevarria and ordered him to come to

the Data Center, as Agent Pearson wanted to speak with him, Mr. Quinones, and Mr. Vega. *Id.* ¶ 107. Upon arriving at the Data Center, Mr. Quinones observed Agents Lange and Pearson allowing Mr. Smith, Mr. Gedeon, and Mr. Eichhorn to access Naicom's Data Center computers, servers, and other hardware equipment without authorization from Naicom. *Id.* ¶ 108.

During the search, Agents Pearson and Lange pressured Mr. Quinones to sign a hold-harmless document accepting that he had run a pirate operation in the past so that they could close the case. *Id.* ¶ 109. Otherwise, they threatened that they would shut down the Data Center operation. *Id.* Mr. Quinones refused, despite Agents Pearson and Lange imploring him to sign the document. *Id.* ¶ 110.

Sometime thereafter, Mr. Vega arrived and, upon entering the Data Center, asked Agents Pearson and Lange if they had another search warrant to enter and search the Data Center. *Id.* ¶ 111. Agent Lange represented to Mr. Vega that the search warrant gave him ten days to come in and out and search the Data Center. *Id.* Mr. Vega told Agent Lange that Agent Lange was violating the United States Constitution and Federal law. *Id.*

Mr. Vega thereafter informed Agents Pearson and Lange that he had discovered via LinkedIn that the alleged FBI

experts who executed the search and interrogated Mr. Quinones and him at the FBI offices were Kevin Gedeon, investigator for DISH Network, and Jordan Smith, Bert Eichhorn, and Emily Rinkel, investigators for NagraStar. *Id.* ¶ 112. Mr. Vega questioned Agents Lange and Pearson as to why the FBI brought in his competition to search, inspect, and photograph private documents and allowed them access to computers and servers containing trade secrets, code sources, and business and intellectual property belonging to Naicom. *Id.* ¶ 113. Mr. Vega called his attorney and told him about the second search. *Id.* ¶ 114. After speaking with Agent Lange, the FBI agents and DISH/NagraStar investigators shut down Naicom's business operation and left the premises. *Id.*

G. The Demand for the Return of Property Under Rule 41(g)

On September 6, 2019, the Plaintiffs filed a motion to demand the return of seized property under Rule 41(g) of the Federal Rules of Criminal Procedure. *Id.* ¶ 115. The District Court granted the Plaintiffs' Rule 41(g) motion on November 5, 2019, noting that the Government had waived objections to the court's Report & Recommendation. *Id.* ¶¶ 116-17.

H. The Plaintiffs' Alleged Harm

The Plaintiffs allege that the criminal investigation

caused significant damage to their business reputation and unfairly enriched their competitors. *Id.* ¶¶ 118-19. They allege that prior to the execution of the search warrants, they had a great reputation and were about to close on a $15,000,000 investment deal, but investors pulled out upon learning Naicom was under criminal investigation. *Id.* ¶¶ 120-21. The Plaintiffs also allege that Naicom was about to close a multimillion-dollar deal with Claro when Claro learned of the FBI's investigation and pulled out of negotiations. *Id.* ¶ 122. The Plaintiffs say they have lost subscribers because of negative publicity resulting from the investigation and that the Defendants' intrusion into Naicom's Data Center computers, servers, and equipment caused damage leaving subscribers without tv programming services for several weeks and cost more than $500,000 to repair. *Id.* ¶ 123.

I. The Plaintiffs' Causes of Action

***8** The Plaintiffs bring seven counts. Count One alleges that the Defendants violated RICO by forming an association in fact to advance the criminal objective of stealing Plaintiffs' intellectual property and trade secrets by committing mail and wire fraud, among other crimes. *Id.* ¶¶ 124-53.

Count Two alleges that the Defendants engaged in a RICO conspiracy by conspiring to plan and execute the scheme outlined in Count One. *Id.* ¶¶ 154-57.

Count Three alleges that the Defendants violated the CFAA by accessing Naicom's computer systems without authorization or in excess of authorization and obtaining and using valuable information from those computers. *Id.* ¶¶ 158-68.

Count Four alleges that the Defendants violated the SCA by "willfully and intentionally access[ing] without authorization a facility which operates servers, encoders, computers, and telecommunications systems and technology, by electronically transmitting communications involved in Webservers, Email-Servers, Carrier Grade Routers which interconnected with local ISP providers through Border Gateway Protocols (BGP) in exchanging routing information between autonomous systems." *Id.* ¶¶ 169-75.

Count Five alleges that the Defendants violated the DMCA by illegally obtaining Plaintiffs' copyright-protected software programs, documents, confidential information, and research. *Id.* ¶¶ 176-84.

Count Six alleges that the Defendants violated the DTSA by stealing Plaintiffs' trade secrets, including DISME technology, intellectual property, and other confidential information. *Id.* ¶¶ 185-94.

Finally, Count Seven alleges that the Defendants misappropriated Plaintiffs' trade secrets in violation the

PTSA. *Id.* ¶¶ 195-202.

III. THE PARTIES' POSITIONS

A. The Toltec Defendants' Motion to Dismiss [7]

The Toltec Defendants initially argue that "Plaintiffs cannot plead a viable RICO claim on the facts" because "Plaintiffs' RICO allegations consist solely of boilerplate and conclusory language," and they "cannot plead a viable RICO enterprise on the facts." *Defs.' Mot.* at 12 (capitalization altered).

The Toltec Defendants submit that "Plaintiffs do not (and cannot) allege a RICO enterprise involving the Toltec Defendants with an ongoing organization, devoted to a common illicit purpose, unrelated to legitimate law enforcement activity, that functioned as a continuing unit separate and apart from the pattern of racketeering activities alleged in this case." *Id.* at 15.

***9** In support, the Toltec Defendants aver that they "were not parties to the searches and seizure conducted in August 2019 and are not subject to liability for merely assisting or performing a service for the alleged enterprise." *Id.* Further, they contend that "Toltec's online purchase of the Naicom IPTV set top boxes and related subscription services using a pseudonym as part of an undercover federal investigation to detect pirated IPTV content is not mail or wire fraud." *Id.* Finally, they

note that "even when accepting Plaintiffs' allegations as true, the conduct they attribute to the Toltec Defendants was not in furtherance of some shared illicit purpose reminiscent of an enterprise, but rather was due to lawfully authorized investigative activity." *Id.* at 16.

The Toltec Defendants similarly argue that "Plaintiffs cannot plead the conduct of a criminal enterprise that is separate and apart from the conduct of Defendants' own affairs." *Id.* at 17 (capitalization altered). This is so, they continue, because "Plaintiffs fail to plead any factual allegations establishing how the Toltec Defendants took part in the 'operation or management' of the alleged RICO enterprise." *Id.* at 18 (quoting *Reves v. Ernst & Young*, 507 U.S. 170, 185, 113 S.Ct. 1163, 122 L.Ed.2d 525 (1993)).

Next, the Toltec Defendants contend that they "committed no predicate offenses," *id.* at 18 (capitalization altered), because each of the predicate acts alleged by Plaintiffs " '[is] supported by allegations of legitimate government action' and 'even when viewed in the inflammatory light bestowed upon them by Plaintiff[s], in no way resemble criminal activity." *Id.* at 19 (alterations in *Defs.' Mot.*) (quoting *Kahre v. Damm*, No. 2:07-CV-00231-DAE-RJJ, 2007 U.S. Dist. LEXIS 95978 at *26, 2007 WL 9728869 (D. Nev. Dec. 18, 2007)). The Toltec Defendants assert that "Plaintiffs do not (and cannot) plead" their mail and wire fraud allegations

"with the requisite specificity," and they reiterate that "it is undisputed that the Toltec Defendants did not participate in the execution of the search warrants." *Id.* at 20.

In a similar vein, the Toltec Defendants maintain that they "lacked the criminal intent to engage in 'racketeering activity,' " *id.* (capitalization altered), because "all actions undertaken by the Toltec Defendants were performed under color of federal law, and at the direction and supervision of the Federal Defendants to assist them in discharging certain governmental duties." *Id.*

Even if Plaintiffs could sufficiently allege one or more predicate acts, the Toltec Defendants continue, "Plaintiffs cannot plead an actionable pattern of racketeering activity on the facts." *Id.* at 21 (capitalization altered). According to the Toltec Defendants, "[w]hen, as here, a complaint explicitly presents a distinct and non-reoccurring scheme with a built-in termination point and provides no indication that the perpetrators have engaged or will engage in similar misconduct, the complaint does not sufficiently allege continuity for § 1962(c) purposes even if the purported scheme takes several years to unfold, involves a variety of criminal acts, and targets more than one victim." *Id.* at 22 (quoting *Gamboa v. Velez*, 457 F.3d 703, 708-09 (7th Cir. 2006)).

Turning to Plaintiffs' RICO conspiracy claim, the Toltec Defendants argue that this claim "fails for two independent reasons." *Id.* at 23. First, they submit that Plaintiffs' RICO conspiracy claim should be dismissed because "Plaintiffs have failed to allege an actionable substantive RICO claim." *Id.* Further, they aver that "Plaintiffs' allegations of agreement and conspiracy are too vague and conclusory to state a claim for relief and consist of ... formulaic recitations and conclusory allegations." *Id.* (internal quotations omitted).

The Toltec Defendants conclude their motion by incorporating by reference several arguments made by the Federal Defendants and the DISH/NagraStar Defendants. *Id.* at 23-24. They then ask the Court to dismiss Plaintiffs' claims with prejudice. *Id.* at 24.

B. Plaintiffs' Opposition

***10** In response, Plaintiffs first argue that "the procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Pls.' Opp'n* at 11 (capitalization altered). They contend that the Toltec Defendants helped procure search warrants containing "materially false representations and perjured testimony," which ultimately lacked probable cause. *Id.* at 12. Plaintiffs submit that "the alleged initial probable cause dissipated

with the first search warrant execution," and thus the second search was "illegal and warrantless." *Id.* at 16.

Plaintiffs go on to argue that "the affidavit in support of the search warrant was defective on its face." *Id.* at 17 (capitalization altered). They contend that their computer systems were protected under the SCA, that the "conclusory" statements in the affidavit were insufficient to justify a search, and that the search ultimately did not comply with the SCA. *Id.* at 18-22. According to Plaintiffs, the Federal Defendants did not "seek authorization from the Magistrate to bring Plaintiffs' competitors, the Dish/NagraStar [8] Defendants, to execute the search warrant," and although Plaintiffs concede that 18 U.S.C. § 3105 allows private parties to assist in the execution of a search warrant, they counter that "the statute clearly prohibited the executing officer from bringing to the search a party which had another interest, profit, or other marketplace incentive." *Id.* at 22. Further, Plaintiffs submit that the Toltec Defendants cannot rely on the search warrants because the Federal Defendants conceded the invalidity of the warrants when they did not oppose Plaintiffs' motion for return of property under Federal Rule of Criminal Procedure 41(g). *Id.* at 24-26.

Shifting gears, Plaintiffs contend that "the *Noerr-Pennington* doctrine does not apply to the case at bar." *Id.* at 26 (capitalization altered). This is so, they continue,

because the Toltec Defendants "knew that the Dish/NagraStar grievance was a sham, knowingly assisted and carried out by the Federal defendants in order to gain access to Plaintiffs' premises and deprive them of their intellectual and trade secret property." *Id.* at 29 (emphasis omitted). Plaintiffs assert that the *Noerr-Pennington* doctrine "does not protect 'objectively baseless' sham litigation." *Id.* at 29.

Plaintiffs next argue that sovereign immunity does not bar their RICO claims. *Id.* at 30-31. They submit that "the charges in this civil action were not brought against the United States, but against specific federal official/ agent[ ]/Dish/NagraStar and the Toltec Defendants, in their individual and personal capacities, for criminal actions indictable under RICO, falling outside their scope of employment, and beyond their statutory authority," and thus, "Plaintiffs are allowed to prosecute under equitable civil remedies of the United States laws." *Id.*

Turning to the elements of the RICO counts, Plaintiffs submit that they have "pleaded a colorable RICO claim on the facts," *id.* at 31 (capitalization altered), because they have pleaded "enough facts in the [Second Amended Complaint to give the] Toltec defendants a fair notice of what there is, and the grounds upon [which] they rest." *Id.* at 32. Plaintiffs add that they have also "pleaded a cognizable RICO enterprise on the facts." *Id.* at 33-35 (capitalization altered).

***11** Plaintiffs further maintain that they have sufficiently "pleaded conduct of a criminal enterprise that is separate and apart from the conduct of Defendants' own affairs." *Id.* at 35 (capitalization altered). In their view, the three required elements for establishing a RICO enterprise are: 1) "an ongoing organization, formal or informal"; 2) that "the various associate[s] function as a continuing unit"; and 3) that the enterprise exists "separate and apart from the pattern of activity in which it engages." *Id.* at 36 (quoting *United States v. Turkette*, 452 U.S. 576, 583, 101 S.Ct. 2524, 69 L.Ed.2d 246 (1981)). Plaintiffs assert that while they "will ultimately need to establish each of these factors, at this early juncture it is sufficient to merely [ ] allege the existence of an association-in-fact enterprise." *Id.* (quoting *Pappa v. Unum Life Ins. Co. of Am.*, No. 3:07-cv-0708, 2008 U.S. Dist. LEXIS 21500 at *29-30, 2008 WL 744820 (M.D. Pa. Mar. 18, 2008)). They add that it is reasonable to infer from the complaint that "the Association in Fact defendants functioned as a continuing unit and had an ascertainable structure distinct from that inherent in the conduct of a pattern of racketeering activity." *Id.* at 38.

Plaintiffs go on to argue that the "Toltec Defendants committed the predicate offense[s] and acted with criminal intent and in bad faith." *Id.* at 39 (capitalization altered). Plaintiffs emphasize that "the Toltec Defendants' mail and wire predicate acts are criminal and indictable."

Id. at 40 (capitalization altereted). They also maintain that, even if the Toltec Defendants' misrepresentations did not amount to mail or wire fraud, they nevertheless contributed to the Defendants' theft of trade secrets under 18 U.S.C. §§ 1831 and 1832. *Id.* at 40.

Plaintiffs then argue that they have "pleaded a pattern of racketeering activities on the facts," *id.* at 42 (capitalization altered), because they "pleaded that the Association in Fact defendants ... committed over 30 racketeering acts ranging from Mail and Wire fraud to theft of trade secrets, in a period of two years which began in July 2017 and ended in August[ ] 2019." *Id.* at 43. In their view, these facts "satisfied the closed period of repeated conduct," and there are also "allegations of a threat of continued activity, in reference to the Dish Network and NagraStar corporation joint venture." *Id.* at 43-44.

Finally, Plaintiffs submit that they have pleaded a viable RICO conspiracy claim because 18 U.S.C. § 1962(d) "criminalizes an agreement rather than any substantive criminal offense," meaning that "an agreement to associate with and participate in a yet-to-be-formed racketeering enterprise that would affect interstate commerce constitutes a completed offense under § 1962(d)." *Id.* at 46. Therefore, Plaintiffs conclude that a substantive RICO claim is not required for a viable RICO conspiracy claim, although they maintain that they have

adequately alleged a substantive RICO claim. *Id.*

C. The Toltec Defendants' Reply

In reply, the Toltec Defendants argue that "Plaintiffs' opposition fails to remedy pleading deficiencies." *Defs.' Reply* at 2 (capitalization altered).

The Toltec Defendants submit that "Plaintiffs fail to plead a cognizable RICO enterprise," *id.* at 3 (capitalization altered), because "Plaintiffs make no attempt to detail the structure of the alleged RICO enterprise, and instead argue that their [Second Amended Complaint] gives defendants 'fair notice' of their claims and the grounds upon which they rest." *Id.* (quoting *Pls.' Opp'n* at 32). After reviewing Plaintiffs' allegations, the Toltec Defendants aver that the "allegations convey neither the mechanics of a cohesive organization nor the distinct efforts of a collaborative, criminal operation guiding an enterprise's misdeeds." *Id.* at 4-5. Further, the Toltec Defendants reiterate that their "alleged association with the Federal and DISH/NagraStar Defendants to carry out legitimate law enforcement activity cannot constitute a cognizable RICO enterprise." *Id.* at 5.

***12** Similarly, the Toltec Defendants maintain that "Plaintiffs fail to plead conduct of a criminal enterprise separate from Defendants' own affairs." *Id.* at 6 (capitalization altered). In particular, the Toltec

Defendants contend that "Plaintiffs plead no factual allegations establishing how the Toltec Defendants took any part in the 'operation or management' of the RICO enterprise and fail to identify what role Toltec or Jaczewski had in knowingly 'directing' the enterprise's affairs." *Id.*

Shifting gears, the Toltec Defendants argue that "Plaintiffs allege no predicate offenses." *Id.* at 7 (capitalization altered). They aver that, although Plaintiffs suggest the Toltec Defendants committed the predicate offenses of mail fraud, wire fraud, and theft of trade secrets, Plaintiffs "fail to plausibly plead allegations establishing the Toltec Defendants' personal participation in wrongful conduct that gives rise to these predicate offenses." *Id.* at 7-8. Further, the Toltec Defendants maintain that their rendering aid to an "undercover federal investigation to detect pirated IPTV content by making more than 30 undercover purchases from Naicom using a pseudonym does not give rise to mail or wire fraud predicate offenses." *Id.* at 8.

Next, the Toltec Defendants briefly discuss the *Noerr-Pennington* doctrine. *Id.* at 9. They point out that their conduct "was determined credible for the Federal Defendants to seek—and a magistrate judge to independently find probable cause to issue—search warrants for Plaintiffs' business premises." *Id.* According to the Toltec Defendants, "that a magistrate judge found

probable cause sufficient to issue search warrants based on this petitioning conduct is the clearest indicator that the conduct was not objectively baseless." *Id.*

Turning back to the elements of Plaintiffs' RICO claim, the Toltec Defendants maintain that "the single, narrow scheme alleged ... also forecloses the existence of any RICO pattern." *Id.* at 10. According to the Toltec Defendants, "[t]he First Circuit has 'consistently declined to find continuity where [as here] the RICO claim concerns a single, narrow scheme targeting few victims.' " *Id.* (second alteration in original) (quoting *Giuliano v. Fulton*, 399 F.3d 381, 391 (1st Cir. 2005)). Moreover, the Toltec Defendants submit that "Plaintiffs' attempt to manufacture a pattern and threat of continued criminal activity by referencing past, unrelated litigation involving DISH or its corporate affiliates over a span of 20 years does not vary the character of the narrow, close-ended scheme alleged by them." *Id.* The Toltec Defendants note that this is "especially true" here because "Plaintiffs have failed to plausibly plead facts linking the Toltec Defendants to such litigation or demonstrating the relatedness necessary to show a pattern." *Id.*

The Toltec Defendants then briefly discuss Plaintiffs' RICO conspiracy claim. *Id.* at 11. They argue that this claim must be dismissed because "Plaintiffs fail to allege any facts showing that the Toltec Defendants

consciously agreed to anything—much less that they agreed to commit at least two predicate acts or understood the overall objective of the alleged RICO enterprise and consciously agreed to further its affairs or facilitate any criminal 'endeavor, which, if completed, would satisfy all the elements of a substantive [RICO] offense.' " *Id.* (alteration in original) (quoting *United States v. Rodríguez-Torres*, 939 F.3d 16, 23 (1st Cir. 2019)).

Finally, the Toltec Defendants suggest that "Plaintiffs' failure to address their remaining claims related to the Toltec Defendants renders them waived or abandoned." *Id.* at 12 (capitalization altered). As such, they conclude that "Plaintiffs' [Second Amended Complaint] should be dismissed with prejudice." *Id.*

D. Plaintiffs' Sur-Reply

***13** In their sur-reply, Plaintiffs suggest that the Court should "either reject and/or strike" any portion of the Toltec Defendants' reply "not addressing a new matter in compliance with their request for leave to file the Reply." *Pls.' Sur-Reply* at 2. Plaintiffs further submit that, upon close examination, the Toltec Defendants' "factual argument and legal discussion[ ] did not contribute anything new that they had not already discussed" in their motion to dismiss. *Id.* at 3. Plaintiffs also ask the Court to strike all the defenses raised in the Toltec Defendants' motion to dismiss pursuant to Federal Rule

of Civil Procedure 12(f). *Id.* at 15.

Addressing the substance of the Toltec Defendants' reply, Plaintiffs reiterate that the factual allegations in the Second Amended Complaint "clearly show that Plaintiffs are entitled to relief." *Id.* at 6. Although Plaintiffs concede that the "factual allegations are 'circumstantial,' " they insist that the Second Amended Complaint "provides a plausible basis ... for believing that [the] TOLTEC defendants participated in the crimes charged." *Id.* at 8.

With respect to the enterprise element of their RICO claim, Plaintiffs aver that the record reveals the Toltec Defendants "provided the Federal Defendants [with] false information" which was then incorporated into the search warrant affidavits. *Id.* at 10. Plaintiffs therefore assert that the Toltec Defendants "used their resources to fabricate evidence to support the Magistrate Judge's probable cause finding." *Id.*

Regarding the RICO predicate offenses, Plaintiffs assert, in bold and without providing citations, that the record "clearly establishes that all TOLTEC had to do was call Disney, Turner, FOX or even NRTC and ask if Naicom was in fact authorized to distribute their content, and it would have ended the investigation." *Id.* at 11 (emphasis omitted).

Turning to their RICO conspiracy claim, Plaintiffs

submit that a "RICO conspiracy and a RICO violation do not necessarily require the participation of the same people," because "the agreement to violate RICO by conspiring to commit racketeering acts could be made by a different group of people than the ones who end up committing the substantive violation." *Id.* at 12. Applying general civil conspiracy principles, Plaintiffs further declare that they "have pleaded a prima facie claim for relief for misappropriation of trade secrets against all the defendants charged." *Id.* Plaintiffs emphasize that "[l]egal impossibility is not a defense to a charge of attempted or conspiracy misappropriation of trade secrets in violation of 18 U.S.C. § 1832(a)(4)" because the "impossibility of achieving the goal of a conspiracy is irrelevant to the crime itself." *Id.* at 13

Finally, with respect to Counts III through VII of the Second Amended Complaint, Plaintiffs claim that their allegations could, in the light most favorable to them, be construed to allege that the Toltec Defendants acted in concert with the other Defendants "to commit the misappropriation." *Id.*

IV. LEGAL STANDARD

Rule 12(b)(6) requires dismissal of a complaint that "fail[s] to state a claim upon which relief can be granted." FED. R. CIV. P. 12(b)(6). To state a claim, a complaint must contain, among other things, "a short and plain statement of the claim showing that the pleader is

entitled to relief." FED. R. CIV. P. 8(a)(2). In other words, a complaint must contain "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting *Bell Atl. Corp v. Twombly*, 550 U.S. 544, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). A claim is facially plausible when "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly*, 550 U.S. at 556, 127 S.Ct. 1955). Plausible means " 'something more than merely possible' or 'merely consistent with a defendant's liability.' " *Germanowski v. Harris*, 854 F.3d 68, 71-72 (1st Cir. 2017) (internal citation omitted) (quoting *Schatz v. Republican State Leadership Comm.*, 669 F.3d 50, 55 (1st Cir. 2012)); *Ocasio-Hernández v. Fortuño-Burset*, 640 F.3d 1, 11 (1st Cir. 2011). This is a " 'context-specific' job that compels [judges] 'to draw on' [their] 'judicial experience and common sense.' " *Schatz*, 669 F.3d at 55 (quoting *Iqbal*, 556 U.S. at 679, 129 S.Ct. 1937).

***14** This is a "two-step analysis." *Cardigan Mountain Sch. v. N.H. Ins. Co.*, 787 F.3d 82, 84 (1st Cir. 2015). "First, the court must distinguish 'the complaint's factual allegations (which must be accepted as true) from its conclusory legal allegations (which need not be credited).' " *García-Catalán v. United States*, 734 F.3d 100, 103 (1st Cir. 2013) (quoting *Morales-Cruz v. Univ.*

of P.R., 676 F.3d 220, 224 (1st Cir. 2012)); *see also Schatz*, 669 F.3d at 55 (stating that a court may "isolate and ignore statements in the complaint that simply offer legal labels and conclusions or merely rehash cause-of-action elements"). "Second, the court must determine whether the factual allegations are sufficient to support 'the reasonable inference that the defendant is liable for the misconduct alleged.' " *García-Catalán*, 734 F.3d at 103 (quoting *Haley v. City of Boston*, 657 F.3d 39, 46 (1st Cir. 2011)).

V. DISCUSSION

A. Plaintiffs' Claims Against the Toltec Defendants

As an initial matter, the Court attempts to clarify which of the seven counts in the Second Amended Complaint implicate the Toltec Defendants. The Second Amended Complaint, which spans eighty-seven pages, is far from a model of clarity. Counts I and II, which respectively allege a RICO violation and a RICO conspiracy, facially implicate the Toltec Defendants. *See, e.g.*, *Second Am. Compl.* ¶ 126 (describing the Toltec Defendants as being part of the association in fact); *id.* ¶ 155 (alleging that the association in fact "knowingly agreed, combined, and conspired to conduct the affairs of the Racketeering Enterprise").

The remaining Counts, Counts III through VII, are

confusing. None of Plaintiffs' allegations related to these Counts specifically mentions either of the Toltec Defendants. *Id.* ¶¶ 158-202. However, some of the allegations related to Counts III through V do refer to Brian Parsons as one of the DISH/NagraStar Defendants. *Id.* ¶¶ 162-63, 171, 178-79. Brian Parsons is not a real person; rather it is the alias used by one of the Toltec Defendants, Mr. Jaczewski, to purchase the Naicom set-top boxes and subscription. *See id.* ¶¶ 133-35. Adding to the confusion, Counts III through V are based on the August 27 and 29, 2019 search warrant executions. *Id.* ¶¶ 160-61, 171, 178. Yet Plaintiffs nowhere allege that Mr. Jaczewski used the Brian Parsons alias in connection with, or was even present during, the search warrant executions. Plaintiffs also do not dispute the Toltec Defendants' contention that "Toltec and Jaczewski ... were not parties to the searches and seizure that took place at Plaintiffs' business premises, were not in Puerto Rico, and did not participate in those searches in any way." *Defs.' Mot.* at 1. Therefore, the Court finds the allegations that Brian Parsons was present during the search warrant executions perplexing.

The allegations related Plaintiffs' DTSA and PTSA claims (Counts VI and VII) are no less puzzling. Apart from the statement, without elaboration, that Count VII applies to all Defendants, the Court cannot find any reference to the Toltec Defendants in the allegations

supporting these Counts. *Second Am. Compl.* ¶¶ 185-202. However, in discussing the DTSA as a predicate offense for their RICO claims, Plaintiffs repeatedly refer to Brian Parsons, again characterizing Brian Parsons as one of the DISH/NagraStar Defendants. *Id.* ¶¶ 138-41.

Further, while Counts III through V are limited to the search warrant executions, the scope of Plaintiffs' DTSA and PTSA claims is unclear. Plaintiffs mention only the search warrant executions with respect to their standalone DTSA claim (Count VI), *id.* ¶ 188, and they do not mention any dates or specific conduct when discussing their PTSA claim (Count VII). [9] *See id.* ¶¶ 195-202.

***15** Complicating matters, when discussing the PTSA as a RICO predicate act, Plaintiffs appear to refer to conduct beyond the search warrant executions. Plaintiffs generally allege that "[b]eginning on or before August 7, 2017" several Defendants, including Brian Parsons: "stole, and without authorization misappropriated, took, carried away, or by fraud, artifice, or deception obtained trade secrets," *id.* ¶ 138; "did without authorization, spy, reverse engineered, copied, duplicated, downloaded, uploaded, altered, destroyed, replicated, transmitted, delivered, sent, communicated, and/or conveyed intellectual property and trade secrets," *id.* ¶ 139; and "misappropriated, obtained, or converted without authorization [the trade secrets] to the economic benefit

of [the] Racketeering Enterprises and other defendant coconspirators." *Id.* ¶ 140. Additionally, Plaintiffs clearly allege that the *Federal Defendants* violated the DTSA on August 27 and 29, 2019 (the dates of the search warrant executions) by "facilitating and assisting" the entry of several Defendants, including Brian Parsons, into Naicom's facility to steal Naicom's trade secrets. *Id.* ¶ 141. However, it is unclear whether this allegation encompasses Defendants other than the Federal Defendants.

The only clarity the Court can glean from Plaintiffs' opposition to the Toltec Defendants' motion to dismiss is Plaintiffs' averment that the Toltec Defendants are liable under the DTSA because the statute "prohibits the attempt or conspiracy to illegally obtain a trade secret," including through misrepresentations. *Pls.' Opp'n* at 40. Plaintiffs' sur-reply further clarifies that Plaintiffs are alleging the Toltec Defendants "used their resources to fabricate evidence to support the Magistrate Judge's probable cause finding." *Pls.' Sur-Reply* at 10-11.

The Court finds this latter clarification helpful because the Second Amended Complaint does attribute the information supporting the search warrants to all association-in-fact Defendants, including the Toltec Defendants. *See Second Am. Compl.* ¶ 90 ("According to the affidavit filed in support of the search warrant application the Association in Fact defendants

collectively represented to the Court that their investigation revealed ”). However, notwithstanding the conclusory references to Brian Parsons, the Second Amended Complaint fails to connect the Toltec Defendants to the execution of the search warrants.

Based on the content of Plaintiffs' Second Amended Complaint and Plaintiffs' statements in opposition to the Toltec Defendants' motion to dismiss, the Court takes the following actions. First, the Court narrows the scope of the DTSA inquiry, both the standalone DTSA claim and the alleged DTSA violation incorporated into Plaintiffs' RICO claims, [10] to include only conduct associated with the issuance and execution of the search warrants. The Court discards all other allegations related to the DTSA as insufficiently pleaded. Even when narrowed, however, the DTSA inquiry does implicate the Toltec Defendants, since the Second Amended Complaint alleges the Toltec Defendants assisted in the procurement of the allegedly unconstitutional search warrants. Therefore, the Court will assess the merits of Plaintiffs' DTSA allegations.

Next, because Plaintiffs' CFAA, SCA, and DMCA claims (Counts III through V) are premised on the search warrant executions, the Court dismisses those claims with respect to the Toltec Defendants. *See Second Am. Complaint* ¶¶ 160-61, 171, 178. The Court is unconvinced that the Toltec Defendants were present during the search warrant executions, especially because

Plaintiffs do not dispute the Toltec Defendants' representation that they were not present. Therefore, Plaintiffs have failed to carry their burden of pleading "factual content that allows the court to draw the reasonable inference that [the Toltec Defendants are] liable for the misconduct alleged." [11]
Iqbal, 556 U.S. at 678, 129 S.Ct. 1937.

***16** Finally, because Plaintiffs' PTSA claim does not mention the Toltec Defendants, or any specific conduct, the Court dismisses this claim as insufficiently pleaded with respect to the Toltec Defendants. "While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiffs' obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555, 127 S.Ct. 1955 (alteration in original) (quoting FED. R. CIV. P. 8(a)(2)). The facts connecting the Toltec Defendants to the PTSA claim are "too meager, vague, or conclusory to remove the possibility of relief from the realm of mere conjecture." *Legal Sea Foods, LLC v. Strathmore Ins. Co.*, 36 F.4th 29, 33-34 (1st Cir. 2022) (quoting *SEC v. Tambone*, 597 F.3d 436, 442 (1st Cir. 2010) (en banc)).

To summarize, the Court reads the Second Amended Complaint as potentially alleging Counts I, II, and VI against the Toltec Defendants. The Court assess the

merits as to those Counts only. The Court dismisses Counts III, IV, V, and VII as insufficiently pleaded with respect to the Toltec Defendants. [12]

B. Plaintiffs' Request to Strike the Toltec Defendants' Reply

Before turning to the merits of the Second Amended Complaint, the Court briefly addresses Plaintiff's contention that it should "reject and/or strike" any portion of the Toltec Defendants' reply "not addressing a new matter." *Pls.' Sur-Reply* at 2. Plaintiffs submit that upon "close examination," "the Toltec defendants' factual argument and legal discussion[ ] did not contribute anything new that they had not already discussed in their [motion to dismiss], and their Reply is nothing more than a second response." *Id.* at 3.

The Court disagrees. Plaintiffs rely on District of Puerto Rico Local Civil Rule 7(c), which provides:

> With prior leave of court and within seven (7) days of the service of any objection to a motion, the moving party may file a reply, which shall not exceed ten (10) pages in length, and which shall be strictly confined to responding to new matters raised in the objection or opposing memorandum.

As this rule makes clear, a reply is proper so long as it addresses "new matters raised in the ... opposing memorandum."

Plaintiffs reason that the Toltec Defendants' reply is noncompliant because it contains the same general arguments as their motion to dismiss. For example, Plaintiffs ask the Court to strike the portions of the Toltec Defendants' reply discussing the enterprise and predicate-act elements of RICO because "these issues were raised and discussed" in the Toltec Defendants' motion to dismiss. *Pls.' Sur-Reply* at 5.

But this reads Local Civil Rule 7(c) too narrowly and the Toltec Defendants' reply too strictly. The Court does not view Local Civil Rule 7(c) as prohibiting a reply from expanding upon issues raised both in the original memorandum and response so long as the response addressed the issues generated in the motion. *See Torres-Talavera v. Ford Motor Co.*, 965 F. Supp. 2d 220, 222 n.3 (D.P.R. 2013) (noting that, pursuant to Local Civil Rule 7(c), the plaintiffs' sur-reply was "confined to respond to the arguments made in defendant Ford's reply"). Local Civil Rule 7(c) is a rule of basic fairness, clearly prohibiting the use of a reply to introduce new arguments not previously addressed by the respondent.

***17** The Court's review of the reply reveals that the Toltec Defendants are responding to the arguments in

Plaintiffs' opposition brief. *See, e.g.*, *Defs.' Reply* at 6 ("Plaintiffs' Opposition fails to address the deficiencies raised in the Toltec Defendants' motion to dismiss concerning Toltec and Jaczewski's conduct or participation in the 'enterprise's affairs' "). While the Toltec Defendants' reply discusses the same subject matter as their motion to dismiss, the specific argumentation in the reply is different and responds to the arguments in Plaintiffs' opposition brief. Therefore, the reply is proper under Local Civil Rule 7(c).

The Court denies Plaintiffs' request to strike. [13]

C. Plaintiffs' RICO and RICO Conspiracy Claims

To state a civil RICO claim under 18 U.S.C. § 1962(c), a plaintiff must allege four elements: (1) conduct; (2) of an enterprise; (3) through a pattern; (4) of racketeering activity. *Lerner v. Colman*, 26 F.4th 71, 77 (1st Cir. 2022) (citing *Sedima, S.P.R.L. v. Imrex Co.*, 472 U.S. 479, 496, 105 S.Ct. 2787, 86 L.Ed.2d 384 (1985)). "Racketeering activity" is defined to include a variety of predicate offenses, including mail fraud, wire fraud, and theft of trade secrets. 18 U.S.C. § 1961(1). The civil-suit provision of the RICO statute grants the right to sue to "[a]ny person injured in his business or property by reason of a violation of" the substantive provisions of the statute. *Id.* § 1964(c).

Civil RICO claims "premised on mail or wire fraud must

be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron v. Embassy Suites (P.R.), Inc.*, 223 F.3d 12, 20 (1st Cir. 2000). "[I]n cases alleging civil RICO violations, particular care is required to balance the liberality of the Civil Rules with the necessity of preventing abusive or vexatious treatment of defendants." *Miranda v. Ponce Fed. Bank*, 948 F.2d 41, 44 (1st Cir. 1991), *abrogated on other grounds by Salinas v. United States*, 522 U.S. 52, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997). "Civil RICO is an unusually potent weapon—the litigation equivalent of a thermonuclear device. The very pendency of a RICO suit can be stigmatizing and its consummation can be costly." *Id.* Accordingly, "courts should strive to flush out frivolous RICO allegations at an early stage." *Figueroa Ruiz v. Alegria*, 896 F.2d 645, 650 (1st Cir. 1990).

1. RICO Enterprise

a. Legal Framework

In interpreting the RICO "enterprise" requirement, the Supreme Court has explained that "there is no restriction upon the associations embraced by the definition: an enterprise includes any union or group of individuals associated in fact." *Turkette*, 452 U.S. at 580, 101 S.Ct. 2524. The enterprise concept is not unbounded, however, because an enterprise must be "an entity, for present purposes a group of persons associated together

for a common purpose of engaging in a course of conduct." *Id.* at 583, 101 S.Ct. 2524. In cases "involving an alleged associated-in-fact RICO enterprise, the existence of the charged enterprise does not follow, ipso facto, from evidence that those named as the enterprise's associates engaged in crimes that collectively may be characterized as a 'pattern of racketeering activity.' " *United States v. Cianci*, 378 F.3d 71, 81 (1st Cir. 2004).

Put differently, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of 'racketeering activity' do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.* at 82. Ultimately, the First Circuit has "read *Turkette* to impose a requirement that those associated in fact function as an ongoing unit and constitute an ongoing organization. Also important to such an enterprise is that its members share a common purpose." *Id.* at 82 (internal quotations omitted). Finally, the existence of an enterprise "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Turkette*, 452 U.S. at 583, 101 S.Ct. 2524.

***18** "Threadbare recitals of the elements of a cause of

action, supported by mere conclusory statements, do not suffice," *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937, especially where "plaintiffs attempt to camouflage conclusory statements as allegations of fact." *A.G. ex rel. Maddox v. Elsevier, Inc.*, 732 F.3d 77, 81 (1st Cir. 2013).

b. Analysis

After sifting out Plaintiffs' conclusory statements, the RICO enterprise allegations as pleaded are wafer thin, and the well-pleaded facts remaining are insufficient to establish that the alleged association in fact "function[ed] as an ongoing unit" or constituted an "ongoing organization." *Cianci*, 378 F.3d at 82 (internal quotations omitted).

As to the enterprise requirement, the Second Amended Complaint offers that, starting in 2017, all Defendants conspired at the outset and together "formed an Association in Fact, [including] Legal Entity Enterprises that would help the Association in Fact defendants advance the purpose and goals of the Racketeering Enterprises' conspiratorial objectives in misappropriating themselves from Plaintiffs DISME intellectual technology property, and trade secrets." *Second Am. Compl.* ¶¶ 17-18; *see also id.* ¶¶ 126-28. It adds that the "Association-In-Fact defendants knowingly agreed, combined, and conspired to conduct the affairs of the Racketeering Enterprise in attempting and committing theft of trade secrets through a hoax

criminal investigation operation." *Id.* ¶ 155.

The Second Amended Complaint does assert that on August 7, 2017, Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel "instructed" Mr. Jaczewski to purchase a Naicom TV set-top-box receiver as part of an operation "supervised and approved" by the Federal Defendants. *Id.* ¶¶ 133-34. It also alleges that Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel subsequently "supervised and approved" Mr. Jaczewski's payments to Naicom. *Id.* ¶ 135. However, these allegations are almost entirely vague, conclusory, and devoid of factual development. At best, they describe the inner workings of the association in fact in a few isolated instances. But they fail to adequately describe how, apart from these isolated instances, the alleged association in fact 'function[ed] as an ongoing unit" or constituted an "ongoing organization" during the two-plus years it allegedly existed. *Cianci*, 378 F.3d at 82 (internal quotations omitted). In other words, Plaintiffs offer virtually no well-pleaded facts explaining how the Defendants functioned together as an ongoing unit or organization.

Plaintiffs attempt to compensate for this lack of well-pleaded facts by offering that "[t]he Association-In-Fact defendants had an ongoing organizational framework for carrying out the Racketeering Enterprises' criminal objectives" because "[t]he Association-In-Fact defendants could not have carried out the intricate task of robbing

Plaintiffs' Intellectual Property and Trade Secrets ... unless it had some structure for making and communicating group decisions." *Second Am. Compl.* ¶ 130. The Court views this allegation as the epitome of a "[t]hreadbare recital[ ] of the elements of a cause of action, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937. The allegation merely restates the requirement that the enterprise have an organizational framework, supported by nothing but the circular logic that the purported enterprise could not have succeeded unless it were truly an enterprise. There is, however, an obvious alternative explanation: the Toltec Defendants were assisting with a legitimate law enforcement investigation, not joining with the other Defendants to steal Plaintiffs' intellectual property as part of an elaborate conspiracy. Plaintiffs' allegations do not adequately plead the existence of an "ongoing unit" or "ongoing organization" required for a RICO claim. *Cianci*, 378 F.3d at 82 (internal quotations omitted).

***19** Furthermore, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of 'racketeering activity' do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.*; *see also Bachman v. Bear Stearns & Co., Inc.,* 178 F.3d 930, 932 (7th Cir. 1999) (noting that

a contrary rule would erroneously make "every conspiracy to commit fraud ... a RICO [enterprise] and consequently every fraud that requires more than one person to commit ... a RICO violation"). While Plaintiffs assert that the DISH/NagraStar Defendants have been previously involved in trade secret misconduct, they do not allege that this association in fact as a whole has engaged or will engage in any misconduct unrelated to the one-off goal of stealing Plaintiffs' intellectual property. In its review of the Second Amended Complaint, the Court is unable to find the "[s]omething more" that "must be found ... that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Cianci*, 378 F.3d at 82.

As noted earlier, Civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron*, 223 F.3d at 20. Ultimately, stripped of its conclusory allegations, the Second Amended Complaint does not assert sufficient facts to plead the existence of a RICO enterprise, and Plaintiffs' RICO claim must fail.

2. Pattern of Racketeering Activity

Plaintiffs must also plead a "pattern of racketeering activity," which "means the commission of at least two related acts of racketeering activity during a period of

ten years." *Humana, Inc. v. Biogen, Inc.*, 666 F. Supp. 3d 135, 147 n.4 (D. Mass. 2023) (citing 18 U.S.C. § 1961(5)). "Racketeering activity" is defined to include a variety of predicate offenses, including mail fraud, wire fraud, and theft of trade secrets. 18 U.S.C. § 1961(1). The First Circuit has observed that the Supreme Court has found "that the civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements." *In re Neurontin Mktg. & Sales Pracs. Litig.*, 712 F.3d 21, 34 (1st Cir. 2013) (citing *Holmes v. Secs. Investor Prot. Corp.,* 503 U.S. 258, 268, 112 S.Ct. 1311, 117 L.Ed.2d 532 (1992)).

Plaintiffs allege that the purported RICO conspiracy's pattern of racketeering activity involved numerous predicate acts, including:

> Acts indictable under Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy to Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.), while in addition, committing the possible underlying criminal offenses as prohibited under [the Computer] Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.), 18 U.S.C.A.§ 2235-Search warrant procured maliciously; 18

> U.S.C.A. § 1621-Perjury generally; 18 U.S.C.A. § 1001-Statements or entries generally, 18 U.S.C.A. § 912-Officer or employee of the United States; 18 U.S.C.A. § 2234-Authority exceeded in executing warrant; 18 U.S.C.A. § 2236-Searches without warrant, 18 U.S.C.A. § 1905-Disclosureof Confidential Information, while accomplishing their racketeering objectives. *Second Am. Compl.* ¶¶ 132 [14] ; *see also id.* ¶ 155.

***20** Most of these alleged offenses are not "predicate acts" under the RICO statute. Mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), and theft of trade secrets (18 U.S.C. §§ 1831-1832) [15] qualify; the rest do not. *See* 18 U.S.C. § 1961(1) (listing qualifying offenses).

a. Wire and Mail Fraud

"Mail or wire fraud requires proof of (1) a scheme to defraud based on false pretenses; (2) the defendant's knowing and willing participation in the scheme with the specific intent to defraud; and (3) the use of interstate mail or wire communications in furtherance of the scheme." *Sanchez v. Triple-S Mgmt., Corp.*, 492 F.3d 1, 9-10 (1st Cir. 2007). "The 'in furtherance' requirement is to be read broadly." *United States v. Simon*, 12 F.4th 1, 33 (1st Cir. 2021). "[T]he mails need not be an essential

element of the scheme. It is sufficient for the mailing to be incident to an essential part of the scheme, or a step in [the] plot." *Schmuck v. United States*, 489 U.S. 705, 710-11, 109 S.Ct. 1443, 103 L.Ed.2d 734 (1989) (internal citations and quotations omitted).

Federal Rule of Civil Procedure 9(b) requires that "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." FED. R. CIV. P. 9(b); *see also Humana*, 666 F. Supp. 3d at 154 ("Civil RICO claims based on the predicates of mail or wire fraud must meet the heightened pleading standard of Rule 9(b)"). A complaint must specify "the time, place, and content of an alleged false representation." *United States ex rel. Kelly v. Novartis Pharms. Corp.*, 827 F.3d 5, 13 (1st Cir. 2016) (quoting *Doyle v. Hasbro, Inc.*, 103 F.3d 186, 194 (1st Cir. 1996)). Furthermore, "[t]he false or fraudulent representation [in a mail or wire fraud claim] must be material." *United States v. Appolon*, 715 F.3d 362, 367 (1st Cir. 2013) (first alteration in original) (citation omitted).

Plaintiffs' mail and wire fraud claims are limited to allegations that Mr. Jaczewski—in an operation "instructed" by Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel and "supervised and approved" by the Federal Defendants—used an alias to purchase two Naicom set-top boxes and a monthly subscription he

maintained for two years. *Second Am. Compl.* ¶¶ 132-37. In Plaintiffs' view, each purchase or payment "constitutes a wire fraud racketeering act since [Mr. Jaczewski, acting under the alias] Brian Parsons, posed as [a] legitimate client and used the interstate internet electronic services to access Naicom's website, and register online under the false pretenses of BRIAN PARSONS" and "made online payments through the use of interstate internet electronic services ... to defraud and deprive Naicom Corporation of its legitimate products, intellectual property and trade secrets." *Id.* ¶ 134. Between the initial purchases and monthly subscription payments, Plaintiffs tally 22 acts of wire fraud. *Id.* ¶ 135. They also consider the initial purchase to constitute mail fraud because Mr. Jaczewski "posed as a legitimate client and used the United States Postal Services to have Naicom mail him the IPTV Set Top Box to a fake address." *Id.* ¶ 133.

***21** Accepting these allegations as true, the Court concludes that the facts are insufficient to support Plaintiffs' wire and mail fraud claims because the purportedly fraudulent representations (limited to Mr. Jaczewski's use of an alias for the set-top-box and subscription purchases) were not material. Nor could the mail and wire fraud allegations be predicate acts for Plaintiffs' RICO claims because the set-top-box operation was not causally connected to Plaintiffs' damages.

A material statement "has a natural tendency to influence, or [is] capable of influencing, the decision of the decisionmaking body to which it was addressed" but plaintiffs "need not prove that the decisionmaker actually relied on the falsehood or that the falsehood led to actual damages." *Appolon*, 715 F.3d at 368 (alteration in original) (citations and internal quotation omitted). In *Appolon*, the defendant provided untrue responses on a mortgage application, in response to questions "that specifically sought information regarding the purchaser's income, assets, and intent to reside in the property." *Id.* The First Circuit considered the false responses material because the questions "were designed to assess the borrower's creditworthiness" and thus the statements "were capable of influencing [the lender's] decision." *Id.*

The purported false statements here are far afield from providing false financial information on a mortgage application. Naicom's set-top boxes are commercial electronic products sold in retail stores like Sam's Club, and its subscription services are available on Apple's AppStore as the Naicom TV App. *Second Am. Compl.* ¶ 70 ("On February 16, 2017, Apple Corporation approved Naicom Corporation App for Apple's AppStore as Naicom TV App"); *id.* ¶ 71 ("On December 15, 2017, Sam's Club approved Naicom Corporation to officially launch and distribute in their retail stores [ ] Naicom's IPTV Set Top Box which offered the distribution of tv programming to

customers in Puerto Rico"). Plaintiffs allege that Mr. Jaczewski committed wire and mail fraud by providing a false name "of BRIAN PARSONS, fake Phone (727) 409-9464, fake Email: parsons.brian716@outlook.com and Address: 9079 FOURTH STREET NORTH SAINT PETERS FL 33702 IP: 70.127.233.139, and made online payments through the use of interstate internet electronic services using the PM Visa ending in 2775." *Id.* ¶ 134. Plaintiffs also allege that Mr. Jaczewski used the alias of Brian Parsons when purchasing two Naicom set-top boxes. *Id.* ¶ 133.

The allegations confirm that Mr. Jaczewski used the false name of Brian Parsons. It is unclear, however, what Plaintiffs mean by a "fake Phone"—whether Mr. Jaczewski used a different phone as part of the alias or if the number provided was entirely made up. Plaintiffs have not adequately pleaded that the remaining "false" statements are actually false. The Second Amended Complaint does not allege that email services require customers to use their real name in their email address. Thus, the Second Amended Complaint fails to allege that using an email with "parsons.brian" in the address is a false statement as there is no allegation that the address itself does not actually exist. It is unclear what Plaintiffs mean by a "fake" address, but the Second Amended Complaint does not allege that online retail customers are prohibited from having a product shipped to any address they desire, and Plaintiffs

have offered nothing to suggest that this constitutes a false representation. [16] Likewise, nothing in the Second Amended Complaint suggests that the IP address or credit card involved false statements. [17]

***22** The Court is thus left to consider whether Mr. Jaczewski's purchase of two commercially available products and an accompanying subscription using the name Brian Parsons can support Plaintiffs' alleged mail and wire fraud violations. The Court concludes that it cannot, because—absent allegations to the contrary—a customer providing a false name in such circumstances does not have "a natural tendency to influence, [nor is it] capable of influencing, the decision of the decisionmaking body to which it was addressed." *Appolon*, 715 F.3d at 368. Nothing in the Second Amended Complaint suggests that the use of this alias was material to Plaintiffs' decision to sell Mr. Jaczewski their commercially available product. There is no allegation that Mr Jaczewski was either known to Plaintiffs or prohibited from purchasing Plaintiffs' products. What is missing is an allegation that the alias could have reasonably affected the "decision of the decisionmaking body" (for example, Naicom's sales department's decision to process Mr. Jaczewski's payment or ship his order). Absent allegations regarding how Mr. Jaczewski's alias affected Naicom's decision to sell him their product, Plaintiffs have not pleaded

material fraud with the requisite particularity. Plaintiffs' wire and mail fraud claims cannot stand and thus do not count as predicate acts in support of their RICO claim.

Furthermore, even if the Court did find the alleged representations material, Plaintiffs' claims fall short of the causation standard required for a wire- or mail fraud-based RICO claim. *Neurontin*, 712 F.3d at 34 ("[T]he civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements" (citing *Holmes,* 503 U.S. at 268, 112 S.Ct. 1311)). "The 'central question' in evaluating proximate causation in the RICO context 'is whether the alleged violation led directly to the plaintiff's injuries.' " *Sterling Suffolk Racecourse, LLC v. Wynn Resorts, Ltd.*, 990 F.3d 31, 35 (1st Cir. 2021) (quoting *Anza v. Ideal Steel Supply Corp.*, 547 U.S. 451, 461, 126 S.Ct. 1991, 164 L.Ed.2d 720 (2006)). Quoting the U.S. Supreme Court, the First Circuit has noted that "[a] link [between the RICO predicate acts and plaintiff's injuries] that is too remote, purely contingent, or indirect is insufficient to show proximate cause." *Id.* (alterations in original) (quoting *Hemi Grp., LLC v. City of New York*, 559 U.S. 1, 9, 130 S.Ct. 983, 175 L.Ed.2d 943 (2010)). In addition, the First Circuit has identified "three functional factors with which to assess whether proximate cause exists under RICO." [18] *Id.* (quoting *Neurontin*, 712 F.3d at 35-36). The but-for causation question, in contrast, asks whether

the plaintiff would have suffered the same injury absent the defendant's violation. *See Neurontin*, 712 F.3d at 34.

Here, the alleged violations fail both causation tests because Plaintiffs portray the set-top-box operation as an unmitigated failure that only provided further proof that Naicom was a legitimate company. They allege that "after testing Naicom TV several times to identify if it was providing DISH programming, on each case the test *revealed no DISH content*." *Second Am. Compl.* ¶ 90 (emphasis added). After attempting to use the boxes to penetrate Plaintiffs' network and steal their secrets, the "Dish/NagraStar defendants also informed the Racketeering Enterprises that the Association in Fact defendants couldn't penetrate Naicom's Data Center computers, servers, encoders electronic security system, and that a physical intrusion was necessary to extract the intellectual property from the computers, servers, and encoders by physical access." *Id.* ¶ 93. Plaintiffs allege further that the operation did not yield evidence that would support a search warrant and thus the defendants had to provide "affidavits they knew contained material information known to be false and perjured to create probable cause to gain legal access into Plaintiffs[] private business." *Id.* ¶ 20.

***23** As the Court understands the Second Amended Complaint, Plaintiffs allege that all Defendants conspired from the outset to steal their intellectual

property. The set-top-box operation was an attempt to steal Plaintiffs' secrets by reverse engineering the technology and/or penetrating Plaintiffs' networks. But the operation failed. All the Defendants gained was more proof that Naicom was a legitimate company, and they then had to resort to falsifying affidavits to justify physical access to Naicom's Data Center (through a search warrant) that would finally allow them access to the desired technology. Plaintiffs have not alleged any harm prior or unrelated to the execution of the warrants. Nor have Plaintiffs alleged that the Defendants would not have sought and executed the search warrants had they not undertaken the set-top-box operation.

The Court concludes that there is no connection—proximate or but-for—between the allegedly fraudulent set-top-box purchase and Defendants acquiring Plaintiffs' intellectual property during the execution of the warrants. The alleged mail and wire fraud is "too remote" from Plaintiffs' alleged harms, *Hemi Grp.*, 559 U.S. at 9, 130 S.Ct. 983, and there is no indication that Plaintiffs would not have suffered their alleged harms absent the set-top-box operation. Plaintiffs' Second Amended Complaint thus falls short on both the materiality and causation standards for wire and mail fraud as predicate acts.

b. Theft of Trade Secrets

RICO predicate offenses include any act indictable under

18 U.S.C. § 1832, relating to theft of trade secrets under the DTSA. 18 U.S.C. § 1961(1). 18 U.S.C. § 1832 provides that "[w]hoever, with intent to convert a trade secret ... to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information," or attempts to do so, shall be subject to criminal penalties. *Id.* § 1832(a)(1), (a)(4). "Trade secret" is defined broadly to include "all forms and types of financial, business, scientific, technical, economic, or engineering information," as long as "the owner thereof has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." *Id.* § 1839(3). Critically, however, the DTSA also provides that "[t]his chapter does not prohibit ... any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State."
Id. § 1833(a)(1).

The Toltec Defendants argue that Plaintiffs fail to state a claim under the DTSA because the conduct alleged in the Second Amended Complaint was "supported by

allegations of legitimate government action." *Defs.' Mot.* at 19 (quoting *Kahre v. Damm*, No. 2:07-CV-00231-DAE-RJJ, 2007 U.S. Dist. LEXIS 95978 at *26, 2007 WL 9728869 (D. Nev. Dec. 18, 2007)). They submit that "all actions undertaken by the Toltec Defendants were performed under color of federal law, and at the direction and supervision of the Federal Defendants to assist them in discharging certain governmental duties, including assisting in the investigation of Naicom's IPTV business operations, and executing search warrants signed by a magistrate judge." *Id.* at 20, 130 S.Ct. 983.

Plaintiffs respond that the conduct alleged in the Second Amended Complaint was not legitimate law enforcement activity because the "procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Pls.' Opp'n* at 11. Because the DTSA contains an exception for governmental activity, and the parties dispute whether the conduct alleged in the Second Amended Complaint constitutes governmental activity, the Court addresses this issue first. To do so, the Court examines the validity of the warrants.

***24** The relevant standard for evaluating the validity of a warrant is the *Franks v. Delaware* framework, which requires Plaintiffs to adequately allege that both (1) "a false statement knowingly and intentionally, or with

reckless disregard for the truth, was included by the affiant in the warrant affidavit" and (2) "the allegedly false statement is necessary to the finding of probable cause." *United States v. Reiner*, 500 F.3d 10, 14 (1st Cir. 2007) (quoting *Franks v. Delaware,* 438 U.S. 154, 155-56, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978)). Plaintiffs cite ten statements that the Defendants allegedly "falsely submitted to the Court" in an affidavit supporting their search warrant application. *Pls.' Opp'n* at 12. The Court has examined each and concludes that none supports Plaintiffs' claims.

The first purportedly false statement identified by Plaintiffs is the Defendants' statement that they believed there was probable cause that Plaintiffs were violating copyright and money laundering laws. *Id.* Plaintiffs allege that this statement is false because:

The execution of the search and seizure warrant in this case did not produce any criminal evidence whatsoever; there was no probable cause. That is why the United States never opposed Plaintiffs['] Motion for Return of Property under Rule 41(g) of the Fed.R.Crim.P. In fact, they didn't even contend the serious violations Plaintiffs imputed under *Franks* in the Rule 41(g) motion. *Id.* This logic is unavailing. Plaintiffs cannot rely on the circular reasoning that the search's alleged failure to produce incriminating evidence thereby proves the Defendants could not have believed there was probable cause to search. *See Karamanoglu v. Town of Yarmouth*, 15 F.4th 82, 88 (1st Cir. 2021) (defining the probable cause inquiry

as "whether, on balance, the facts *known to the officer at the time of the arrest* support probable cause" (emphasis in original)).

Equally inadequate is Plaintiffs' claim that the Federal Defendants' failure to oppose Plaintiffs' motion to return the seized property proves not only that the seized property was not incriminating, but also that there was no probable cause to search in the first place. *See United States v. Pierre*, 484 F.3d 75, 87 (1st Cir. 2007) ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return").
The government's return of the seized hard drives and thumb drives, which—unlike drugs or illegal firearms—are not inherently contraband and can easily be downloaded or duplicated, is consistent with *Pierre*.

Furthermore, Plaintiffs are simply incorrect that success on a Rule 41(g) motion conclusively establishes the invalidity of a search. Rule 41(g) allows motions for return of property from "[a] person aggrieved by an unlawful search and seizure of property *or* by the deprivation of property." FED. R. CRIM. P. 41(g) (emphasis supplied). Without more, the property's return alone cannot demonstrate an absence of probable cause to search and seize in the first place. Ultimately, Plaintiffs' first purportedly false statement offers nothing to undermine the validity of the warrants and searches.

Second, Plaintiffs offer that the Defendants "assured the Court they had evidence based on an investigation conducted by NagraStar of Naicom's unauthorized use of Direct TV signal to distribute its programming to its paid subscribers." *Pls.' Opp'n* at 12. Plaintiffs assert that this statement was false because "[t]he United States did not produce any evidence as to the above allegations," whereas "Naicom did produce all the documentary evidence establishing that they were authorized to distribute the copyright material and running a legitimate IPTV system." *Id.* at 13.

***25** Again, Plaintiffs appear to be suggesting that exculpatory evidence they produced during the search warrant execution proves that the underlying affidavit was false. These conclusory assertions tied together by circular logic do not adequately demonstrate the falsity of the affidavit. While Plaintiffs contend that the affidavit did not "produce any evidence" supporting the suggestion that Naicom was distributing DirecTV content without authorization, the affidavit avers that Naicom's system displayed DirecTV error messages on at least 16 channels (and includes a photo of the message), [19] that Naicom's satellite dishes were precisely oriented in a manner necessary to receive DirecTV satellite signals, that representatives of the companies offering some channels Naicom purported to provide confirmed that Naicom was not licensed to provide them, and other

indicia of piracy. *See Pls.' Opp'n to DISH/NagraStar Mot.*, Attach. 1, *Aff. in Supp. of an Application for a Search Warrant* (*Warrant Aff.*). Simply put, Plaintiffs' argument that the affidavit contained no evidence of piracy is incorrect.

Third, Plaintiffs assert that, during a 2018 FBI site visit of Naicom's property, Mr. Vega "repeatedly told the agent that Naicom was a legal corporation and showed the agent a certificate from the National Cable Television Cooperative (NCTC) on the wall," yet the Federal Defendants still "filed the affidavit containing materially false and perjured statements." *Pls.' Opp'n* at 13. It is not clear specifically which "materially false and perjured statements" Plaintiffs are referring to, but the affidavit states that the FBI called NCTC's management group, which confirmed that Naicom was *not* a member. *Warrant Aff.* ¶ 15. Nothing in Plaintiffs' assertion that Mr. Vega told the FBI his company was legitimate and showed them a certificate on the wall establishes that the affidavit's claim—that NCTC management represented to the FBI that Naicom was not a member—was perjured.

Fourth, Plaintiffs contend that the affidavit's claim that Naicom was using the NCTC certificate to create the appearance of legal access to channels was a "false and perjured statement" because an FBI agent took pictures of "Naicom's National Rural Telecommunications

Cooperative 'NRCT' Certificate" and Naicom had licenses with other networks. *Pls.' Opp'n* at 13.

Fifth, Plaintiffs focus on the affidavit's claim that an FBI agent spoke with NCTC management, who confirmed that Naicom was not a member of their organization. *Id.* They allege that this "is a false and perjured statement" because Naicom provided evidence that it is a member of the NRTC. *Id.* at 14.

The distinction between NCTC and NRTC here is somewhat confusing. It appears that Plaintiffs are alleging that the FBI took pictures of a NRTC certificate on the wall but incorrectly referred to it in the affidavit as a NCTC certificate, or that the FBI mistook their NRTC certificate for an NCTC certificate. However, Plaintiffs also claim that the affidavit's assertion that they are not a member of the NCTC is a perjured statement because they provided evidence that they are a member of the NRTC. Plaintiffs offer no evidence that the latter statement was perjured because proving they are a NRTC member does not contradict the claim that they are not a NCTC member. To the extent the FBI may have misidentified a NRTC certificate as a NCTC certificate, the record does not suggest that this "allegedly false statement is necessary to the finding of probable cause," especially given the strength of the other supporting claims in the affidavit. *United States v. Patterson*, 877 F.3d 419, 424 (1st Cir. 2017) (quoting

Franks, 438 U.S. at 156, 98 S.Ct. 2674).

***26** Sixth, Plaintiffs turn to the affidavit's assertion that FBI agents contacted officials at HBO and DirecTV, who verified that Naicom did not have a relationship with their organizations despite offering HBO content. *Pls.' Opp'n* at 14. Plaintiffs claim that "[t]his is a false and perjured statement" because "Naicom provided evidence that it is licensed to distribute HBO and Cinemax programming." *Id.* (citing *Pls.' Opp'n to DISH/NagraStar Mot.*, Attach. 1 at 356 (HBO invoice dated August 31, 2019, for roughly $200 per month for "Cable — Private Home" services). Plaintiffs' claim is unpersuasive for two reasons: (1) this invoice for inexpensive "Cable – Private Home" services does not appear to provide evidence of a licensing agreement; and (2) Plaintiffs have not directly contradicted the purportedly perjured claim, which was that HBO and DirecTV officials represented to the FBI that they did not have a relationship with Naicom.

Seventh, Plaintiffs focus on the affidavit's claim that the "external appearance of the Data Center offered indicia of piracy," calling it a "false and perjured statement" because "[a]t the conclusion of the search and seizure warrant execution the FBI agents found that [ ] Naicom's equipment (encoders) were provided by the networks authorizing the programming distribution and that the use of the satellite was in fact to download the codes

provided by the networks." *Pls.' Opp'n* at 14. Plaintiffs again rely on circular logic, as the discovery of exculpatory evidence at the conclusion of a warrant's execution does not provide a "substantial preliminary showing" that the underlying affidavit was perjured. *Franks*, 438 U.S. at 155-56, 98 S.Ct. 2674.

Plaintiffs' eighth point suffers from the same defect. They claim that the affidavit's statements that there were suspicious financial transactions between Naicom and other businesses owned by Mr. Quinones and Mr. Vega were false and perjured because "[d]uring the execution of the Search Warrant S/A Lange interviewed employees from the Business Office and was provided with financial records," which established "that none of the Corporations were involved in any money laundering activities." *Pls.' Opp'n* at 15. Again, the fact that a search did not uncover incriminating evidence does not establish that it was predicated on a perjured affidavit.

Plaintiffs' ninth point takes issue with the affidavit's request to seize computers and data based on claimed probable cause that they contained evidence. *Id.* Plaintiffs contend that this statement was perjured because "the FBI agents were not looking for any criminal evidence" during the search and they did "not find[ ] any evidence whatsoever of the crimes described in the warrant, which also denied any probable cause." *Id.* at 15-16. The Court does not fully follow Plaintiffs'

logic across these seemingly contradictory assertions, but they appear to utilize the same circular reasoning (the assertion of probable cause was perjured because the resulting search "denied any probable cause"), along with the conclusory contention that the FBI was not actually looking for evidence. These claims do not undermine the validity of the warrants.

Tenth, Plaintiffs claim that the affidavit's request to seize evidence of statutory violations was "false and perjured" because the FBI did not find any evidence at the conclusion of the search warrant execution. *Id.* at 16. Beyond the fact that this argument relies on the same circular logic, an affidavit's request to seize "things and ... records" is not an assertion of fact and cannot be false or perjured. *Id.*

To summarize, none of these purportedly false statements, alone or in combination, satisfies Plaintiffs' burden under the *Franks* standard to overcome the presumed validity of the warrants. Moreover, Plaintiffs offer several additional, similarly unavailing, arguments that their DTSA allegations do not constitute legitimate law enforcement activity.

***27** Plaintiffs submit that the August 29, 2019 search was "illegal" and "warrantless" because "[t]he Federal and Dish/NagraStar Defendants knew for a fact that the first search warrant execution had already denied any

criminal wrongdoing, and that the initial alleged probable cause had dissipated." *Id.* at 23. This assertion—that the Defendants knew probable cause had dissipated—is wholly conclusory (especially in light of Plaintiffs' argument that the entire investigation was a hoax, and the agents knew probable cause never existed). Furthermore, the warrant did not expire until September 4, 2019 and courts generally recognize a "reasonable continuation rule" providing that a search may be reasonably continued if the warrant remains valid. [20] *See United States v. Keszthelyi*, 308 F.3d 557, 568-569 (6th Cir. 2002) (describing the rule and collecting cases). Plaintiffs have not offered any well-pleaded, nonconclusory allegations suggesting that the continuance here was unreasonable. [21]

Plaintiffs also contend that the searches were unlawful because the Federal Defendants did not follow the procedure to obtain a Stored Communications Act warrant (also known as a SCA order). *Pls.' Opp'n* at 17-20. But this argument lacks merit because the Federal Defendants appropriately obtained a traditional search warrant in lieu of a SCA order.

SCA orders are different from traditional search warrants. As one court has explained:

SCA warrants "are not like the search warrants used in the physical world: they are 'executed' when a law

enforcement agent delivers (sometimes by fax) the warrant to the [service provider]. The [service provider], not the agent, performs the 'search'; the [service provider] 'produces' the relevant material to the agent; the user associated with the inbox often never learns that his inbox has been 'searched.' In sum, these are not search warrants at all and to call them such confuses legal terminology." *In re Info. Associated with @gmail.com*, No. 16-mj-00757 (BAH), 2017 U.S. Dist. LEXIS 130153, at *52-53, 2017 WL 3445634 (D.D.C. July 31, 2017) (quoting Paul K. Ohm, *Parallel–Effect Statutes and E–Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1610-11 (2004)). Additionally, the standard for a SCA order is "less stringent than the probable cause standard generally required for a search warrant." *United States v. Taylor*, 54 F.4th 795, 804 (4th Cir. 2022). Finally, even if the Defendants were seeking information protected by the SCA, the statute gives law enforcement the option of seeking either a SCA order or a traditional search warrant. [22] *See* 18 U.S.C. § 2703(b) (the government may obtain "a court order for such disclosure under subsection (d) of this section" *or* "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"); *id.* § 2703(c) (same).

***28** Plaintiffs' argument is groundless because the Federal Defendants were primarily—if not entirely—seeking information not protected by the SCA.

Regardless, they obtained search warrants for the facility and computer systems, thereby satisfying the requirements of the SCA.

Plaintiffs also submit once again that "[t]he Toltec Defendants can't raise at this time the defense that the execution of the search and seizure warrant was authorized, legal and constitutional, which was waived during the Rule 41(g) proceedings, and abandoned forever." *Pls.' Opp'n* at 25-26. However, as the Court has already explained, the government's decision not to oppose a motion to return property does not affect the validity of the warrant or seizure. *See Pierre*, 484 F.3d at 87 ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return").

Finally, while Plaintiffs contend that the search warrant executions were unlawful due to the involvement of the DISH/NagraStar Defendants, they acknowledge that "Congress has explicitly authorized" private parties to assist law enforcement in the execution of search warrants. *Pls.' Opp'n* at 20 (citing 18 U.S.C. § 3105). Further, although they contend that any civilian assisting with a search "must have been serving a legitimate investigative function," *id.*, Plaintiffs fail to make any well-pleaded, nonconclusory allegation that the DISH/NagraStar Defendants were not serving such a function. Indeed, Plaintiffs do not offer any persuasive

argument that would permit the Court to find that the DISH/NagraStar Defendants' presence rendered the search illegal. [23]

In sum, Plaintiffs have failed to adequately challenge the validity of the search warrants or establish that anything about the warrants' executions was unlawful. Plaintiffs have thus failed to plead a DTSA violation as a predicate act in support of their RICO claim because the allegations in the Second Amended Complaint, even when read in the light most favorable to Plaintiffs, merely suggest that the Defendants were engaging in legitimate law enforcement activity. *See* 18 U.S.C. § 1833(a)(1) ("This chapter does not prohibit ... any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State"). Absent both an enterprise and any predicate acts, Plaintiffs' RICO claim must be dismissed as to the Toltec Defendants.

***29** These same pleading shortfalls doom Plaintiffs' RICO conspiracy claim. *See Efron*, 223 F.3d at 21 (1st Cir. 2000) ("A conspiracy claim under section 1962(d) may survive a *factfinder's* conclusion that there is insufficient evidence to prove a RICO violation, but if the pleadings do not state a substantive RICO claim upon which relief may be granted, then the conspiracy claim also fails" (citations omitted) (emphasis in original)); *see also Salinas*

v. United States, 522 U.S. 52, 64, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997) ("A conspirator must intend to further an endeavor which, if completed, *would satisfy all of the elements of a substantive criminal offense*, but it suffices that he adopt the goal of furthering or facilitating the criminal endeavor" (emphasis supplied)).

D. Plaintiffs' DTSA Claim

As noted above, the Court reads Plaintiffs' freestanding DTSA claim as containing the same allegations as the DTSA claim offered as a predicate act for the RICO claim. Thus, the standalone DTSA claim fails for the reasons previously described. While the DTSA does provide a private right of action for owners "of a trade secret that is misappropriated ... if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce," 18 U.S.C. § 1836, this right of action cannot be used to challenge "otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State." *Id.* § 1833(a) (1).

VI. CONCLUSION

The Court GRANTS Defendants Toltec Investigations L.L.C. and Mike Jaczewski's Motion to Dismiss (ECF No. 137). The Court DISMISSES Counts I through VII of Plaintiff's Second Amended Complaint as pleaded against the Toltec Defendants.

SO ORDERED.

All Citations

Not Reported in Fed. Supp., 2024 WL 1363772

Footnotes

1 This is the second lawsuit arising out of the underlying events at issue. On August 25, 2020, a group of plaintiffs, including many of Plaintiffs here, filed a *Bivens* action against many of the same defendants. *See Quinones-Pimentel v. Cannon*, No. 3:20-cv-01443-JAW, 2022 U.S. Dist. LEXIS 48109 at *2-3, 2022 WL 826344 (D.P.R. Mar. 17, 2022). On March 17, 2022, the Court dismissed the plaintiffs' *Bivens* action. *Id.* at *88. The plaintiffs appealed, and the Court of Appeals for the First Circuit affirmed the Court's dismissal on October 27, 2023. *Quinones-Pimentel v. Cannon*, 85 F.4th 63, 66-68 (1st Cir. 2023).

2 In their Second Amended Complaint, Plaintiffs use the spelling, "Rinkle." *See, e.g.*, *Second Am. Compl.*

¶ 43. In her filings, however, Ms. Rinkel uses the spelling, "Rinkel." *See, e.g.*, *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Mot. to Dismiss* at 1. No doubt, Ms. Rinkel knows how to spell her own name, and the Court uses "Rinkel" throughout this order.

3 Consistent with Federal Rule of Civil Procedure 12(b)(6), in describing the facts, the Court has relied upon the allegations in the Plaintiffs' Second Amended Complaint. *Foley v. Wells Fargo Bank, N.A.*, 772 F.3d 63, 68 (1st Cir. 2014); *Medina-Velázquez v.*

Hernández-Gregorat, 767 F.3d 103, 108 (1st Cir. 2014) ("We examine whether the operative complaint states a claim for which relief can be granted when we construe the well-pleaded facts in the light most favorable to the plaintiffs, accepting their truth and drawing all reasonable inferences in plaintiffs' favor" (internal citation omitted)).

4 Presumably because Claro Puerto Rico is a well-known business in Puerto Rico, the Second Amended Complaint does not describe Claro Puerto Rico except by name. *See Second Am. Compl.* ¶ 68. According to Wikipedia, Claro Puerto Rico is the one of the largest telecommunications companies in Puerto Rico. *See Claro P.R.*, WIKIPEDIA (updated Oct. 14, 2023), *https://en.Wikipedia.org/wiki/Claro_Puerto_Rico.*

5 Plaintiffs often refer in the Second Amended Complaint to the "Association in Fact defendants." *See, e.g., Second Am. Compl.* ¶ 87. As the Court interprets Plaintiffs' complaint, this term refers to all Defendants collectively. *See id.* ¶¶ 17, 62 (listing all the Defendants as together "form[ing] an Association in Fact").

6 Here, the Court quotes the language in the Second Amended Complaint. *Second Am. Compl.* ¶ 103. In the context of this sentence, the meaning of the verb, "counted," is unclear. It would make more sense if the sentence used "complied with," rather than "counted." Whichever verb is correct, however, makes no difference in this Court's ruling on the motion to dismiss.

7 The Toltec Defendants initially filed their motion to dismiss pursuant to Federal Rules of Civil Procedure 12(b)(2) and 12(b)(6). *Defs.' Mot.* at 1. However, on February 21, 2023, the Toltec Defendants withdrew their Rule 12(b)(2) arguments and elected to proceed solely under their Rule 12(b)(6) arguments. *Unopposed Notice of Partial Withdrawal of Toltec Investigations L.L.C. and Mike Jaczewski's 12(b)(2) Mot. to Dismiss* at 1 (ECF No. 163). The Toltec Defendants explained that Toltec's predecessor had rented a storage unit in San Juan, Puerto Rico and, after Toltec's formation,

Toltec "paid the storage fees associated with that unit until its rental was terminated." *Id.* at 1 n.1. Although the Toltec Defendants represented that the storage unit was not used in connection with the Naicom investigation, they conceded that the storage unit's existence "nevertheless impacts the 12(b)(2) jurisdictional analysis." *Id.*

Because the Toltec Defendants voluntarily withdrew their Rule 12(b)(2) arguments, the Court summarizes only their Rule 12(b)(6) arguments.

8 The Plaintiffs variously spell NagraStar with a capital "S" and with a lower-case "s." *Compare Second Am. Compl.* ¶ 21, *with Pls.' Opp'n* at 1. NagraStar spells its name with a capital "S." *Defs.' Mot.* at 1. Again, on the assumption that NagraStar knows how to spell its own name, the Court has used NagraStar and inserted this spelling in lower case references.

9 With respect to their PTSA claims, Plaintiffs first allege that:

The Confidential Information the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle misappropriated from Plaintiffs through association, assistance and facilitation of the [Federal Defendants], exfiltrated from the D&V IP Holdings and Naicom computer systems trade secrets under Puerto Rico law, as discussed above, and in keeping with the definition of trade secrets under Puerto Rico law: information, including a formula, pattern, compilation, program, device, method, technique, or process, that (A) Derives actual or potential independent economic value, from not being generally known, and not being readily ascertainable by proper means by another who can obtain economic value from its disclosure or use; and (B) Is the subject of reasonable efforts to maintain its secrecy, pursuant to Section 11 of Puerto Rico Industrial and Trade Secrets Protection Act (Law No.

80, of June 3, 2011). *Second Am. Compl.* ¶ 197. Plaintiffs subsequently allege that:

> Each Defendant disclosed, received, and used these misappropriated trade secrets without Plaintiff's consent, knowing or having reason to know that the trade secrets were acquired by improper means.

Id. ¶ 199.

10 Although the allegations related to the standalone DTSA claim do not mirror the DTSA allegations accompanying Plaintiffs' RICO claims, the Court sees no reason why there would be different factual bases for what is effectively the same violation. Therefore, the Court reads the allegations in Count VI as coextensive with the allegations in the RICO Counts.

11 Plaintiffs may have intended for Counts III through V to encompass the Toltec Defendants based on the Toltec Defendants' furnishing of allegedly false information for use in the search warrant application. Even so, Plaintiffs have only alleged that the search warrant application contained ten misrepresentations. In accordance with the Court's discussion of these ten misrepresentations below, Plaintiffs have failed to show that any of the allegedly false statements were actually false. Without these ten allegedly false statements, Plaintiffs' allegations that the Toltec Defendants supplied misinformation that somehow made its way into the search warrant application are threadbare and conclusory. Therefore, even if Counts III through V were premised on this theory, the Court would dismiss these Counts for the same reasons the Court dismisses Plaintiffs' DTSA claim.

12 Even if these claims had been sufficiently pleaded against the Toltec Defendants, the Court still would have dismissed them. As discussed in the Court's order on the DISH/NagraStar Defendants'

motion to dismiss, Counts III, IV, V, and VII lack merit because, even accepting as true all the well-pleaded facts in the Second Amended Complaint, the Defendants' conduct was authorized pursuant to valid search warrants. Because Plaintiffs fail to impugn the validity of the search warrants, they cannot state a claim for relief against any of the Defendants under the CFAA, SCA, DMCA, or PTSA.

13 Plaintiffs also suggest that the Court should strike all the defenses raised by the Toltec Defendants pursuant to Federal Rule of Civil Procedure 12(f) because "there are not factual issues nor issues of law to be resolved before the validity of the defenses in the present context may be determined." *Pls.' Sur-Reply* at 15. The Court declines to do so.

14 Paragraph 132 of the Second Amended Complaint names the following: "The D[ISH]/NagraStar defendants Emily Rinkle, Bert Eichhorn, Jordan Smith, and Kevin Gedeon, and Federal defendants U.S. Attorney Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Person, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Named Agents of the Federal Bureau of Investigations, and John Does 1-20." *SecondAm. Compl.* ¶ 132. The Toltec Defendants are notably absent. The Court assumes that this must have been an oversight since the Plaintiffs have otherwise included the Toltec Defendants in their predicate act allegations.

15 The statutory provision cited by Plaintiffs—18 U.S.C. § 1836—governs civil proceedings for misappropriation of trade secrets and is not listed as a predicate act in 18 U.S.C. § 1961(1). Since the Court assumes Plaintiffs' reference to 18 U.S.C. § 1836 was in error, the Court has recharacterized Plaintiffs' predicate-act allegations relating to theft of trade secrets as arising under 18 U.S.C. §§ 1831 and 1832.

16 In theory, Mr. Jaczewski could have provided an address that was entirely made up. This seems unlikely, however, in light of

the Second Amended Complaint's allegations that the Defendants used the set-top boxes to attempt remote attacks on Naicom's servers. Had the boxes been shipped to an address that didn't exist, they would have been returned to Naicom as undeliverable, meaning that the Defendants could not have used them to launch sniffing attacks. The Plaintiffs do not appear to allege that the mailing address is a fake address, and the Court doubts that they could do so, based on the information in this case.

17 To the contrary the Second Amended Complaint includes a table listing all the payments made to Naicom by Mr. Jaczewski posing as Brian Parsons. *Second Am. Compl.* ¶ 136. In the Court's view, these payments confirm that the credit card number provided by Mr. Jaczewski was valid.

18 These factors are:

(1) "concerns about proof" because "the less direct an injury is, the more difficult it becomes to ascertain the amount of a plaintiff's damages attributable to the violation, as distinct from other, independent, factors," ... (2) "concerns about administrability and the avoidance of multiple recoveries," ... and (3) "the societal interest in deterring illegal conduct and whether that interest would be served in a particular case[.]"

Sterling Suffolk Racecourse, 990 F.3d at 35-36 (quoting *Neurontin*, 712 F.3d at 35-36).

19 In their sur-reply, Plaintiffs claim that "while the picture shows a Naicom TV Set Top Box ('STB') displayed at a table in front of a Television, the truth of the matter is that the Toltec defendants forgot to plug in and turn on the STB. Plaintiffs are assuming that the Toltec defendants plugged a pen drive behind the Television and used its content to display the image appearing in the television screen." *Pls.' Sur-Reply* at 10 n.3. Plaintiffs cite no support for this claim, and their assumptions are insufficient to impugn the contents

of a sworn affidavit.

20 The "reasonable continuation rule" requires the satisfaction of two conditions: 1) "the subsequent entry must indeed be a continuation of the original search, and not a new and separate search"; and 2) "the decision to conduct a second entry to continue the search must be reasonable under the totality of the circumstances." *Keszthelyi*, 308 F.3d at 569.

21 The closest Plaintiffs come to a nonconclusory allegation is their assertion that U.S. Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned, after the execution of the first search warrant, that Naicom complied with "all the programming distribution contract and agreements." *Second Am. Compl.* ¶ 103. But this allegation is still conclusory, and it is undercut by the sentence immediately following it, which alleges that the USAO Defendants instructed S/A Pearson "to order Darwin Quinones and Victor Vega to report to the FBI Offices in San Juan with the licensing contracts for an interview regarding Naicom's company." *Id.* Clearly, whatever U.S Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned did not absolve Naicom of wrongdoing; otherwise, there would have been no need to conduct an interview.

22 Further, "the statute offers no express direction as to when the government should seek a warrant versus" a SCA order. *Taylor*, 54 F.4th at 804.

23 Plaintiffs quote *Bellville v. Town of Northboro*, 375 F.3d 25 (1st Cir. 2004) for the proposition that "it might be a better practice, if circumstances permit, for law enforcement officers to disclose to the magistrate that civilians will be involved in the execution of the search and for the warrant to indicate that the magistrate permitted this involvement." *Pls.' Opp'n* at 21 (footnotes omitted) (quoting *Bellville*, 375 F.3d at 33-34). They fail to quote the preceding sentence, which states, "we will not improvise a rule that seems unnecessary in light of the overarching requirement that the use of

civilians in the execution of a search must still meet the constitutional standard of reasonableness." *Bellville*, 375 F.3d at 33. The Court declines Plaintiffs' invitation to convert the best practice outlined by the First Circuit into a rule.

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF PUERTO RIC

NAICOM CORPORATION; D&V IP HOLDINGS, LLC; PAYLINK, LLC; AND KIARAS, LLC,

PLAINTIFF,

v.

DISH NETWORK CORPORATION; DISH NETWORK, LLC; NAGRASTAR, LLC; BERT EICHHORN, NAGRASTAR INVESTIGATOR; EMILY RINKLE NAGRASTAR INVESTIGATOR; JORDAN SMITH, NAGRASTAR INVESTIGATOR; KEVIN GEDEON, DISH NETWORK INVESTIGATOR; TOLTEC INVESTIGATIONS, LLC; MICHAEL THOMAS JACZEWSKI, A.K.A. BRIAN PARSONS; ROSA EMILIA RODRIGUEZ-VELEZ, FORMER UNITED STATES ATTORNEY; JOSE CAPO-IRIARTE, FORMER AUSA, CHIEF CRIMINAL DIVISION; NICHOLAS W. CANNON, AUSA, DEPUTY CHIEF, CYBERCRIMES, CRIMINAL DIVISION; DOUGLAS A. LEFF, FBI

Civil No. 21-1405-JAW

SECOND AMENDED COMPLAINT

JURY TRIAL DEMANDED
COUNT ONE RICO (18 U.S.C. § 1962(c)) COUNT TWO
RICO CONSPIRACY (18 U.S.C. § 1962(d)) COUNT THREE
COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1030(a))
COUNT FOUR STORED COMMUNICATIONS ACT (18 U.S.C. §§ 2701-2712)
COUNT FIVE
DIGITAL MILLENNIUM COPYRIGHT ACT (17 U.S.C. § 1201 et seq.)
COUNT SIX
MISAPPROPRIATION OF TRADE SECRETS UNDER THE DEFEND TRADE SECRETS ACT (18 U.S.C. § 1836 et seq.) COUNT SEVEN PUERTO RICO INDUSTRIAL AND TRADE SECRETS PROTECTION ACT (Law No. 80, of June 3,

SPECIAL AGENT IN CHARGE OF SAN JUAN DIVISION; BRADLEY REX, FBI SUPERVISORY SPECIAL AGENT; LANCE LANGE, FBI SPECIAL AGENT; KEVIN PEARSON, FBI SPECIAL AGENT; CLAY REHRIG, FBI SPECIAL AGENT JUAN GALARZA, FBI COMPUTER SCIENTIST; JASON LOPEZ, FBI EVIDENCE TECHNICIAN; SEVERAL UNKNOWN NAMES AGENTS OF FEDERAL BUREAU OF INVESTIGATIONS; JOHN DOES 1-20.

DEFENDANTS.

2011).

PROPOSED

SECOND AMENDED COMPLAINT

TO THE HONORABLE COURT:

HEREIN appears Plaintiffs**, D&V IP HOLDINGS, LLC; NAICOM CORPORATION; KIARAS, LLC, PAYLINK, LLC; (hereinafter collectively "the Plaintiffs"),** through their undersigned counsel and most respectfully pray and request:

I. NATURE OF ACTION

INTRODUCTION

1. The tree of law must be pruned from time to time so that its branches keep our government institutions lawful. Our founders delegated this duty to the judiciary branch; no one is above the law.

2. This is a civil action for statutory, compensatory and punitive damages against all the defendants in the above captioned case, in their personal and individual capacities based on a conspiracy, association, combination, and agreement, involving acts of gross criminal misconduct in violation of the United States statutory laws as prohibited under the Digital Millennium Copyright Act (17 U.S.C. § 1201(a)&(b); the False Statements or entries generally (18 U.S.C.A.§ 1001); the Computer Fraud and

Abuse Act (18 U.S.C. § 1030(a)&(b); the Mail Fraud (18 U.S.C. § 1341); Wire Fraud (18 U.S.C. § 1343); Conspiracy to Commit Mail And Wire Fraud laws (18 U.S.C. § 1341); Perjury generally (18 U.S.C.A. § 1621) the Disclosure of Confidential Information (18 U.S.C.A. § 1905); the Theft and conspiracy to commit Theft of Trade Secrets (18 U.S.C. § 1832(a)&(b); the Racketeering Influenced and Corrupt Organization (18 U.S.C.A. § 1962(a)(c)&(d); Authority exceeded in executing warrant (18 U.S.C.A. § 2234); Search warrant procured maliciously (18 U.S.C.A. § 2235); Searches without warrant (18 U.S.C.A. § 2236); the Stored Communications Act (18 U.S.C. §§ 2701(a); and the Puerto Rico Industrial And Trade Secrets Protection Act (Law No. 80, of June 3, 2011).

3. The defendants' criminal statutory violations are all redressable under the plaintiffs' statutory and equitable rights as secured under the United States Civil Remedy laws pursuant the Digital Millennium Copyright Act (17 U.S.C. § 1203 (a)&(c); the Computer Fraud and Abuse Act (18 U.S.C. § 1030(g); the Theft of Trade Secrets (18 U.S.C. § 1836 (b)(c)&(d); the Racketeering Influenced and Corrupt

Organization (18 U.S.C.A. § 1964 (a)&(c); the Stored Communications Act (18 U.S.C. §§ 2707(a)(b)(c)&(g) and 2712; and the Puerto Rico Industrial And Trade Secrets Protection Act (Law No. 80, of June 3, 2011).

4. Darwin Quinones-Pimentel ("Darwin") is a veteran in systems architect with expertise in coding, algorithms and methods, software designs, formulas, patterns, compilations, programs, device methods, UI designs, database designs, network architect, and successful project leader with many other extraordinary skills in the computer science technology industry.

5. Beginning in the year 2002 through 2012, Darwin invested 10 years, a great expense of personal monetary funds, and an extraordinary effort in developing and engineering the source codes which operate the programs of the intellectual technology which trade secret confidential information (hereinafter "intellectual technology"), were granted to D&V IP Holdings, LLC, Naicom Corporation, Kiara, LLC, and Paylink, LLC (hereinafter the Plaintiff), a proprietary solution protected under the Defend Trade Secrets Act.

6. The PAYLINK AND KIARAS Cloud

Workforce Management is an ALL-IN-ONE web-based software solution designed to streamline business programs and operations. The features include HR Management, Time & Attendance, Business Unit Management, and Electronic Payment Transmission, all accessible through PAYLINK AND KIARAS Cloud Network. The program creates, sends, collects, stores and manages important employee documents, records, and information including, employee wages, timecards, tracks benefits plans, PTO, vacation and sick data, makes electronic communications transmission payments to banks, and government entities, from customers, partners and private business, via the internet and private networks, (hereinafter "intellectual technology"). A complete proprietary business solution protected under the Defend Trade Secrets Act.

7. Naicom Corporation is in the business of distributing live television programming content services in interstate and foreign commerce to residential and business customers using Multicast transit system via private networks interstate electronic wire through a new distribution intellectual technology.

8. Darwin's intellectual technology and algorithms methods allow the passing of multicast traffic through interstate electronic wire networks no matter how the routers were configured by ISP companies, thus, the most efficient way of live TV distribution, an intellectual technology concept never known or used, because the Cable and Satellite TV industry did not have the solution to pass this type of traffic via private networks or the internet to end users, using server equipment, and filtering multicast content through tunnels by delivering only what the receiver is viewing.

9. Darwin's intellectual technology proprietary solution also managed to transcode the video and audio traffic to 2mps maintaining a broadcast quality in Full HD. An intellectual technology that the Cable and Satellite TV companies could not execute since their current distribution technology required at least more than 10mps to maintain the same quality and the TV content distributors had to transmit all the channels at the same time even though the receiver could only watch one.

10. One good example is that when cable tv companies were transmitting 120 channels at the same time, the transmission required

1200mps to be able to deliver the 120 channels. On the other hand, Darwin's technology allowed the distribution of 200 channels and the end user only needs 2mps.

11. This intellectual technology proprietary solution enabled for the first time the broadcast of media via private networks and the internet, a new concept of IPTV service to distribute Live-Video Television Content (media) to residences, business, and primes customers. Darwin's intellectual technology proprietary solution was characterized under the concept of Dynamic Internet Semantic Multicast Environment ('DISME"), a new technology concept that was not known in the Cable, Satellite, or IPTV industry, and unascertainable by any means, since according to engineer's expert in the computer science and telecommunications industry, claimed that the DISME concept, of distributing live television content using Multicast (UDA packets) via the internet system is impossible.

12. In 2016, the DISME Intellectual Technology reach its final developed stage, and all alfa/beta tests were completed. Darwin and Victor Vega-Encarnacion ("Mr. Vega" or collectively "Naicom's Founders) founded

Naicom Corporation, a Network & Internet Communication Platform capable of delivering live Television, Video on Demand content services via private fiber, internet, and wireless network to subscribers in interstate and foreign commerce worldwide, instant access to their favorite TV Shows, Movies, Music/Videos on Demand and Live Sports & Music events through its Set-Top-Box using the Internet Protocol Television and TV Everywhere ("TVE") on any mobile device.

13. Darwin and Mr. Vega also founded D&V IP Holdings, LLC, as the proprietor of the DISME, and its intellectual technology property were kept secret and confidential and were never revealed to any person, employee, company, corporation or third party, protected in a Hard Drive secured in a Safe Box and guarded under the protections defined pursuant to the Federal Defend Trade Secrets Act ("DTSA") (18 U.S.C. § 1839 (3)(A)&(B).

14. During this same period of time Darwin and Mr. Vega also engaged in joint business ventures marketing Kiaras, LLC a Human Resources, Time and Attendance Management company, and PayLink, LLC, a Payroll Processing company which

intellectual technology were filed and stored, under secured methods in Naicom's Offices and Data Center computers and servers. Kiaras and Paylink, LLC intellectual technology were also kept in a Hard Drive secured in a Safe Box, at Naicom Corporation and Data Center Facility. Paylink, LLC intellectual technology were also copyrighted and filed with the U.S. Copyright Office.

15. The NAICOM DATA CENTER is an interstate and foreign electronic communications services Facility affecting interstate or foreign commerce. The Facility provides the communications services through the aid of the internet and private network wire cable electronic communication systems. The Facility operates servers, encoders, computers, and telecommunications systems and technology, by electronically transmitting communications involve in Webservers, Email-Servers, Carrier Grade Routers which interconnected with local ISP providers through Border Gateway Protocols (BGP) in exchanging routing information between autonomous systems. The Facility also uses Satellite Dish systems to download video encrypted content, and delivers telephone fixets, internet, video programming

distribution, and data information, through Tower Cells Air Fiber Antennas radio frequency transmissions. The Facility also operates Customer Relation Management program which effectuate electronic transmissions to collect and make payments transactions from partners and customers' accounts through gateway and merchant financial systems, via the internet and private networks, as those terms are defined under 18 U.S.C. § 1030(e), 18 U.S.C. § 2711(2) and 18 U.S.C. § 2510.

16. In 2017, the Dish Network Corporation, Dish Network LLC, and NagraStar, LLC (hereinafter the "Racketeering Enterprises"), learned through defendant's investigators Bert Eichhorn, Emily Rinkle, Jordan Smith, Kevin Gedeon, (collectively hereinafter "the Dish/NagraStar defendants"), that Naicom Corporation was utilizing a new technology to distribute content programing to residential and business end users via private networks and internet, as described in paragraphs 7, 8, 9, 10, and 11, a technology unknown to them, and which they needed to advance the Sling TV distribution system technology. The Dish/NagraStar defendants decided to misappropriate and deprive Plaintiffs of their intellectual technology

property and trade secrets and convert them to the economic benefit of the Racketeering Enterprises, knowing that the offense would injure the Plaintiffs' businesses.

17. In 2017, the Dish/NagraStar defendants, orchestrated a plan, which consisted in associating themselves with the Federal Defendants former U.S. Attorney for the District of P.R. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA, Nicholas W. Canon, and the defendants FBI S/A Douglas A. Leff, FBI S/A Bradley Rex, FBI S/A Lance Lange, FBI S/A Kevin Pearson, FBI S/A, FBI S/A Clay Rehrig, FBI S/A Juan Galarza, FBI S/A Jason Lopez, ("collectively the Federal Defendants"), with Toltec Investigations, LLC, the defendant President and CEO, Michael Thomas Jaczewski, A.K.A. Brian Parsons, (collectively the Toltec Defendants") and John Does 1-20, formed an Association In Fact, and used the United States Attorney's Office of the District of Puerto Rico, (hereinafter "USAPR"), and the Federal Bureau of Investigation, San Juan, Field Office, (hereinafter "FBISJO"), as the Legal Entity Enterprises that would help the Association in Fact defendants advance the purpose and goals of the Racketeering Enterprises conspiratorial objectives in

misappropriating themselves from Plaintiffs DISME intellectual technology property, and trade secrets and favor the Racketeering Enterprises economic and market growth, at the expense of the Plaintiffs' financial and business detriment.

18. The conspiracies objective and purpose of forming the Association in Fact was that its members would use the Legal Entity Enterprise power to invent a hoax criminal investigation and deceive the judiciary system into authorizing the execution of an unlawful search and seizure warrant and facilitate the Dish/Nagrastar defendants an illegal entry and trespass into Plaintiffs' private business premises, and thus photograph, copy, download, seize and misappropriate themselves from Plaintiffs' DISME's intellectual property, and other proprietary solutions, trade secrets, even if they had to search files, brake cabinets, secure storage rooms, or safe boxes, and personally intrude into security systems of the computers, servers, encoders, to find and steal the intellectual property and trade secrets, and turn them over to the Racketeering Enterprises, and advance their distribution technology, for economic gain, while destroying Plaintiffs' business.

19. On August 27, 2019, the Federal defendants agreed to use the Legal Entity Enterprises power, and applied for two Search and Seizure Warrants; (1) Case No. 19-1680 (SCC), to search the premises of Building Centro de Seguro's, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907; and (2) Case No. 19-1679 (SCC), to search the premises of Villa Fontana, 4SS N2 Via Josefina, Carolina, PR.

20. The search warrant order was issued under illegal and unlawful means in that the Federal defendants used the Legal Entity Enterprises power to have the judiciary authorize the search and seizure warrants through the use of affidavits they knew contained material information known to be false and perjured[1] to create probable cause to gain legal access into Plaintiffs private business in violation the United States

---

[1] Please take Judicial notice that the record containing the false and perjured statements submitted to the Court in the affidavit in support of probable cause are factually discussed in the Bivens Actions litigation Second Amended Complaint pages 32-36 ¶¶ 78 through 79 Items a through j [Civil Case # 20-cv-1443 ECF 202] and fully legally discussed in Plaintiffs' Response to Motion to Dismiss pages 49-57 [Civil Case # 20-cv-1443 ECF 196]. The factual allegations and legal discussion therein are incorporated herein by reference and made part hereof.

criminal laws as prohibited pursuant to 18 U.S.C.A. § 2235- Search warrant procured maliciously: 18 U.S.C.A. § 1621- Perjury generally, 18 U.S.C.A. § 1001- False Statements or entries generally.

21. On August 27, 2019, the Federal and Dish/NagraStar defendants executed the search and seizure warrants and while acting as federal agents photographed and seized documents containing trade secret information, downloaded and seized from Plaintiffs' computers, servers, encoders data containing business confidential information, intellectual property, trade secrets, proprietary solutions, and also seized 2 Hard Drives, 2 USB Thumb Drives, 1 Cell Phone, 1 Tablet, found in Plaintiffs secured cabinets, safe boxes, storage rooms, and private offices to further misappropriate themselves with Plaintiffs intellectual technology property and trade secrets, by illegal means, using the judicial system[2] to

[2] The underlying basis for the search warrant was false and the search warrant against plaintiffs was dismissed on the government's own motion on 11/05/2019, Dkt 13, and the government was ordered to return the property listed in claimant's demand. (Docket No. 1)" pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure. Rule 41(g) provides that, on a Motion to Return Property, "[a] person aggrieved by an unlawful search and seizure of property or by the

help the Racketeering Enterprises advance their conspiratorial objectives.

22. On August 29, 2019, the Federal and Dish/NagraStar defendants executed illegal and warrantless searches and seizures while acting as federal agents, trespassed Naicom's Data Center Facility and inserted pen drives and other electronic instruments to bypass its computers, servers, encoders security protections to download and seize Plaintiffs' confidential information, intellectual property, trade secrets, and copyrighted material data by illegal means, using the power of the Legal Entities Enterprises to help the Racketeering Enterprise advance their conspiratorial objectives.

23. The Federal defendants' actions in allowing the Dish/NagraStar defendants the entrance into Plaintiffs premises under the pretense that they were federal agents violated 18 U.S.C.A. § 912- Officer or employee of the United States.

24. The Federal defendants' actions in allowing the Dish/NagraStar defendants to execute the second warrantless search and seizure

---

deprivation of property may move for the property's return." Fed.R.Crim.P. 41(g).

and trespass into Naicom's Data Center facility violated 18 U.S.C.A. § 2236- Searches without warrant; and violated 18 U.S.C.A. § 1905- Disclosure of Confidential Information, by allowing the Dish Network defendants to learn and acquire Plaintiffs confidential information and trade secrets without authorization.

25. The Association in Fact defendants actions in this case also violated the Mail Fraud (18 U.S.C. § 1341); Wire Fraud (18 U.S.C. § 1343); Conspiracy to Commit Mail And Wire Fraud (18 U.S.C. § 1341), laws; the Misappropriation and Conspiracy to commit the Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.); and the Puerto Rico Industrial And Trade Secrets Protection Act (Law No. 80, of June 3, 2011), all in violation of the RICO laws as prohibited under 18 U.S.C. § 1962.

26. The Federal and Dish/NagraStar defendants' actions in penetrating into Plaintiffs Offices and a protected Data Center Facility involved in the telecommunication electronic services, and illegally searching and bypassing its computers, servers, encoders security protections containing Plaintiffs confidential information, intellectual property, trade

secrets, and copyrighted material were committed in violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); and Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.).

27. Plaintiffs bring this civil action against defendants in their individual and collective capacity for their unlawful conduct under law, in violation of the federal criminal statutes discussed herein and are entitled to redress and equitable relief from all those involved in the scheme and conspiracy to deprive Plaintiffs of their intellectual property and trade secrets under the United States statutory civil remedy laws.

JURISDICTION AND VENUE

28. This Court has federal question jurisdiction pursuant to 28 U.S.C. § 1331 because this action arises under 18 U.S.C. § 1030 (the Computer Fraud and Abuse Act); 18 U.S.C. §§ 1961-68 (Racketeer Influenced and Corrupt Organizations Act); 18 U.S.C. §§ 2701, 2707 & 2712 (the Stored Communications Act); The Defend Trade Secrets Act of 2016, codified at 18 U.S.C. § 1836; Original jurisdiction is granted to the federal courts by 18 U.S.C. § 1964, (Civil Remedies); 18 U.S.C. 1836(c), (Civil

Proceedings); 28 U.S.C. § 1338, (the protection of copyrights, and unfair competition); 17 U.S.C. § 1201 et seq. (the Digital Millennium Copyright Act), and 17 U.S.C. § 1203, Civil Remedies.

29. This Court has supplemental jurisdiction over the state law claims alleged in this action, pursuant to 28 U.S.C. § 1367(a), because these claims are so intimately related to claims exclusively within the Court's original jurisdiction, that they form part of the same case or controversy under Article III of the United States Constitution, and because these claims arise out of the same nexus of facts and events.

30. This Court also has jurisdiction over this case pursuant to 28 U.S.C. § 1332(a)(2), because this suit is between a citizen of a domestic state (Naicom Corporation), (Kiaras, LLC), and (Paylink, LLC, and a citizen of a foreign state (Dish Network Corporation), (Dish Network, LLC) and (Nagrastar, LLC), and (Toltec Investigations, LLC), and the amount in controversy exceeds $75,000; and section 1343 (1)(3)(4), which creates pendent jurisdiction to hear and decide claims arising under state law.

31. Plaintiffs further invoke the supplemental

jurisdiction of this Court to hear and adjudicate claims arising under the laws of the Commonwealth of Puerto Rico, specifically, Puerto Rico Industrial and Trade Secrets Protection Act (Law No. 80, of June 3, 2011), since they are so related to the federal claims that they all form part of the same case or controversy under Article Ill of the Constitution of the United States.

32. Venue is proper in this Court under 28 U.S.C. § 1391(b)(2) because these causes of action arose out of several incidents/events occurring in the Commonwealth of Puerto Rico, in the Jurisdiction of the United States District Court of Puerto Rico. Venue is also invoked pursuant to 28 U.S.C. § 1391(e)(1) since many of the defendants in this civil action are employees of the United States and were acting under color of legal authority when the constitutional and statutory cause of action accrued and a substantial part of the events or omissions giving rise to the claim occurred. Venue is also proper in this Court under 28 U.S.C. § 1400(a) because this case asserts claims relating to the protection of copyrighted works. Lastly, venue is also proper for the claims arising under RICO pursuant to 18 U.S.C. § 1965(a) because some of the defendants reside, are found, have agents, transact affairs, and Dish Network

Corporation, does business, as Dish Network, PR, in San Juan, Puerto Rico.

PARTIES AND PARTICIPANTS

33. Naicom Corporation was organized in 2016 as a corporation existing under the laws of the Commonwealth of Puerto Rico with its place of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907.

34. D&V IP HOLDINGS, LLC was organized in 2016 as a corporation existing under the laws of the Commonwealth of Puerto Rico with its place of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907.

35. Paylink, LLC was organized in 2014 as a corporation existing under the laws of the Commonwealth of Puerto Rico with its place of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907.

36. Kiaras, LLC was organized in 2010 as a corporation existing under the laws of the Commonwealth of Puerto Rico with its place of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907.

37. Defendant, DISH Network Corporation, was organized in 1995 as a corporation under the laws of the State of Nevada. Dish Network started offering the DISH® branded pay-tv service in March 1996 and are the nation's third largest pay-tv provider. Dish Network's principal executive offices are located at 9601 South Meridian Boulevard, Englewood, Colorado 80112: telephone number (303) 723-1000.

38. Defendant, DISH Network Corporation, LLC was organized in 1987 as a Limited Liability Corporation under the laws of the State of Colorado. Dish Network Corporation, LLC principal executive offices are located at 9601 South Meridian Boulevard, Englewood, Colorado 80112.

39. Defendant, NagraStar, LLC 90 Inverness Cir E, Englewood, CO 80112 is a joint venture between Dish Network Corporation (formerly EchoStar Communications Corporation) and Kudelski SA that was formed in 1998. NagraStar's focus is delivering and maintaining security solutions for satellite and Internet-based television systems and other connectivity initiatives in North America. Their mission also includes carrying strong

anti-piracy activities from field investigations to legal and joint actions with law enforcement agencies. The company is located onsite with Dish in Colorado. NagraStar is a joint venture between Dish Network Corporation (formerly EchoStar Communications Corporation) and Kudelski SA that was formed in 1998.

40. Defendant, Toltec Investigations, LLC, was organized in 2001, as a Limited Liability Corporation under the laws of the State of Florida. Toltec Investigations is licensed by the Florida Department of Agriculture and Consumers Services under License number A 2900314, as a Private Investigative Agency. Toltec Investigations is in the business of investigating the technology and distribution involved in IPTV systems, Copyrights, Patent, and Trademark and Brand's Intellectual Property investigations. Toltec Investigations, LLC is located at 535 Central Ave Saint Petersburg, FL, 33701-3703.

41. Defendant Jordan Smith is and was at all times relevant herein a resident of Parker, Colorado, employed by NagraStar as Manager of Field Security Investigations and Senior Anti-Piracy Investigator. As the Manager of Field Security & Investigations Jordan Smith is responsible for investigating piracy matters, in particular the piracy or compromise of NagraStar's

encryption technology used by DISH to protect its signal from unauthorized reception, decryption, and viewing. He also moves the FBI, U.S. Customs, and the United States Attorney Offices in investigating and prosecuting piracy matters within the United States, and participates in the execution of search and seizure warrants, during criminal and civil raids, identifies the Dish/NagraStar satellite television product devices, and analyses products and devices seized at the search site. Defendant Jordan Smith participated individually and collectively in concert with defendants in the violation of the above captioned statutory criminal and civil offenses.

42. Defendant, Bert Eichhorn is and was at all times relevant herein a resident of Denver, Colorado, employed by NagraStar as Manager of Field Security & Investigations. As the Manager of Field Security & Investigations Bert Eichhorn is responsible for investigating piracy matters, in particular the piracy or compromise of NagraStar's encryption technology used by DISH to protect its signal from unauthorized reception, decryption, and viewing. He has also assisted the FBI, U.S. Customs, and the United States Attorney Offices in investigating and prosecuting piracy

matters within the United States and participates in the execution of search and seizure warrants, during criminal and civil raids, and identifies the Dish/NagraStar satellite television product devices, and analysis products and devices seized at the search site. Defendant Bert Eichhorn participated individually and collectively in concert with the above-mentioned defendants in the violation of the above captioned statutory criminal and civil offenses.

43. Emily Rinkle is and was at all times relevant herein, a resident of Denver, Colorado, employed by NagraStar as the Manager of Field Security & Investigations. As the Manager of Field Security & Investigations Emily Rinkle is responsible for investigating piracy matters, in particular the piracy or compromise of NagraStar's encryption technology used by DISH to protect its signal from unauthorized reception, decryption, and viewing. She has also assisted the FBI, U.S. Customs, and the United States Attorney Offices in investigating and prosecuting piracy matters within the United States and participates in the execution of search and seizure warrants, during criminal and civil raids, and identifies the Dish/NagraStar satellite television product devices, and analyses products and devices

seized at the search site. Defendant Emily Rinkle participated individually and collectively in concert with the above-captioned defendants in the violation of the above captioned statutory criminal and civil offenses.

44. Defendant, Kevin Gedeon, is and was at all times relevant herein, a resident of Lone Tree, Colorado, employed by Dish Network as the Manager of Fraud Investigations. As the Manager of Fraud Investigations Kevin Gedeon was involved in the investigation of unauthorized interception of DISH Network's satellite television signals; the utilization of unauthorized software, hardware, and other technologies to circumvent DISH Network's, encryption technology and piracy investigations. He also directs and/or participates in undercover investigations of individuals or entities engaged in the unauthorized interception of Dish Network's signals (sometimes referred to as "pirates"), and individuals or entities engaged in the manufacture, sale or distribution of devices, software, and services to enable individuals to obtain the unauthorized interception of DISH Network's signals (sometimes referred to as "pirate dealers" and/or "pirate distributors"). He also performs the forensic analysis of certain devices obtained from the subjects of

Dish Network undercover investigations to determine the capabilities of the devices, specifically to determine if and/or how the devices are primarily of assistance in the unauthorized interception of Dish Network satellite television signals. He also analyzes the activities of individuals and entities to determine if they are acting as pirate dealers or pirate distributors trafficking in Dish Network piracy software, hardware and technology. He is also familiar with digital satellite encryption and decryption software and hardware technology and with pirate (unauthorized black market) digital satellite decryption software, hardware, and internet technology. Defendant Kevin Gedeon participated individually and collectively in concert with the above-captioned defendants in the violation of the above captioned statutory criminal and civil offenses.

45. Defendant, Michael Thomas Jaczewski, A.K.A. Brian Parsons, is and was at all times relevant herein, a resident of Saint Peters, Florida, and the President, Chief Executive Officer and Founder of Toltec Investigations, LLC. He was hired by the Dish/NagraStar defendants and participated and committed the racketeering acts to perpetrate the fraud upon Naicom TV to deprive Plaintiffs of its intellectual property

and to advance the Racketeering Enterprise's conspiratorial objectives. Defendant Michael Thomas Jaczewski, A.K.A. Brian Parsons, participated individually and collectively in concert with the above-captioned defendants in the violation of the above captioned statutory criminal and civil offenses.

46. Defendant Rosa Emilia Rodriguez-Velez was at all times relevant herein, a resident of Puerto Rico, employed by the United States Government. Rosa Emilia Rodriguez-Velez was appointed by the District Court to serve as the United States Attorney for the District of Puerto Rico. She was charged with the responsibility to investigate, and collect, analyze, and corroborate if the evidence presented by the Department of Justice Agencies or Departments Investigative Special Agents (hereinafter "DOJISA"), qualified as evidence in support of search warrant probable cause and criminal prosecution determinations. She was also in charge with the ultimate responsibility in providing DOJISA statutory legal interpretations, advice and guidance during criminal investigations regarding the potential violation of the piracy, computer crimes, telecommunications, and theft of intellectual property laws against the United States or its citizens in the Criminal Division,

Cyber Crimes Unit, and had the ultimate decision-making authority to approve or decline an investigation or criminal prosecution determination. She was sworn under oath before taking office to execute faithfully her duties, the United States Laws, uphold Local Laws, and to abide by the United States Constitution. Defendant Rosa Emilia Rodriguez-Velez participated individually and collectively in concert with the above-captioned defendants in the violation of the above captioned statutory criminal and civil offenses.

47. Jose Capo-Iriarte was at all times relevant herein, a resident of Puerto Rico, employed by the United States Government. Jose Capo-Iriarte was appointed by the Attorney General as Assistant United States Attorney. He was in charge of the United States Attorney Criminal Division for the District of P.R. He was charged with the responsibility to investigate, collect, analyze, and corroborate if the evidence presented by the DOJISA qualified as evidence in support of search warrant probable cause and criminal prosecution determinations. He was also in charge with the responsibility in providing DOJISA statutory legal interpretation, advice and guidance during criminal investigations regarding the potential violation of piracy, computer crimes, telecommunications, and

theft of intellectual property laws against the United States or its citizens in the Criminal Division, Cyber Crimes Unit, and had the ultimate decision-making authority to approve or decline an investigation or criminal prosecution determination. He was sworn under oath before taking office to execute faithfully his duties, the United States Laws, uphold Local Laws, and to abide by the United States Constitution. Defendant Jose Capo-Iriarte participated individually and collectively in concert with the above-captioned defendants in the violation of the above captioned statutory criminal and civil offenses.

48. Nicholas W. Cannon is and was at all times relevant herein, a resident of Puerto Rico, employed by the United States Government as Assistant United States Attorney, Deputy Chief, Cybercrimes, Criminal Division in the District of P.R. As Assistant United States Attorney, Nicholas W. Cannon was appointed by the Attorney General to assist the United States Attorney for the District of Puerto Rico. He was in charge of the United States Attorney Criminal Division for the District of P.R. He was charged with the responsibility to investigate, collect, analyze, and corroborate if the evidence presented by the DOJISA qualified as evidence in support of search

warrant probable cause and criminal prosecution determinations. He was also in charge with the ultimate responsibility in providing DOJISA statutory legal interpretation, advice and guidance during criminal investigations regarding the potential violation of the piracy, computer crimes, telecommunications, theft of intellectual property laws against the United States or its citizens in the Criminal Division, Cyber Crimes Unit, and decision-making authority to approve or decline an investigation or criminal prosecution determination. He was sworn under oath before taking office to execute faithfully his duties, the United States Laws, uphold Local Laws, and to abide by the United States Constitution. Defendant Nicholas W. Cannon participated individually and collectively in concert with the above-captioned defendants in the violation of the above captioned statutory criminal and civil offenses.

49. Defendant Douglas A. Leff was at all times relevant herein, a resident of Puerto Rico, and the FBI Special Agent in Charge of the San Juan Division. As FBI Special Agent in Charge of the San Juan Division, Douglas A. Leff was responsible for participating, overseeing, and supervising all criminal investigations conducted by the FBI San Juan Division. He

was also charged with the duty and power to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. He was also responsible for reviewing, analyzing, and discussing with the USAPR if the evidence collected during criminal investigations by his FBI Agents subordinates qualified as evidence supporting probable cause pursuant to Fourth Amendment constitutional standards in support of search warrant applications and/or legally met the elements of the crime prohibited by the statute for criminal prosecutions in the District of Puerto Rico. He was also the final decision-making authority to approve or decline a criminal investigation where the evidence collected and discussed with the USAPR did not represent a crime in violation of the United States criminal laws. He was sworn under Oath to faithfully execute the laws of the United States, uphold local laws and to abide by the United States Constitution. The defendant Douglas A. Leff participated individually and collectively in concert with the above-captioned defendants in the violation of the above statutory criminal and civil offenses.

50. Defendant Brad Rex is and was at all times relevant herein, a resident of Puerto Rico, and

the FBI Supervisory Special Agent in the San Juan Division. As the FBI Supervisory Special Agent in the San Juan Division Brad Rex was charged with the responsibility of supervising and assuring that FBI Special Agents assigned to his squad would follow the rule of law. He was also charged with the duty and power to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. He was also responsible for reviewing, analyzing, and discussing with the FBI Special Agent in Charge and the USAPR if the evidence collected during criminal investigations by his FBI Agents subordinates qualified as evidence supporting probable cause pursuant to Fourth Amendment constitutional standards in support of search warrant applications and/or legally met the elements of the crime prohibited by the statute for criminal prosecutions in the District of Puerto Rico. He was also involved in the final decision-making authority of recommending the continuing or cancelation of a criminal investigation where the evidence collected did not represent a crime in violation of the United States criminal laws. He was sworn under Oath to faithfully execute the United States Laws, uphold local laws and to abide by the United States Constitution. The

defendant Brad Rex participated individually and collectively in concert with the above-captioned defendants in the violation of the above captioned statutory criminal and civil offenses.

51. Defendant Lance Lange is and was at all times relevant herein a resident of Puerto Rico and Special Agent in the San Juan Division. As Special Agent in the San Juan Division Lance Lange was charged with the duty and powers to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. He was also responsible for investigating complaints filed with the FBI, to gather data, collect information and evidence representing the potential violation of United States criminal laws, and to ascertain if the evidence discovered during criminal investigation reliably represented a criminal violation or required the rejection of the complaint and close the case. As such he was sworn under oath to faithfully execute the United States Laws, uphold the local laws and to abide by the United States Constitution. The defendant Lance Lange participated individually and collectively in concert with the defendants in the violation of the above captioned statutory criminal and civil offenses.

52. Defendant Kevin Pearson is and was at all times relevant herein, a resident of Puerto Rico, and Special Agent in the San Juan Division. As Special Agent in the San Juan Division Kevin Pearson was charged with the duty and powers to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. He was also responsible for investigating complaints filed with the FBI, gather data, collect information, evidence representing the potential violation of the United States criminal laws, and to ascertain if the evidence discovered during the criminal investigation reliably represented a criminal violation or required the rejection of the complaint and close the case. He was sworn under oath to faithfully execute the United States Laws, uphold the local laws and to abide the United States Constitution. The defendant Pearson participated individually and collectively in concert with the defendants in the violation of the above captioned statutory criminal and civil offenses.

53. Defendant Clay Rehrig is and was at all times relevant herein, a resident of Puerto Rico, and Special Agent in the San Juan Division. As Special Agent in the San Juan Division Clay Rehrig was charged with the duty and powers

to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. He was also responsible for investigating complaints filed with the FBI, and to gather data and collect information and evidence representing the potential violation of the United States criminal laws, and to ascertain if the evidence discovered during criminal investigation reliably represented a criminal violation or required the rejection of the complaint and closure of the investigation. He was sworn under oath to faithfully execute the United States Laws, uphold local laws and to abide by the United States Constitution. The defendant Clay Rehrig participated individually and collectively in concert with defendants in the violation of the above captioned statutory criminal and civil offenses.

54. Defendant Juan Galarza is and was at all times relevant herein, a resident of Puerto Rico, and the FBI Computer Science Officer in the San Juan Division. As Computer Science Officer in the San Juan Division Juan Galarza was charged with the powers to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants, and to make seizures of property. He was responsible for investigating computer and

internet cybercrimes. He was also responsible for conducting investigations regarding criminal violations of the electronic telecommunications services, transmission, systems, networks, piracy, intellectual property, theft of trade secrets laws, copyrights, attacks on computers, child pornography, contributed to the development and acquisition of new systems to combat cybercrimes within the FBI. He was sworn under oath to faithfully execute the United States Laws, uphold local laws and to abide by the United States Constitution. Defendant Juan Galarza participated individually and collectively in concert with defendants in the violation of the above captioned statutory criminal and civil offenses.

55. Defendant Jason Lopez is and was at all times relevant herein, a resident of Puerto Rico, and the FBI Evidence Technician in the San Juan Division. As FBI Evidence Technician in the San Juan Division Jason Lopez was charged with the duty to enforce the criminal laws of the United States, to execute and serve search warrants, arrest warrants and to make seizures of property. He was responsible for collecting, preserving, documenting, analyzing the evidence collected by the FBI Agents in the course of the investigation, or a crime scene,

and for preparing reports of investigations for the USAPR in support of search warrant applications and criminal prosecution determinations. He was sworn under Oath to faithfully execute the United States Laws, uphold local laws and to abide by the United States Constitution. The defendant Jason Lopez participated individually and collectively in concert with the defendants in the violation of the above captioned statutory criminal and civil offenses.

56. Several Unknown Named Agents of Federal Bureau of Investigations also participated individually and collectively in concert with the defendants in the violation of the above statutory criminal and civil offenses.

57. John Doe 1-20, individually and collectively participated in concert with defendants in the violation of the above captioned statutory criminal and civil offenses.

THE RACKETEERING AND LEGAL ENTITY ENTERPRISES AND THE ASSOCIATION IN FACT DEFENDANTS

58. The Dish Network Corporation, Dish Network, LLC and Nagrastar LLC, are the Racketeering Enterprises, as that term is defined under 18 U.S.C. 1961 (4)

59. The United States Attorney Office for the District of Puerto Rico, is a statutory creature responsible for investigating, collecting, analyzing, and corroborating evidence in support of search warrant probable cause determinations, the enforcement and prosecutions for violation of the laws against the United States in the Criminal Division of the District of Puerto Rico. The USAPR is the Legal Entity Enterprise used by the Association in Fact Defendants to commit the racketeering activities in advancing the Racketeering Enterprises conspiratorial objectives, as that term is defined under 18 U.S.C. 1961 (4)

60. The Federal Bureau of Investigation, San Juan, Field, in Puerto Rico, is a statutory creature responsible for investigating, detecting, and prosecuting crimes against the United States. The FBISJO is the other Legal Entity Enterprise used by the Association in Fact Defendant to commit the racketeering activities in advancing the Racketeering Enterprises conspiratorial objectives, as that term is defined under 18 U.S.C. 1961 (4)

61. The Toltec Investigations, LLC is the Person used by the Association in Fact Defendants to commit the racketeering activities in advancing the Racketeering Enterprises

conspiratorial objectives, as that term is defined under 18 U.S.C. 1961 (3)

62. The Dish/Nagrastar and Federal Defendants, and Michael Thomas Jaczewski, A.K.A. Brian Parsons are the Association in Fact Defendants, who committed the racketeering activities to advance the Racketeering Enterprises conspiratorial objective, as that term is defined under 18 U.S.C. 1961 (4)

II. FACTUAL ALLEGATIONS

A. D&V IP HOLDINGS AND NAICOM'S GENESIS

63. Through the years 2015-2016, Darwin and Mr. Vega engaged in a joint business venture to create a Network and Internet Communications Company capable, among other matters, of offering IPTV services.[3] To

[3] Please take Judicial notice that the record containing some of the evidence supporting factual allegations in this Civil Case are found in the Motion for Demand for Return of Property in the form of Attachments 1through 33 filed in miscellaneous Case No. [19-mc-308 (FAB)]. See Federal Rules of Civil Procedure Rule 10 Form of Pleadings (c) Adoption by Reference; Exhibits. A statement in a pleading may be adopted by reference elsewhere in the same pleading or in any other pleading or motion. A copy of a written instrument that is an exhibit to a pleading is a part of the pleading for all purposes. Id. These exhibits include true and exact copies of Naicom's Licenses agreements authorizing the distribution of

accomplish the business structure legal entity Darwin and Mr. Vega created two corporations, D&V IP Holding, LLC, the company who would hold the DISME proprietary solution, source codes, intellectual technology; and Naicom Corporation, who would license the DISME technology from D&V IP Holding, LLC to use its technology to distribute television programing from authorized content providers networks.

64. In complementing the development of the DISME technology through the performance of alpha/ beta tests, D&V IP Holdings and Naicom Corporation, with considerable economic investment, created and developed significant amounts of confidential and proprietary information, including non-public information relating to DISME's source codes, patterns, formulas, algorithms, methods techniques, the technological vision for Naicom's IPTV content distribution, marketing, servicing, research and development efforts and strategies, business and marketing performance strategies; financial data, business plans; technical data; customer development management

---

content the Dish/Nagrastar and Federal defendants alleged Naicom was pirating from all the authorized networks.

programs; subcontractor and vendor relationships, collectively identified as Trade Secret, which owners took reasonable measures to keep the information secret, since the information derived actual and potential economic value, was unknown, and which information represented economic value if disclosed or used by other persons or competitors as that term is defined under 18 U.S.C. s 1839 (3)(A)(B). The same procedures were implemented for Kiara's and Paylink's corporations. (Collectively, "Confidential Information"),

65. In protecting and keeping the Confidential Information secret, D&V IP Holdings and Naicom Corporations, only installed on their servers, located at the Naicom's Data Center Facility, what is known as a compiled executable. The entire system was installed with Ubuntu operating system which allows the hard disk to be encrypted. To access Naicom's servers the authorized employee needed to enter a secure data center facility structure, and access its computer systems through user and password, which were assigned by hierarchy. The SSH access is in private LAN, which is not exposed to the internet. To be able to attack the server through internal ports it was necessary to be

inside the facility. The intellectual technology was then downloaded into a hard disk and kept in a safe box mark as a trade secret property. The same procedures were implemented for Kiara. Paylink's intellectual property was copyrighted.

66. In 2016, Darwin and Mr. Vega founded and registered in the State Department of Puerto Rico Naicom Corporation as a closed corporation business company doing business in Puerto Rico and complied with all the requirements to perform as a legitimate IPTV business.

67. In 2016, Naicom Corporation also requested the manufacture of its own brand of tv set top boxes for end users through Informir LLC. The communication between Naicom's TV Set Top Box and the servers also had what is known as a security hash and key.

68. In 2016, Naicom Corporation acquired the programing licenses to distribute television media and video on demand content in United States, Puerto Rico, and U.S. Virgin Islands through worldwide television network companies and in 2017, Naicom Corporation became a member of the National Rural Telecommunications Cooperative "NRTC".

69. On January 6, 2017, Naicom Corporation submitted a request to have Apple Corporation place its Naicom TV App in Apple's AppStore. Apple Corporation's legal division requested Naicom Corporation to produce all the licenses authorizing the programing distribution available to Naicom's subscribers via Naicom TV TVE function at iPhone Cellular phones.

70. On February 16, 2017, Apple Corporation approved Naicom Corporation App for Apples' AppStore as Naicom TV App.

71. On December 15, 2017, Sams Club approved Naicom Corporation to officially launch and distribute in their retail stores the Naicom's IPTV Set Top Box which offered the distribution of tv programming to customers in Puerto Rico.

72. D&V IP Holdings, Naicom, Kiara, and Paylink Corporations also developed policies and practices to maintain the secrecy of its confidential and proprietary information, including, internal policies and procedures regarding the identification and classification of proprietary and confidential information.

73. To safeguard D&V IP Holdings', Naicom's, Kiaras', and Paylink's own confidential information and proprietary data as well as

that of customers and other third parties, the corporations restricted employees' access to confidential and proprietary information as required by each employee's business needs and required employees to execute non-disclosure agreements, among other protections.

74. D&V IP Holdings, Naicom, Kiaras, and Paylink also invested significantly to acquire and implement multi-faceted layered data security technology and other protections in order to safeguard its confidential and proprietary data, including, for example: Imposing restrictions on remote access to corporations networks; Requiring individual password protection; Implementing data encryption on the corporations computers, servers, and Naicom's mobile devices TV application; and conducting internal periodic cybersecurity audits.

75. Pursuant to its internal policies, the classification "D&V IP Holdings, Naicom, Kiaras and Paylink Proprietary" applies to the corporation's internal and contractually protected highly sensitive information, where if compromised, would be substantially and irreversibly detrimental to the corporation's business interests. D&V IP Holdings', Naicom's, Kiaras', and Paylink's

internal policies regarding the safeguarding of corporations Proprietary Information and trade secrets specifically includes in the definition of "D&V IP Holdings', Naicom's, Kiaras', and Paylink's Proprietary and Confidential Information" all technical information, source codes, compilations, programs, formulas, contracts data, systems designs, algorithms and methods, performance capabilities, data relating to Naicom's, Kiaras', and Paylink's business operations and administration, trade secrets, data protected by state or federal privacy regulations, proposal data, financial and employee information, intellectual property, trade secrets, and data pertaining to D&V IP Holdings', Naicom's, Kiaras', and Paylink's technical developments.

76. D&V IP Holdings', Naicom's, Kiaras', and Paylink's policies require that documents containing D&V IP Holdings', Naicom's, Kiaras', and Paylink's Proprietary and Confidential Information shall be conspicuously marked with a legend identifying the document as "D&V IP Holdings', Naicom's, Kiaras', and Paylink's Proprietary" in accordance with internal operating guidelines for the marking, maintenance, and transmittal of proprietary

information. Documents submitted to potential investors, content providers networks, companies and business were further marked "Confidential Information" in addition to bearing "D&V IP Holdings', Naicom's, Kiaras', and Paylink's Proprietary" markings.

B. THE NEGOTIATIONS WITH CLARO PUERTO RICO

77. In 2017, CLARO Puerto Rico began negotiations with Naicom Corporation to distribute Naicom Set Top Boxes to their customers.

78. Claro represented to Naicom Corporation that it had approximately 320,000 internet subscribers that could not subscribe to Claro's IPTV services because Claro's internet distribution to those residences delivered only 5 Megabytes and Claro's IPTV Set Top Box required 60 Megabytes to adequately upload the Claro's IPTV distribution programing, and if Naicom's technology only needed two megabytes to deliver the IPTV services it would work like a charm for Claro's triple pack (mobile, internet and tv services), competition against Liberty double pack (internet and tv services).

79. During the negotiation process Naicom

Corporation and Claro Puerto Rico executed a mutual NDA agreement prior to having the executive members meeting to discuss and analyze business information involving the letter of intent and the resellers agreement contents.

80. After extensive business negotiations Claro's Product Development Officer Anibal Rios represented to Naicom executives that the Claro-Naicom business alliance represented to Claro business projections of over $10,000,000.00 of monthly gross revenue for the first year and over $13,000,000.00 for the second year just by penetrating Claro's corporate and residential subscribers in Puerto Rico.

81. On the other hand, the Claro-Naicom business alliance represented to Naicom business projections to achieve 100,000 Corporate subscribers, plus another 150,000 residential subscribers, projecting a monthly income revenue of $9,000,000.00 in the first year, and $12,000,000.00 for the second year in gross sales to Claro's subscribers and Naicom's new customers.

82. Upon information and belief, Claro had a contract with Dish Network Satellite TV, where Dish Network was providing the TV programming to Claro's internet subscribers

which could not subscribe to Claro's IPTV services and the Naicom deal represented a contract cancelation threat to Dish Network's contract with Claro, and Claro was also considering shutting down its IPTV business division for loss of revenue.

83. Mr. Carlos Garcia of Claro Puerto Rico assisted to several meetings during the Claro-Naicom deal negotiations since he was Claro's IPTV business Manager. During these meetings Mr. Carlos Garcia became privy to the technology and business details of the Claro-Naicom deal that would leave him jobless if Claro opted at the end and shut down the IPTV division he managed.

84. Upon information and belief Mr. Carlos Garcia fears moved him to alert the executives of Dish Network Puerto Rico that Claro-Naicom's IPTV deal would require the cancelation of Dish Network Satellite TV contracts with Claro and even he could lose his job. The Naicom-Claro IPTV deal news caused Dish Network great animosity towards Naicom TV in the industry of Cable and IPTV market.

85. August 14, 2018, after a year of meetings, the Naicom-Claro IPTV negotiation was a done deal. Nevertheless, for reasons unbeknownst to Naicom Corporation's executive officers,

Claro mysteriously disappeared from the table of negotiations and never informed Naicom Corporation why they pulled out of the deal.

86. Upon information and belief, the Dish Network defendants, informed Claro's executives to withdraw from the deal because the FBI was investigating Naicom and its founders for criminal prosecution.

C. THE DISH/NAGRASTAR DEFENDANTS INVOLVEMENT IN THE RACKETEERING ENTERPRISE'S CONSPIRATORIAL CRIMINAL OBJECTIVE IN THE THEFT OF PLAINTIFFS' TRADE SECRETS AND INTELLECTUAL PROPERTY.

87. On August 7, 2017, the Racketeering Enterprise contracted the Toltec defendants to purchase two (2) Naicom TV Set Top Box receivers so that the Association in Fact defendants could conduct reverse engineering on Plaintiffs' Intellectual Technology by analyzing the ports in the box for open SSH connections to be able to reach the box's operating system and thus extract the codes and image residing in Naicom's IPTV Set Top Box middle firmware. The Association in

Fact defendants also conducted sniffing to identify where the Naicom TV traffic was pointing to, and where its Facility resided. The Association in Fact defendants also conducted sniffing to attack and penetrate Naicom's servers, computers, and remotely access, capture usernames, passwords, exchange of security keys, encryption, analyze, monitor content and data information passing through the network without any explicit authorization from Plaintiffs, under the supervision and authority of the Legal Entity Enterprises.

88. Out of the two (2) Naicom TV Set Top Boxes (TV Box) acquired by the Association in Fact defendants one of the TV Box bearing MAC Address (00:1A:79:46:97:AD) and Serial Number (012017N024821), was sent to and maintained in the Racketeering Enterprise, premises, located in Denver, Colorado, and the attacks on Naicom's Data Center Facility came though the Racketeering Enterprise IP 8.18.116.2. The other TV Box bearing MAC Address (00:1A:79:46:A4:BE) and Serial Number (012017N028166), was kept and maintained in Toltec Investigations, LLC, premises, located in Tampa, Florida and the attacks on Naicom's Data Center Facility came though Toltec Investigations, IP 107.72.162.96.

89. In order to disguise the Association in Fact defendants fraudulent and illegal racketeering objectives, the defendant Michael T. Jaczewski, a.k.a. acting as Brian Parsons created an account via the internet on 03/07/2018 at 03:01 PM and placed an order via Naicom's website, and registered online under the following false pretenses; he alleged that he was customer: BRIAN PARSONS, Phone (727) 409-9464, Email: parsons.brian716@outlook.com with an Address at: 9079 FOURTH STREET NORTH SAINT PETERS FL 33702 IP: 70.127.233.139, using a Visa Credit Card ending in 2775, and purchased two Naicom's IPTV set top boxes, MAC Numbers 00:1A:79:46:97:AD; and 00:1A:79:46:A4: which he requested be mailed to Brian Parsons residence, via the United States Postal Service, to the above address. Brian Parsons later provided the Racketeering Enterprise one of the TV Boxes purchased.

90. According to the affidavit filed in support of the search warrant application the Association in Fact defendants collectively represented to the Court that their investigation revealed that the receiver provided access to approximately 43-channels- including channels such as Disney, TBS, ESPN, CNN, HBO, Showtime, and Cinemax; and that Naicom TV application could be downloaded through Apples'

Appstore, which required a registration to enable the subscriber to create its login credentials as the receiver and provided access to approximately 42 channels, and that after testing Naicom TV several times to identify if it was providing DISH programming, on each case the test revealed no DISH content.

91. Upon information and belief, the Association in Fact defendants also contacted several Media Network Companies[4] to inquire if Naicom had the appropriate licensing contracts and authorization to distribute its programming and on each occasion these defendants were informed that Naicom Corporation was authorized to distribute its content.

92. Upon information and belief, after performing the sniffing analysis on Plaintiffs Network, the Racketeering Enterprise learned through the Dish/Nagrastar defendants that Naicom's TV intellectual technology was transmitting Multicast (UDP Packets) over the internet, and performed its tv programming distribution service to its end user with the use of only 2mps per channel, and that this was a threat to the Racketeering Enterprise's product Sling

[4] It should be noted that Dish Network is a member of the same Network Media Companies that licensed Naicom the authorization to distribute television programming content

TV that represented future competition for subscribers in Puerto Rico and the United States.

93. The Dish/Nagrastar defendants also informed the Racketeering Enterprises that the Association in Fact defendants couldn't penetrate Naicom's Data Center computers, servers, encoders electronic security system, and that a physical intrusion was necessary to extract the intellectual property from the computers, servers, and encoders by physical access.

94. The Dish/Nagrastar defendants knew that by physically entering Naicom's Data Center and turning off the computers and servers, and connecting a USB boot up with Linux and turning on the server from the USB and not from the internal disk, they would access to the internal hard drive and bypass the security measures of the operating system installed on the hard drive.

95. The Racketeering Enterprise also knew that the intellectual property represented a new valuable technology worth of obtaining by any means necessary, even if it meant by illegal means, to advance its television programming distribution system, and authorized the Dish/Nagrastar defendants to form the

Association in Fact, and use the Legal Entity Enterprises to advance its conspiratorial objective in misappropriating the Plaintiffs of its intellectual technology and gain economic advantage in the television programming distribution market to the detriment of the plaintiffs business.

D. THE RACKETEERING ENTERPRISE ULTRA VIRES MOTIVES BEHIND THE ALLEGED CRIMINAL INVESTIGATION TO ROB PLAINTIFFS' INTELLECTUAL PROPERTY AND TRADE SECRETS.

96. On March 18, 2019, Dish Network Company filed its ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 with the UNITED STATES SECURITIES AND EXCHANGE COMMISSION, Washington, D.C. 20549 Form 10-K FOR THE FISCAL YEAR ENDED DECEMBER 31, 2018.

97. In said report Dish Network reported to its shareholders the risk companies like Naicom IPTV represented to their market as follows:

    a. Changing consumer behavior and competition from digital media companies

that provide or facilitate the delivery of video content via the Internet may reduce our subscriber activations and may cause our subscribers to purchase fewer services from us or to cancel our services altogether, resulting in less revenue to us.

b. Economic weakness and uncertainty may adversely affect our ability to grow or maintain our business.

c. Our competitors may be able to leverage their relationships with programmers to reduce their programming costs and/or offer exclusive content that will place them at a competitive advantage to us.

d. Our over-the-top ("OTT") Sling TV Internet-based services face certain risks, including, among others, significant competition.

e. If government regulations relating to the Internet change, we may need to alter the manner in which we conduct our Sling TV

business, and/or incur greater operating expenses to comply with those regulations

f. Technology in the pay-TV industry changes rapidly, and our success may depend in part on our timely introduction and implementation of, and effective investment in, new competitive products and services, and our failure to do so could cause our products and services to become obsolete and could negatively impact our business.

g. Competition, our business has historically focused on providing pay-TV services. We face substantial competition from established pay-TV providers and broadband service providers and increasing competition from companies providing/facilitating the delivery of video content via the Internet to computers, televisions, and other streaming and mobile devices, including wireless service providers. In recent years, the traditional pay-TV industry has matured, and industry consolidation and convergence has created competitor with greater scale and multiple

product/service offerings.

h. These developments, among others, have contributed to intense and increasing competition, and we expect such competition to continue.

i. We also face increasing competition from content providers and other companies who distribute video directly to consumers over the Internet. These content providers and other companies, as well as traditional satellite television providers, cable companies and large telecommunication companies, are rapidly increasing their Internet-based video offerings. Programming offered over the Internet has become more prevalent and consumers are spending an increasing amount of time accessing video content via the Internet on their mobile devices. In particular, consumers have shown increased interest in viewing certain video programming in any place, at any time and/or on any broadband-connected device they choose. Video content distributed

> over the Internet[5] includes services with live-linear television programming such as DirecTV Now, Sony PlayStation Vue, YouTube TV, Fubo TV, Philo TV and Pluto TV, as well as single programmer offerings such as HBO NOW, CBS All Access, STARZ and SHOWTIME and offerings of large libraries of on-demand content, including in certain cases original content, by companies such as Netflix, Hulu, Apple, Amazon, Alphabet and Verizon. Certain of these companies have invested extensive resources in producing original content that is exclusive to their platform.

98. Upon information and belief, the above information was the moving force behind the Racketeering Enterprises decision to have the Dish/NagraStar defendants file with the Legal Entity Enterprise the complaint against Naicom Corporation, which allegedly triggered the criminal investigation that culminated in the illegal and warrantless execution the

---

[5] The Racketeering Enterprise knew that Naicom TV is the only Live TV programming distribution company with Multicast system (DISME technology) capable of distributing UDC Packets over the Internet at a very low-cost effective bandwidth consumption and reliable infrastructure.

Federal and Dish/Nagrastar defendants performed at Naicom's Offices and Data Center Facility which resulted in the seizure of Plaintiffs' intellectual property and trade secrets stolen from their computers, servers, encoders, the hard and pen drives, belonging to D&V IP Holdings, Naicom, Kiara, and Paylink Corporations,

99. Such confidential, intellectual, and trade secret information is economically valuable to the Plaintiffs', and as described previously, its value extends far beyond the Racketeering Enterprise's Sling TV streaming and DISH Television distribution technology. The Racketeering Enterprise's access to Plaintiffs' Intellectual Technology, Confidential Information and Trade Secrets gives the Racketeering Enterprise an unfair competitive advantage with respect to future marketing of television programming distribution. The bell cannot be unrun—the Racketeering Enterprise cannot unlearn what they discovered and learned from that they stole from Plaintiffs'; it has now been improperly misappropriated, accessed, and Plaintiffs' do not have the means, absent judicial intervention, of preventing the Racketeering Enterprise from incorporating D&V IP Holding's DISME intellectual

technology and Naicom's IPTV trade secrets, confidential and proprietary information into the Racketeering Enterprises own streaming technology strategic plans and competing in the television programming distribution and public and private sector proposals contracts going forward, to Plaintiffs' business detriment.

100. Lastly, the Racketeering Enterprise defendants has a history of misappropriations with intellectual property and patents infringements belonging to other companies and owners, which have resulted in civil actions, and redress settlements amounting over $500,000,000.00 dollars.

E. THE FEDERAL DEFENDANTS' CONSPIRATORIAL INVOLVEMENT AND USE OF THE LEGAL ENTITY ENTERPRISES TO FACILITATE BY ILLEGAL MEANS THE DISCH/NAGRASTAR DEFENDANTS ACCESS TO PLAINTIFFS' BUSINESS PREMISSES TO ADVANCE THE RACKEETERING ENTERPRISES ILLEGAL PURPOSE OF STEALING PLAINTIFFS' INTELLECTUAL PROPERTY AND TRADE SECRETS.

101. The Association in Fact defendants collectively knew for a fact that the electronic data and the FF proof analysis information collected from Plaintiffs' Data Center through electronic sniffing investigation, revealed that Naicom TV was authorized to distribute programming content from the networks, since pirated material does not contain close caption and second audio program in its illegal tv distribution.

102. The Association in Fact defendants also knew that collected evidence in the Legal Entity Enterprise's investigatory files, logs, notes, memorandums, reports of investigation, photographs, videos, "the collected evidence," negated any criminal wrongdoing that Naicom's founders were committing the crimes charged in the search and seizure warrant affidavit and application, and yet, proceeded with the Racketeering Enterprise conspiratorial criminal objectives of stealing from Plaintiffs its intellectual and trade secrets property through the illegal and warrantless search and seizure execution.

103. At the conclusion of the first illegal search and seizure warrant execution AUSA Jose Capo -Iriarte, and USA Rosa E. Rodriguez-Velez learned that Naicom TV counted with

all the programming distribution contract and agreements and ordered AUSA Nicholas W. Cannon to instruct the defendant FBI S/A Kevin Pearson to order Darwin Quinones and Victor Vega to report to the FBI Offices in San Juan with the licensing contracts for an interview regarding Naicom's company.

104. At the San Juan FBI offices the Federal defendants lead by FBI S/A Kevin Pearson in one table with the Dish/NagraStar defendants Jordan Smith, Kevin Gedeon, FBI S/A Lance Lange, together with Bert Eichhorn and Emily Rinkle in another table posing as federal agents questioned Darwin Quinones in the presence of Naicom's legal Attorney Patricia Rivera as to how Naicom acquired the IPTV distribution contracts with the content providers and inquired as to the technology Naicom was using to distribute the programing via private networks and the internet, inspected Naicom's contracts with the Networks Content Providers, containing trade/ business secrets and confidential information justifying D&V IP Holdings DISME technology content programming distribution contracts belonging strictly to Naicom Corporation as trade secret business information.

105. On August 29, 2019, the defendants Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-

Iriarte, AUSA Nicholas W. Canon, knowing that Naicom' TV was in fact a legitimate IPTV business company, and that there was no probable cause or criminal reason to send back the federal agents nor the Dish/Nagrastar defendants into Naicom's Data Center Facility, instructed for a second time Federal defendants Lance Lange, Kevin Pearson to return to Naicom's Data Center with the Dish/NagraStar defendants Jordan Smith, Kevin Gedeon and Bert Eichhorn who posing as federal agents illegally, and using the keys misappropriated from Naicom's Offices without authorization entered without a search warrant Naicom's Data Center, located at Villa Fontana, 4SS N2 Via Josefina, Carolina, PR.

106. Upon entering Naicom's Data Center defendants Lance Lange and Kevin Pearson authorized Dish/NagraStar defendants Jordan Smith, Kevin Gedeon and Bert Eichhorn without Plaintiffs' authorization permission to penetrate Naicom's Data Center and introduce pen drives into D&V IP Holdings and Naicom's computers and servers, and conducted "password dump" by unlawfully performing passwords resets into the Ubuntu controlling system, changing credentials from authorized users,

conducting an access to the D&V IP Holdings and Naicom's domains to resume the misappropriation of Plaintiffs intellectual property, trade secrets and confidential information for the Racketeering Enterprise.

107. Upon defendants Lance Lange, Kevin Pearson, Jordan Smith, Kevin Gedeon and Bert Eichhorn almost completing its second illegal search and unauthorized intrusion and access of the Naicom's Data Center computers, servers and other hardware equipment for prolonged hours, defendant Kevin Pearson decided to contact Naicom's employee Jaime Echevarria at his cell phone and ordered him to show up at the Data Center under the ruse that he wanted to interrogate him, Darwin, and Mr. Vega.

108. Upon arriving at Data Center Darwin Quinones observed defendants Lance Lange, Kevin Pearson allowing in their presence defendants Jordan Smith, Kevin Gedeon and Bert Eichhorn still posing as federal agents, accessing Naicom's Data Center computers, servers, other hardware equipment containing Intellectual Property, Trade Secrets, and Confidential Information without authorization.

109. During the execution of the warrantless search

defendants Kevin Pearson and Lance Lange instead of interrogating Darwin Quinones, began to pressure him into signing a hold harmless document accepting he was running a pirate operation in the past so that they could close the case or else his boss had given him orders to shut down the Data Center operation.

110. Darwin Quinones rejected the proposition outright, and defendants Kevin Pearson and Lance Lange implored Darwin Quinones to sign the document so that they could close the case or else they were going to have problems, but Darwin Quinones again refused to do so.

111. Sometime thereafter, Mr. Vega showed up at the scene and upon entering the Data Center asked defendants Kevin Pearson and Lance Lange if they had another search warrant to enter and search the Data Center. Defendant Lance Lange represented to Mr. Vega that the search warrant gave him ten (10) days to search the Data Center, although, the probable cause, dissipated the moment they executed and concluded the first search which was fruitless without any criminal information to report. Mr. Vega reacted and told defendant Lance Lange to leave Naicom's Data Center premises because he was violating the United States Constitution and Federal law.

112. At that time, Mr. Vega informed defendants Kevin Pearson and Lance Lange that he had already discovered via LinkedIn that the alleged FBI experts who executed the search and seizure warrants at Naicom, Artist Designs, Kiaras, LLC and Naicom's Data Center, who interrogated him, and Darwin Quinones at the FBI Offices were Kevin Gedeon, investigator of Dish Network and Jordan Smith, Bert Eichhorn and Emily Rinkle investigators of NagraStar.

113. Mr. Vega also questioned defendants Lance Lange and Kevin Pearson as to why they brought his competition to search, inspect, and photograph confidential information and allowed them to access computers and servers containing trade secrets codes sources, business, and intellectual property information belonging to the Plaintiff's corporations.

114. The Dish/NagraStar and Federal defendants insisted to continue with the execution of the warrantless search, unauthorized intrusion and access into Naicom's Data Center computers and servers, and Mr. Vega called his Attorney and notified him that the FBI agents were executing a second warrantless search and seizure at Naicom's Data Center, and after speaking to defendant Lance Lange, the defendants shut down Naicom's business

operation and left the premises.

F. THE DEMAND FOR RETURN OF PROPERTY CONTAINING CONFIDENTIAL INFORMATION UNDER RULE 41(G)

115. On September 6, 2019, a Motion for DEMAND for Return of Seized Property was filed Pursuant to Federal Rules of Criminal Procedure 41(g) ("The Rule 41(g) Motion") by Rafael F. Castro-Lang on behalf of Artist Designs and Management Corporation, Kiaras, LLC, Naicom Corporation, Naicom Data Center, Darwin Quinones-Pimentel, Victor Vega-Encarnacion ("The Plaintiffs"). [D.E. 1 Civil Docket 3:19-mc-00308-FAB].

116. On November 5, 2019, the District Court granted Plaintiff's Rule 41(g) Motion and entered the following: ("ORDER re 12 Notice (Other), re 10 Report and Recommendation, re 1 Motion for Return of Property: NOTED. Claimant having waived the 14-day period to file objections to the Report and Recommendation (R&R), the Court ADOPTS the R&R and orders the government to return the property listed in claimant's demand. (Docket No. 1)" pursuant to Rule 41 of the

Federal Rules of Criminal Procedure. [D.E. 12 and 13 Civil Docket 3:19-mc-00308- FAB].

117. The Government never opposed nor denied that the underlying basis for the search warrant was false and the search warrant against plaintiffs was dismissed on the government's own motion. [D.E. 9-page 1 Civil Docket 3:19-mc-00308-FAB].

G. THE SIGNIFICANT HARM INFLICTED UPON PLAINTIFFS.

118. The Association in Fact defendants actions in using the Legal Entity Enterprise and the judicial system to intrude into Naicom Corporation, Data Center, Paylink and Kiaras, LLC, files, cabinets, safe boxes, computers, servers, hardware, secure storage rooms, to photograph and download data containing business confidential information, intellectual property, trade secrets, proprietary solutions, source codes compilation and programs, to facilitate the Racketeering Enterprise the opportunity to steal Plaintiffs intellectual property and trade secrets caused significant damages to Plaintiffs.

119. The Racketeering Enterprises defendant's misappropriation of D&V IP Holdings' DISME

technology and Naicom's IPTV intellectual property and trade secrets confidential Information and copyright material gives the Racketeering Enterprises an unfair competitive advantage with respect to future of television programming distribution technology and marketing. The Racketeering Enterprises discovery, from what they stole from D&V IP Holdings DISME technology and Naicom's trade secrets information will now be improperly used by the Racketeering Enterprises to advance the distribution technology of their products such as Sling-TV through Multicast system over the internet and private networks, a technology which they did not have a clue existed, and could not develop, since they only deliver the distribution of programming using satellite, and unicast over -the-top streaming systems, which would unfairly enrich the Racketeering Enterprises, while destroying Plaintiffs' business.

120. Prior to the execution of the search warrants, Plaintiffs enjoyed a great reputation and were about to close an investment deal of $15,000,000.00 dollars to advance Naicom's goals to the next level of launching the brand in the United States by 2019 in the States of Florida and New York.

121. When the investors found out that Naicom Corporation and its executive officers were under criminal investigation and that their offices were raided by the FBI, the investors emailed Darwin Quinones that they were abandoning the negotiations due to the pending criminal investigation.

122. Naicom Corporation was also about to close a multimillion contract with Claro Puerto Rico by August 2018. When the executive officers of Claro Puerto Rico found out through Dish Network that the FBI was investigating Naicom Corporation and that their executive officers were about to be arrested and prosecuted, and Naicom was about to be dismantled for running an illegal IPTV pirate content distribution operation, Claro Puerto Rico pulled out of the negotiations and never again contacted Naicom's executive officers to renew them.

123. In the aftermath of the search warrant execution of Naicom's Data Center, Naicom lost a great deal of subscribers because of the negative reputation caused by the defendants. Furthermore, the Dish/NagraStar and Federal defendants' intrusion into Naicom's Data Center computers, servers and other equipment caused enormous damages to the Data Center computers and server's system

leaving many subscribers without tv programming services for weeks, causing Plaintiffs the expense of having spent over $500,000.00 and man hours resources in repairing and acquiring new equipment due to the damages caused by the defendants actions in shutting down the Data Center telecommunication electronic services and intruding into computers and servers hard drive security and program systems.

CAUSE OF ACTION

COUNT ONE RICO (18 U.S.C. § 1962(C))

(AGAINST ALL DEFENDANTS)

124. Plaintiff realleges and incorporates by reference all prior paragraphs of this Second Amended Complaint and paragraphs in the counts below as set forth fully herein.

A. The Association in Fact Defendants criminal efforts, and the use of the Legal Entity Enterprise to advance the of the Racketeering Enterprises criminal objectives.

125. At all relevant times, the Dish Network Corporation, Dish Network, LLC and

NagraStar Corporation, LLC are the Racketeering Enterprises, as that term is used in 18 U.S.C. § 1961(4) & (5), and 18 U.S.C. § 1962(c).

126. At all relevant times, the Dish/NagraStar defendants Emily Rinkle, Bert Eichhorn, Jordan Smith, and Kevin Gedeon, in association with Federal defendants U.S. Attorney Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, the Toltec Defendants, Several Unknown Named Agents of the Federal Bureau of Investigations, and John Does constitute an Association in Fact, as that term is defined within the meaning of 18 U.S.C. § 1961(4).

127. At all relevant times, the Association in Fact was formed to advance the Racketeering Enterprises criminal objective in robbing D&V IP Holdings DISME intellectual technology property and Naicom's Corporations trade secret confidential information through a pattern of racketeering activities, consisting of Mail and Wire fraud, and the misappropriation of trade secrets, which affected interstate commerce, in violation of 18 U.S.C. § 1962(c).

128. The Association-In-Fact's closed-ended continuity began when it was formed by its defendants in July 2017 or, at the very least, by June 2017 and ended in August 2019. The Association in Fact defendants committed at least over 30 racketeering acts in their criminal conspiratorial objective to steal from Plaintiffs the D&V IP Holdings DISME intellectual technology property and Naicom's Corporation's trade secrets confidential information.

129. The Racketeering Enterprises conduct also represent a legitimate threat of open-ended continuity pattern of racketeering acts and crimes that may be repeated in the future because of the Racketeering Enterprise's ongoing regular way of business is to attempt steal Intellectual Property, Patents,[6] and Trade Secrets, from their owners every time they can do so. Since 1999, the Racketeering Enterprises have been accused of committing the following crimes and torts against other companies similarly situated in the Plaintiffs' conditions

---

[6] See 18 U.S.C. Section 1839 (definitions) (7) the term "Trademark Act of 1946" means the Act entitled "An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes1, approved July 5, 1946 (15 U.S.C. 1051 et seq.) (commonly referred to as the 'Trademark Act of 1946' or the 'Lanham Act')"

and circumstances: (1) IPPS Enterprise, LLC, filed a civil action against Nagrastar, LLC and EchoStar Communications Corp., which operates Dish Network TV services, and were found guilty by jury trial for infringing IPPS Enterprise intellectual Patent, resulted in a $15 million dollars lump sum damage award, (Case No. 99-cv-577-RRM, (D. Delaware 1999), see also IPPS Enterprise v. EchoStar Communications, 191 F.Supp.2d 530 (D. Del. 2002)(Denying motions for new trial and judgment as a matter of law); (2) TiVo Inc., a Delaware corporation, filed a civil action against Dish Network for infringing TiVo intellectual Patent property, which resulted in a $500 million dollars settlement (Case No. 2-04-cv-01 DF, (E.D.TEXAS 2006); (3) United States and Four States, filed a civil action against Dish Network for violations of the Telemarketing Antitrust and Trade Regulations, which resulted in a bench trial guilty verdict and a total of $280 million dollars judgment award (Case No. 09-cv-3073 (C.D. Illinois 2009)(ECF #870); (4) Disney Enterprise, filed a civil action against Dish Network, for the unauthorized distribution of copyright material, Dismissed by Stipulation, (Case No. 11-cv-2973, (S.D. New York 2011); (5) California Institute of Technology, filed a civil action against Dish Network for infringing its Patent, which resulted in joint stipulation dismissal (Case No. 13-cv-7245

(C.D. Cal. 2013); (6) TQ Beta, LLC, filed a civil action against Dish Network for infringing its Patent, which resulted in joint stipulation dismissal pending Patent resolution (Case No. 14-cv-848 (D. Del. 2014); (7) IPA Technologies Inc., filed a civil action against Dish Network, for Patent Infringement, Dismissed by Stipulation (Case No. 16-cv-1170, (D. Delaware 2016); (8) Real Time Data, LLC d/b/a IXO, filed a civil action against Dish Network for infringing its Patent, which resulted in joint stipulation dismissal settlement (Case No. 17-cv-84 (E.D. Texas 2017), see also resolution of the case at Real Time Data, (2018 WL 1959319); and (9) Unilock 2017, LLC, filed a civil action against Sling TV, for Patent Infringement, Dismissed by Stipulation (Case No. -19-cv-278, (D. Colorado 2019). Twenty years of continuing criminal and tortious misconduct in misappropriating themselves with patents, technologies, trade secrets and intellectual property belonging to others.

130. The Association-In-Fact defendants had an ongoing organizational framework for carrying out the Racketeering Enterprises criminal objectives. The Association-In-Fact defendants could not have carried out the intricate task of robbing Plaintiffs' Intellectual Property and Trade Secrets confidential information for the Racketeering Enterprises, unless it had some

structure for making and communicating group decisions, so that the Dish/NagraStar defendants Emily Rinkle, Bert Eichhorn, Jordan Smith, and Kevin Gedeon could participate directly with the defendants U.S. Attorney Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations; John Does 1-20, into Plaintiffs pirate hoax criminal investigation, and use the powers of the Legal Entity Enterprises to deceive the judiciary in authorizing an otherwise illegal search and seizure warrant execution and also execute a second warrantless search and seizure to facilitate the Racketeering Enterprises the opportunity to the entrance into Plaintiff's premises and complete its criminal and conspiratorial objective goal as fully described above.

131. The Association-In-Fact and the Racketeering Enterprises criminal activities affected interstate and foreign commerce because D&V IP Holdings DISME technology economic value is estimated in the hundreds of millions of dollars.

B. RICO Predicate Acts

132. The Dish/NagraStar defendants Emily Rinkle, Bert Eichhorn, Jordan Smith, and Kevin Gedeon, and Federal defendants U.S. Attorney Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Named Agents of the Federal Bureau Of Investigations, and John Does 1-20 conduct and participation in the affairs of the Racketeering Enterprise criminal goals and conspiratorial objectives consisted in the following pattern of racketeering activity, including acts indictable under Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy to Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.), while in addition, committing the possible underlying criminal offenses as prohibited under Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.), 18 U.S.C.A. § 2235- Search warrant procured maliciously; 18 U.S.C.A. § 1621- Perjury generally; 18 U.S.C.A. § 1001-

Statements or entries generally, 18 U.S.C.A. § 912- Officer or employee of the United States; 18 U.S.C.A. § 2234-Authority exceeded in executing warrant; 18 U.S.C.A. § 2236-Searches without warrant, 18 U.S.C.A. § 1905-Disclosure of Confidential Information, while accomplishing their racketeering objectives.

1. The Mail Fraud

133. On August 7, 2017, the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, instructed Toltec, Investigation, President and CEO, Michael T. Jaczewski, to pose as Brian Parsons, and purchased from Naicom Corporation a TV Set Top Box receiver to conduct reverse engineering on Naicom's IPTV Set Top Box middle firmware in their attempt to misappropriate themselves with the intellectual technology property. The defendant Toltec Investigations, President and CEO, Michael T. Jaczewski, also facilitated the Racketeering Enterprises a Set-Top-Box and both conducted sniffing to attack and penetrate Naicom's servers and computers, and remotely access and capture usernames, passwords, exchange of security keys, encryption, and analyze and monitor content

and data information passing through the network without any authorization from Plaintiffs. This action constitutes a mail fraud racketeering act since A.K.A. Brian Parsons posed as a legitimate client and used the United States Postal Services to have Naicom mail him the IPTV Set Top Box to a fake address, at 9079 FOURTH STREET NORTH SAINT PETERS FL 33702 to defraud and deprive Naicom Corporation from its legitimate products, intellectual property and trade secrets. This operation was supervised and approved by Federal defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, and FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, John Does 1-20, by using the authority of the Legal Entity Enterprises.

2. The Wire Fraud

134. On August 7, 2017, the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, instructed Toltec, Investigation, President and CEO, Michael T. Jaczewski, to pose as Brian

Parsons, and purchase a Naicom TV Set Top Box receiver to conduct reverse engineering on Naicom's IPTV Set Top Box middle firmware in their attempt to misappropriate themselves with the intellectual technology property. The defendant Toltec, Investigation, President and CEO, Michael T. Jaczewski, also facilitated the Racketeering Enterprises a Set-Top-Box and both conducted sniffing to attack and penetrate Naicom's servers and computers, and remotely access and capture usernames, passwords, exchange of security keys, encryption, and analyze and monitor content and data information passing through the network without any authorization from Plaintiffs. This action constitutes a wire fraud racketeering act since A.K.A. Brian Parsons posed as legitimate client and used the interstate internet electronic services to access Naicom's website, and register online under the false pretenses of BRIAN PARSONS, fake Phone (727)409-9464, fake Email: parsons.brian716@outlook.com and Address: 9079 FOURTH STREET NORTH SAINT PETERS FL 33702 IP: 70.127.233.139, and made online payments through the use of interstate internet electronic services using the PM Visa ending in 2775, to purchase two Naicom's IPTV set top boxes, MAC Numbers

00:1A:79:46:97:AD; and 00:1A:79:46:A4:, to defraud and deprive Naicom Corporation of its legitimate products, intellectual property and trade secrets. This operation was supervised and approved by U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, and FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents of Federal Bureau Of Investigations, John Does 1-20, by using the authority of the Legal Entity Enterprises.

135. The Toltec, Investigation defendants, wire fraud scheme lasted two years from 2017 up to 2019, and the defendant President and CEO, Michael T. Jaczewski, posing as Brian Parsons, kept paying Naicom its monthly subscription online through the internet electronic services using his PM Visa ending in 2775, knowingly and intentionally making 22 acts of racketeering fraudulent wiring payments for the total amount of $1,304.81 for a fake subscription, to defraud and deprive Naicom Corporation from its legitimate products, intellectual property and trade secrets, as prohibited pursuant to 18 U.S.C. § 1343. This operation was supervised and approved by the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert

Eichhorn, Emily Rinkle, Brian Parsons, and federal defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, and FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez Several Unknown Names Agents Of Federal Bureau Of Investigations, John Does 1-20, by using the authority of the Legal Entity Enterprises.

136. See table below reflecting Toltec, Investigations, Brian Parsons wired transactions

Transaction of Brain Parsons Customer 1745

Order Number	ClientID	order date	delivery	amount
195	1745	2017-08-07 15:32:49	Shipping	$130.00
271	1745	2018-01-25 19:27:11	Shipping	$130.00
345	1745	2018-03-07 16:53:23	Digital	$54.99
492	1745	2018-05-14 13:18:15	Digital	$54.99
585	1745	2018-06-10 17:16:39	Digital	$54.99
664	1745	2018-07-10 08:38:15	Digital	$54.99
763	1745	2018-08-11 09:00:02	Digital	$54.99
805	1745	2018-08-24 20:22:45	Digital	$54.99
899	1745	2018-09-23 09:00:21	Digital	$54.99
931	1745	2018-09-28 14:58:49	Digital	0
932	1745	2018-09-28 15:02:34	Digital	$54.99
1022	1745	2018-10-27 15:49:32	Digital	$54.99
1119	1745	2018-11-25 14:43:35	Digital	$54.99

1213	1745	2018-12-23 14:06:42	Digital	$54.99
1308	1745	2019-01-21 16:32:11	Digital	$54.99
1424	1745	2019-02-19 07:35:11	Digital	$54.99
1550	1745	2019-03-24 09:00:02	Digital	$54.99
1671	1745	2019-04-21 15:00:45	Digital	$54.99
1800	1745	2019-05-21 00:12:04	Digital	$54.99
1934	1745	2019-06-22 09:00:02	Digital	$54.99
2043	1745	2019-07-22 09:00:01	Digital	$54.99
2185	1745	2019-08-21 09:00:02	Digital	$54.99

3. The Mail and Wire Fraud Conspiracy

137. The factual allegations in paragraphs 133 and 136 including the scheme to defraud set out therein, are realleged and incorporated herein as if set forth in full. The Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, agreement in knowingly and intentionally conspiring with federal defendants U.S.A. Rosa Emilia Rodriguez-Velez, A USA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations; John Does 1-20, while using the authority of the Legal Entity Enterprise in committing the mail and wire fraud offenses

described herein to advance the Racketeering Enterprise defendants conspiratorial and criminal objectives in depriving Naicom of its intellectual property violated 18 U.S.C. § 1341 and 1343 and 1349.

4. Theft of Trade Secrets

138. Beginning on or before August 7, 2017, the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, associated themselves with defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agent Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations; John Does 1-20, and used the power of the Legal Entity Enterprises to repeatedly attempt—and successfully—stole, and without authorization misappropriated, took, carried away, or by fraud, artifice, or deception obtained trade secrets from D&V IP Holdings and Naicom's corporation intellectual property and trade secrets with the intent to convert those trade secrets, which are and were related to products or services used in or intended for use in interstate commerce, to the economic benefit of the Racketeering Enterprises, intending and

knowing that the offense would injure D&V IP Holdings and Naicom's corporations and business in violation of 18 U.S.C. § 1832(a)(1) and (a)(4).

139. Beginning on or before August 7, 2017, the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, associated themselves with the defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 by using the power of the Legal Entity Enterprise, did without authorization, spy, reverse engineered, copied, duplicated, downloaded, uploaded, altered, destroyed, replicated, transmitted, delivered, sent, communicated, and/or conveyed intellectual property and trade secrets from D&V IP Holdings and Naicom's corporation, with the intent to convert those trade secrets, which are related to products or services used in or intended for use in interstate commerce, to the economic benefit of the Racketeering Enterprises and other defendant coconspirators, intending and knowing that

the offense would injure D&V IP Holdings and Naicom's corporation, in violation of 18 U.S.C. § 1832(a)(2).

140. Beginning on or before August 7, 2017, the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, associated with the defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, using the power of the Legal Entity Enterprise possessed D&V IP Holdings and Naicom's corporation trade secrets, with the intent to convert those trade secrets, which are related to products or services used in or intended for use in interstate commerce, knowing the same to have been stolen and misappropriated, obtained, or converted without authorization, to the economic benefit of Racketeering Enterprises and other defendant coconspirators, intending and knowing that the offense would injure the D&V IP Holdings, Naicom, Kiaras and Paylink Corporations, in violation of 18 U.S.C. § 1832(a)(3).

141. On August 27 and 29, of 2019, the Federal

defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 used the power of the Legal Entity Enterprise, facilitating and assisting the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, the entry and access without authorization into D&V IP Holdings and Naicom's corporation computers and servers containing trade secrets, with the intent to facilitate the Dish/NagraStar defendants the opportunity to convert those trade secrets, which are and were related to products or services used in or intended for use in interstate commerce, to the economic benefit of Racketeering Enterprises, intending and knowing that the offense would injure D&V IP Holdings and Naicom's corporations and business, in violation of 18 U.S.C. § 1832(a)(2).

5. RICO DAMAGES.

142. Plaintiffs have been injured in its business and property by Defendants' violation of 18 U.S.C. § 1962(c). Defendants caused enormous harm to Plaintiff's business, as described above, and

to Plaintiff's computers and servers. All of these injuries occurred within the United States.

143. The defendant Juan Galarza is liable because as a computer science officer for the FBI he knew for a fact that the electronic data information he collected through electronic sniffing investigation and the FFproof analysis he performed on Plaintiffs' Data Center revealed that Naicom TV was authorized to distribute programming content from the networks, and yet opted to conspire with the Association in Fact defendants in advancing the Racketeering Enterprises criminal and conspiratorial objectives, knowing that the Racketeering Enterprises had a history of misappropriations of patents and intellectual property, and illegal misconduct which the United States had already successfully litigated in a civil action against them.

144. The defendant Jason Lopez is liable because as the evidence technician for the FBI he knew for a fact that the evidence he collected from the television networks, the crime scene during the illegal search and seizure warrant execution, the evidence he preserved, documented, and analyzed in the course of the Naicom alleged

pirate investigation, revealed that Naicom was running a legitimate IPTV operation, and yet opted to conspire with the Association in Fact defendants in advancing the Racketeering Enterprises criminal and conspiratorial objectives, knowing that the Racketeering Enterprises had a history of misappropriations of patents and intellectual property, and illegal misconduct that the United States had already successfully litigated a civil action against them.

145. The defendants FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, are liable because they knew or should have known that after they contacted the TV Networks, and reviewing the evidence provided by the defendants Jason Lopes and Juan Galarza, and the collected evidence, Naicom Corporation was running a legitimate IPTV operation, and yet opted to conspire with the Association in Fact defendants in advancing the Racketeering Enterprises criminal and conspiratorial objectives, knowing that the Racketeering Enterprises had a history of misappropriations of patents and intellectual property, and illegal misconduct that the United States had already successfully litigated a civil action against

them.

146. The defendants FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, are furthermore liable, because upon executing the first illegal search and seizure warrant, these defendants became aware that Naicom Corporation had all the contracts and licensing to operate an IPTV business, and yet felicitated the Dish/Nagrastar defendants the entrance for a second time into Naicom' Data Center premises and without a warrant authorized them to penetrate Plaintiffs' computers and servers to advance the Racketeering Enterprises criminal and conspiratorial objectives, to rob Plaintiffs' intellectual property and trade secrets knowing of the Racketeering Enterprises history of misappropriations of patents and intellectual property.

147. The defendants FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Jason Lopez and Juan Galarza are furthermore liable, because they knew or should have known that the evidence collected negated any criminal wrongdoing that Naicom's founders were committing the crimes charged in the search and seizure warrant affidavit and application, and yet,

proceeded to the end, and used the power of their Legal Entity Enterprise, to move the judiciary to issue an illegal search and seizure warrant execution, to advance the Racketeering Enterprise conspiratorial criminal objectives in stealing Plaintiffs' intellectual and trade secrets property.

148. The defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, are furthermore liable because while guiding and advising the Federal Special Agents and participating directly in Naicom Corporation criminal investigation, they knew or should have known that the evidence collected did not meet the elements of the crime charged in the sworn affidavit, and yet, proceeded to the end, and used the power of their Legal Entity Enterprise, to move the judiciary to issue an illegal search and seizure warrant execution, to advance the Racketeering Enterprise conspiratorial criminal objectives and stealing Plaintiffs' intellectual and trade secrets property.

149. The defendants the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle are liable because they knew or should have known that by forming an Association in Fact with the Federal

defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, and the Toltec Investigations and President and CEO, Michael T. Jaczewski defendants, and using the Legal Entity Enterprise to advance the Racketeering Enterprise conspiratorial criminal objectives in attempting and stealing Plaintiffs' intellectual and trade secrets property was illegal and prohibited as described above.

150. The Toltec Investigations and President and CEO, Michael T. Jaczewski defendants are liable because they knew that the Racketeering Enterprises had a history of misappropriations of patents and intellectual property, and knew or should have known that it is a crime in the United States to use the mail or the interstate internet electronic telecommunication systems to advance a fraud in an attempt to deprive an owner of his intellectual property for its own benefit or the benefit of another, and yet decided to form part of the Association in Fact defendants to advance the Racketeering Enterprise conspiratorial criminal objectives in attempting to steal Plaintiffs' intellectual and

trade secrets property.

151. The Association in Fact defendants are furthermore liable because they knew or should have known that by agreeing that the operation would involve repeated violations of Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy to Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.), their actions constituted racketeering acts violations as that conduct is prohibited under RICO 18 U.S.C. § 1962(c) and § 1962(d).

152. As fully described above, the Federal defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 are furthermore more liable because they knew or should have known that the Racketeering Enterprises had a history of misappropriating themselves from Patents, Intellectual Property and Trade Secrets belonging to others, and although they were charged with the authority to investigate and enforce the Mail and Wire, Theft of Trade

Secrets, and RICO laws of the United States, instead opted for participating in the crime as fully described above. The Association in Fact defendants are furthermore liable because they knew or should have known that their actions were criminal under established law and prohibited at the time under the United States statutory laws.

COUNT TWO

RICO CONSPIRACY (18 U.S.C. § 1962(D))
(AGAINST ALL DEFENDANTS)

153. Plaintiffs reallege and incorporate by reference all prior paragraphs of this Complaint and those in the counts below as though set forth fully herein.

154. The Association-In-Fact defendants conspired with each other to violate 18 U.S.C. § 1962(c). The Association-In-Fact defendants knowingly agreed, combined, and conspired to conduct the affairs of the Racketeering Enterprise in attempting and committing theft of trade secrets through a hoax criminal investigation operation. Each Defendant agreed that the operation would involve repeated violations of Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy To Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade

Secrets Act (18 U.S.C. § 1836 et seq.), involving the commission of underlying criminal offenses of the Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.), 18 U.S.C.A. § 2235-Search warrant procured maliciously: 18 U.S.C.A. § 1621- Perjury generally, 18 U.S.C.A. § 1001- Statements or entries generally, 18 U.S.C.A. § 912- Officer or employee of the United States; 18 U.S.C.A. § 2234- Authority exceeded in executing warrant; 18 U.S.C.A. § 2236- Searches without warrant, 18 U.S.C.A. § 1905- Disclosure of Confidential Information, while accomplishing their conspiratorial racketeering objectives, all in violation of 18 U.S.C. § 1962(c) and § 1962(d).

155. Plaintiffs have been injured in their business and property by Defendants' joint violation of 18 U.S.C. § 1962(d) and1962(c). Defendants caused enormous harm to Plaintiff's business, as described above, and to Plaintiff's computers and servers. All these injuries occurred within the United States.

156. Paragraphs 143 though 153 are incorporated herein by reference and made part hereof as fully described above.

COUNT THREE

COMPUTER FRAUD AND ABUSE ACT

(18 U.S.C. § 1030(A))

157. Plaintiff realleges and incorporates by reference all prior paragraphs of this Complaint and paragraphs in the counts below as though set forth fully herein.

158. As described above the Naicom Offices and Data Center computers are involved in interstate and foreign commerce and communication and are protected computers under 18 U.S.C. § 1030(e)(2).

159. On August 27, 2019, The Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, and Federal defendants FBI Special Agents Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations; John Does 1-20, did knowingly and intentionally accessed Naicom Offices and Data Center computers without authorization or in excess of authorization, obtained and used valuable information from those computers in violation of 18 U.S.C. § 1030(a)(2)(C). Such information included, but was not limited to intellectual property, trade secrets and confidential information. The information was used to advance the Racketeering Enterprise conspiratorial

criminal objectives in stealing Plaintiffs' intellectual and trade secrets property and give ther Racketeering Enterprise economic advantage and destroy Plaintiffs' business.

160. On August 29, 2019, The Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, and Federal defendants FBI Special Agents Lance Lange, Kevin Pearson, Several Unknown Names Agents Of Federal Bureau Of Investigations; John Does 1-20, did knowingly and intentionally access the Naicom Offices and Data Center computers without authorization or in excess of authorization, obtained and used valuable information from those computers in violation of 18 U.S.C. § 1030(a)(2)(C). Such information included, but was not limited to intellectual property, trade secrets and confidential information. The information was used to advance the Racketeering Enterprise's conspiratorial criminal objectives in stealing Plaintiffs' intellectual and trade secrets property and give the Racketeering Enterprise economic advantage and destroy Plaintiffs' business. The Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and Federal defendants FBI Special Agents Lance Lange, Kevin Pearson,

Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents of Federal Bureau Of Investigations, and John Does 1-20, did intentionally accessed a protected computer or computers without authorization, and as a result of such conduct, caused damage and loss, in violation of 18 U.S.C. § 1030(a)(5)(C) and 18 U.S.C. § 1030(a)(5)(B) to D&V IP Holdings and Naicom corporations.

161. The Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, and Federal defendants FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, caused loss to one or more persons during a one-year period aggregating well over $5,000 in value, and they also caused damages affecting ten or more protected computers during a one-year period.

162. The Naicom Corporation suffered damages and losses as a consequence of the Dish/NagraStar and Federal defendants' actions, including but not limited to the cost of investigating and responding to the unauthorized access and abuse of their computer networks, conducting damage assessments, restoring, and replacing computers, servers and data, programs,

systems, or information, the loss of the value of the D&V IP Holdings and Naicom's trade secrets, and the harm to Naicom's business as described above. The D&V IP HOLDINGS, NAICOM, KIARAS AND PAYLINK CORPORATIONS seeks compensatory and other equitable relief under 18 U.S.C. § 1030(g).

163. The defendants FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza and Jason Lopez are liable because they knew or should have known that by intentionally authorizing and allowing the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle to access Plaintiffs' computers and servers without authorization or in excess of the authorization granted, the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle were going to have access and in fact steal valuable information of the D&V IP Holdings and Naicom's trade secrets, to harm to Naicom's business as described above.

164. The defendants the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle are liable because they knew or should have known that by intentionally accessing Plaintiffs' computers

and servers without authorization to steal valuable information of the D&V IP Holdings and Naicom's trade secrets, to harm to Naicom's business as described above, constituted a crime as prohibited 18 U.S.C. § 1030(a).

165. As fully described above, the Federal defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 are liable because they knew or should have known that the Racketeering Enterprises had a history of misappropriating themselves from Patents, Intellectual Property and Trade Secrets belonging to others. They were charged with the authority to investigate and enforce fraud and related activity in connection with computers under the Computer Fraud And Abuse Act laws of the United States, and instead opted to participate and/or allowed the commission of the crime as described above.

166. The defendants FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez and the Dish/NagraStar

defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle, Several Unknown Names Agents of Federal Bureau Of Investigations, and John Does 1-20 are furthermore liable because they knew or should have known that their actions were criminal under established law and prohibited at the time under United States statutory laws.

COUNT FOUR

STORED COMMUNICATIONS ACT

(18 U.S.C. §§ 2701-12)

167. Plaintiffs reallege and incorporate by reference all prior paragraphs of this Complaint and paragraphs in the counts below as though set forth fully herein.

168. Plaintiffs are a "person" within the meaning of 18 U.S.C. §§ 2510(6) and 2707(a)

169. On August 27 and 29, 2019 the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza and Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, willfully and intentionally accessed without authorization a facility which operates

servers, encoders, computers, and telecommunications systems and technology, by electronically transmitting communications involved in Webservers, Email-Servers, Carrier Grade Routers which interconnected with local ISP providers through Border Gateway Protocols (BGP) in exchanging routing information between autonomous systems. A Facility which also uses Satellite Dish systems to downloaded video encrypted content, and delivers telephone fixets, internet, video programming distribution, and data information, through Tower Cells Air Fiber Antennas radio frequency transmissions. A Facility which also operates Customer Relation Management programs which effectuate electronic transmissions to collect and make payments transactions from partners and customers' accounts through gateway and merchant financial systems, as those terms are defined through which an electronic communication service is provided, namely, the D&V IP Holdings, Naicom's IPTV, Kiaras' and Paylink's services, electronic programs and computer systems, thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18

U.S.C. § 2701(a).

170. As a result of these willful and intentional violations, as above described, Plaintiffs have suffered damages and, as provided in 18 U.S.C. § 2707, seeks an award of the greater of the actual damages suffered or the statutory damages; punitive damages; attorneys' fees and other costs of this action; and appropriate equitable relief.

171. The Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, and defendants FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza and Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 are liable because they knew or should have known that obtaining access without authorization to wire or electronic communications while they were in electronic storage in such systems, constituted a violation of 18 U.S.C. § 2701(a), as those terms are fully described above.

172. The Federal defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez Several Unknown Names Agents

Of Federal Bureau Of Investigations, and John Does 1-20 are liable because they knew or should have known that the Racketeering Enterprises had a history of misappropriating themselves from Patents, Intellectual Property and Trade Secrets belonging to others, and they were charged with the authority to investigate and enforce the Store Communications Act laws of the United States, and instead opted to participate and facilitate the commission of the crime as described above.

173. The defendants FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, and the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle, Juan Galarza and Jason Lopez, and Several Unknown Names Agents of the Federal Bureau of Investigation, and John Does 1-20 are furthermore liable because they knew or should have known that their actions were criminal under established law and prohibited at the time under United States statutory laws.

COUNT FIVE

DIGITAL MILLENNIUM COPYRIGHT ACT

(17 U.S.C. § 1201 ET SEQ.)

174. Plaintiffs reallege and incorporates by reference all prior paragraphs of this

Complaint and paragraphs in the counts below as though set forth fully herein.

175. Plaintiff's computer networks and files contained information subject to protection under the copyright laws of the United States, including software programs, documents, confidential information, and research.

176. On August 27 and 29, 2019, Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons were illegally authorized by Federal defendants FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, and Jason Lopez Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, to access without legal authorization, the Paylink Corporation copyrighted material contained in Paylink's computer software programs, systems, and networks controlled by technological measures, including measures restricting remote access, firewalls, and measures restricting access to users with valid credentials and passwords.

177. The Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, Brian Parsons, circumvented these technological measures when they were illegally authorized by the Federal Bureau Of Investigation, FBI Special Agents Lance Lange, Kevin Pearson,

Clay Rehrig, Juan Galarza, Jason Lopez, and Several Unknown Names Agents Of Federal Bureau Of Investigations to introduce pen drives into D&V IP Holdings and Naicom's computers and servers, authorized and allowed to conduct "password dump" by unlawfully performing passwords resets into the Ubuntu controlling system, changing credentials from authorized users, conducting an access to the D&V IP Holdings and Naicom's domains, in violation of 17 U.S.C. § 1201(a).

178. The Dish/NagraStar and Federal defendant's conduct caused Plaintiffs significant damages. These damages include, but are not limited to, damages resulting from harm to Paylink's computers and servers, loss in the value of D&V IP Holdings and Naicom's trade secrets and confidential business information, and harm to the business as described above. Plaintiff is entitled to the greater of its actual damages or statutory damages as provided by 17 U.S.C. § 1203, in an amount to be proven at trial.

179. Plaintiff is entitled to an award of attorneys' fees and costs as provided by 17 U.S.C. § 1203.

180. The defendants FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza and Jason Lopez, and Several

Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 are liable because they knew or should have known that by illegally trespassing the Naicom Data Center Facility they did not have any legal authority whatsoever to authorize and allow the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, access illegally, the Paylink Corporation's copyrighted material contained in electronic storage in Plaintiffs' computer's hard drive and systems.

181. The Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, are liable because they knew or should have known that trespassing into the Naicom Data Center Facility to obtaining access without authorization to wire or electronic communications while they were in electronic storage in such systems, constituted a crime violation of 18 U.S.C. § 2701(a), as those terms are fully described above.

182. The Federal defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez Several Unknown Names Agents Of Federal Bureau Of Investigations, and John

Does 1-20 are liable because they knew or should have known that the Racketeering Enterprises had a history of misappropriating themselves from Patents, Intellectual Property and Trade Secrets belonging to others, and they were charged with the authority to investigate and enforce the Digital Millennium Copyright Act laws of the United States, and instead opted to participate and/or facilitate the Racketeering Enterprises committing the crime as fully described above.

183. The defendants FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, and the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle, Juan Galarza and Jason Lopez, and Several Unknown Names Agents of Federal Bureau Of Investigations, and John Does 1-20 are liable because they knew or should have known that their actions were criminal under established law and prohibited at the time under the United States statutory laws.

COUNT SIX

MISAPPROPRIATION OF TRADE SECRETS UNDER THE DEFEND TRADE SECRETS ACT

(18 U.S.C. § 1836 ET SEQ.)

184. Plaintiffs reallege and incorporates by reference all prior paragraphs of this

Complaint and paragraphs in the counts below as though set forth fully herein.

185. The DISME technology, Intellectual Property and Confidential Information the Racketeering Enterprise defendants stole from D&V IP Holdings, and Naicom's Corporation, are trade secrets within the meaning 18 U.S.C. section 1839 (3)(A)&(B)(4)(5)(A)&(6)(A), as the terms have been fully described above.

186. D&V IP Holdings and Naicom Corporation are in the business of networks and internet communications, IPTV and internet services. The misappropriation of the confidential and digital information of D&V IP Holdings' DISME technology, Naicom's, Kiaras', and Paylink's trade secrets, research, and business strategies and other confidential information was essential to the future of Plaintiffs business, as those terms are described in 18 U.S.C. section 1839(3)(A)&(B). Plaintiff's trade secrets were related to products or services used in, or intended for use in, interstate or foreign commerce, as those terms are described in 18 U.S.C. section 1832(a). As stated above D&V IP Holdings and Naicom has taken reasonable measures to keep such confidential information protected and secret, as those terms are described in 1839(3)(A).

187. On August 27 and 29, 2022 the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle, conspired with the Federal defendants FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza and Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 to gain access and actually entered Naicom's Data Center with the assistance an collaboration of Federal defendants, FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza and Jason Lopez, whom facilitated the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle unauthorized, illegal access to Plaintiffs computers and servers in order to steal and actually stole intellectual property and trade secrets belonging to the Plaintiffs' for the benefit of the Racketeering Enterprises and to the detriment of Plaintiffs' business all in violation of 18 U.S.C. section 1832 (a)(1)(2)(4)(5).

188. The Federal defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez Several Unknown Names Agents

Of Federal Bureau Of Investigations, and John Does 1-20, conduct and actions in assisting and facilitating the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, and Emily Rinkle access to Plaintiffs' computers and servers to deprive the Plaintiffs of their trade secrets, knowing or having reason to know that the trade secrets were being acquired by improper means, by using the Legal Entity Enterprise under the hoax of a criminal investigation to advance the Racketeering Enterprises conspiratorial objectives as fully described above were committed in violation of 18 U.S.C. § 1832(a), as those terms are fully described in 18 U.S.C. § 1839 (5)(A)&(6)(A).

189. As a direct consequence of Defendants' misappropriation, Plaintiff has suffered damages for the cost of materials, loss of goodwill, and attorneys' fees and costs. Plaintiff is also entitled to punitive damages. These damages include, but are not limited to, damage resulting from harm to D&V IP Holdings and Naicom computers and servers, loss in the value of D&V IP Holdings, DISME technology, and Naicom, Kiaras and Paylink trade secrets and business information, and harm to its business as described above.

190. Plaintiff is also entitled to a preliminary and

permanent injunction pursuant to 18 U.S.C. § 1836(b)(3).

191. As fully described above, the Federal defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 are liable because they knew or should have known that the Racketeering Enterprises had a history of misappropriating themselves from Patents, Intellectual Property and Trade Secrets belonging to others, and after completing their alleged criminal investigation, and learning for a fact that Naicom Corporation was running a legitimate IPTV operation, yet they opted for conspiring, and actually participating with the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle in the theft of Plaintiffs' trade secrets by facilitating them access to Plaintiffs' Data Center, through the use of the Legal Entity Enterprises, when the Federal defendants knew that the computers and servers contained intellectual property and trade secrets, so that the Dish/Nagrastar defendants could steal the

intellectual property and trade secrets for the benefit of the Racketeering Enterprises as fully described above.

192. The Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle are liable because they knew or should have known that accessing Plaintiffs' Data Center computers and servers with the sole intent to steal and actually rob Plaintiffs' intellectual property and trade secrets to advance the technology distribution systems, economic growth and value of the Racketeering Enterprise to the detriment of Plaintiffs business by illegal means, was criminal, and in violation of the statutory laws of the United States as prohibited under 18 U.S.C. § 1832(a).

193. The Federal defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Jason Lopez Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20 are liable because they knew or should have known that the Racketeering Enterprises had a history of misappropriating themselves from Patents, Intellectual Property and Trade Secrets belonging to others, and they were charged with the authority to investigate

and enforce the Theft of Trade Secrets laws of the United States, and instead opted to participate and facilitate the crime as fully described above. The Dish/Nagrastar defendants would have never gained access to Plaintiffs computers, other hardware, trade secrets and intellectual property without the assistance of the federal defendants.

194. The Federal defendants FBI Special Agents Lance Lange, Kevin Pearson, Clay Rehrig, and the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn and Emily Rinkle, Juan Galarza and Jason Lopez, and Several Unknown Names Agents of Federal Bureau of Investigations, and John Does 1-20 are furthermore liable because they knew or should have known that their actions were criminal under established law and prohibited at the time under United States statutory laws.

COUNT SEVEN

PUERTO RICO INDUSTRIAL AND TRADE SECRETE PROTECTION ACT UNDER THE UNIFORM TRADE SECRETS ACT

(LAW NO. 80, OF JUNE 3, 2011)

(AGAINST ALL DEFENDANTS)

195. Plaintiffs reallege and incorporate by reference all prior paragraphs of this Complaint and paragraphs in the counts below as though set forth fully herein.

196. The Puerto Rico Industrial and Trade Secrete Protection Act Under the Uniform Trade Secrets Act empowers a party to recover damages for misappropriation of a trade secret.

197. The Confidential Information the Dish/NagraStar defendants Kevin Gedeon, Jordan Smith, Bert Eichhorn, Emily Rinkle misappropriated from Plaintiffs, through association, assistance and facilitation of the defendants U.S.A. Rosa Emilia Rodriguez-Velez, AUSA Jose Capo-Iriarte, AUSA Nicholas W. Cannon, FBI Special Agents Douglas A. Leff, Bradley Rex, Lance Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, Several Unknown Names Agents Of Federal Bureau Of Investigations, and John Does 1-20, exfiltrated from the D&V IP Holdings and Naicom computer systems trade secrets under Puerto Rico law, as discussed above, and in keeping with the definition of trade secrets under Puerto Rico law: information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (A) Derives actual or potential independent economic value, from not being generally

known, and not being readily ascertainable by proper means by another who can obtain economic value from its disclosure or use; and (B) Is the subject of reasonable efforts to maintain its secrecy, pursuant to Section 11 of Puerto Rico Industrial and Trade Secrets Protection Act (Law No. 80, of June 3, 2011).

198. This information derived an actual independent economic value by remaining confidential and private, and not being readily ascertainable to others. Plaintiffs have taken reasonable measures to keep such information secret, as described and discussed above.

199. Each Defendant disclosed, received, and used these misappropriated trade secrets without Plaintiff's consent, knowing or having reason to know that the trade secrets were acquired by improper means.

200. As a direct consequence of Defendants' attempt or misappropriation, Plaintiffs have suffered damages for actual loss and from Defendants' unjust enrichment. These damages include, but are not limited to, damage resulting from harm to D&V IP Holdings, Naicom computers and servers, loss in the value of D&V IP Holdings, Naicom trade secrets and business information, and harm to its business as described above.

201. Defendants' misappropriation of Plaintiff's trade secrets was willful and malicious.

202. Paragraphs 194 though 197 are incorporated herein by reference and made part hereof as fully described above.

203. Accordingly, Plaintiff is entitled to exemplary damages in an amount up to twice actual damages awarded, as well as attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment against Defendants on all Counts, and seeks such relief as specified below for all Counts for which such relief is provided by law:

a) Awarding Plaintiff damages in an amount to be determined, including but not limited to all damages and losses suffered by Plaintiff as a result of the illegal attempt to steal or theft, and subsequent release of Plaintiff's confidential information and/or Plaintiff's response to and remediation related thereto; Awarding Plaintiff compensatory in excess of $100,000,000 (One Hundred Million dollars) and treble damages, as available, in an amount to be proven at trial;

b) Awarding Plaintiff the financial gain earned by

Defendants as a consequence of the violations described herein;

c) Awarding Plaintiff statutory damages, as available;

d) Awarding Plaintiff punitive damages exceeding $500,000,000.00 (Five Hundred Million dollars);

e) Issuing a declaration that; Defendants, according to proof, conspired and engaged in a common scheme to obtain the illegal and unauthorized attempt or misappropriation of Plaintiff's computer systems and the exfiltration of confidential information;

f) Issuing an injunction restraining Defendants and their officers, agents, servants, employees, assigns, and those acting in active concert or participation with them from accessing Plaintiff's computer networks and/or personal emails without Plaintiff's authorization;

g) Engaging in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of Plaintiff's computer systems, programs, and networks; and

h) Selling, publishing, distributing, or using any property or information obtained from

Plaintiff's computer systems, programs and networks without Plaintiff's authorization;

i) Removing, extracting, or copying any information or data from Plaintiff's computers systems, programs without Plaintiff's authorization;

j) Awarding Plaintiff all costs and attorneys' fees to the full extent permitted under applicable law;

k) Awarding Plaintiff pre- and post-judgment interest as permitted by law;

l) Awarding any other relief as the Court may deem just and proper.

JURY DEMAND: Pursuant to the Seventh Amendment of the United States Constitution, and Rule 38 of the Federal Rules of Civil Procedure, Plaintiff demands trial by jury in this action of all issues so triable.

RESPECTFULLY SUBMITTED.

I hereby certify that on this same date, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties involved.

In San Juan, Puerto Rico, this 6th day of October 2022.

S/ Rafael F. Castro Lang

RAFAEL F. CASTRO LANG

USDC-PR#128505

Attorney for Defendant

P O Box 9023222

San Juan PR 00902-3222

Tel: (787) 723-3672 / (787) 723-1809

Fax: (787) - 725-4133

Email: rafacastrolang@gmail.com;
rafacastrolanglaw@gmail.com

UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

No. 24-1416

Naicom Corporation, et al.,

Plaintiffs-Appellants,

v.

Dish Network Corporation, et al.,

Defendants-Appellees.

Rule 28(j) Letter — Supplemental Authority and Clarification

Pursuant to Fed. R. App. P. 28(j), Appellants respectfully submit the following supplemental authority and clarification in connection with oral argument held on October 30, 2025.

This appeal presents a **statutory controversy**, not a constitutional or *Franks v. Delaware*, 438 U.S. 154 (1978), challenge. The issue in Counts III–VI is whether the federal and private defendants acted **without lawful statutory authorization** when they re-entered Naicom's data center on **August 29, 2019**,

two days after executing and closing the August 27 warrant. Each relevant statute—the **Computer Fraud and Abuse Act** (18 U.S.C. §1030(f)), **Stored Communications Act** (18 U.S.C. §2707(e)), **Digital Millennium Copyright Act** (17 U.S.C. §1201(e)), and **Defend Trade Secrets Act** (18 U.S.C. §1833(a)(1))—limits its law-enforcement exception to "**lawfully authorized investigative activity.**" That authority ends once a warrant is executed and returned.

Under Michigan v. Tyler, 436 U.S. 499, 511–12 (1978); and Bilida v. McLeod, 211 F.3d 166, 171–72 (1st Cir. 2000); a warrant's authority expires upon execution; any later re-entry to collect evidence is a **new search requiring a new warrant.** Once the government executed and returned the August 27 warrant and acknowledged Naicom's lawful licensing, there was no continuing authorization.

The **August 29 re-entry**, performed by FBI agents and Dish/NagraStar engineers using **keys taken from Naicom's offices** to access servers belonging to **D&V IP Holdings,**

Paylink, and Kiaras LLC—entities unrelated to IPTV piracy—was therefore a **new, unauthorized intrusion** under *Tyler* and *Bilida*. Because this re-entry lacked statutory authorization, the law-enforcement exceptions do not apply, and the conduct alleged satisfies the elements Congress prohibited under the **CFAA, SCA, DMCA, and DTSA**, providing RICO predicates. This Circuit is bound to decide the case under **statutory-construction principles**, not constitutional "good-faith" or *Franks* standards. *Franks* is inapposite: the August 29 entry involved **no warrant or affidavit**; the issue is solely the **legality of a warrantless intrusion** into servers unrelated to piracy.

Appellants therefore request, remand for further proceedings on Counts III–VI. Respectfully submitted,

/s/ Rafael F. Castro-Lang
Fed.Cir.Bar #26074
P.O. Box 9023222
San Juan, P.R. 00902-3222 Tel: (787) 723-3672
Email: rafacastrolang@gmail.com;
Dated: November 3, 2025

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

United States Constitution, Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

18 U.S.C. § 1965 (Venue and process)

(a) Any civil action or proceeding under this chapter against any person may be instituted in the district court of the United States for any district in which such person resides, is found, has an agent, or transacts his affairs.

(b) In any action under section 1964 of this chapter in any district court of the United States in which it is shown that the ends of justice require that other parties residing in any other district be brought before the court, the court may cause such parties to be summoned, and

process for that purpose may be served in any judicial district of the United States by the marshal thereof.

(c) In any civil or criminal action or proceeding instituted by the United States under this chapter in the district court of the United States for any judicial district, subpoenas issued by such court to compel the attendance of witnesses may be served in any other judicial district, except that in any civil action or proceeding no such subpoena shall be issued for service upon any individual who resides in another district at a place more than one hundred miles from the place at which such court is held without approval given by a judge of such court upon a showing of good cause.

(d) All other process in any action or proceeding under this chapter may be served on any person in any judicial district in which such person resides, is found, has an agent, or transacts his affairs.

18 U.S.C. § 3105 (Persons authorized to serve search warrant)

A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other

person, except in aid of the officer on his requiring it, he being present and acting in its execution.

18 U.S.C. § 1030(f) (Computer Fraud and Abuse Act)

This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

18 U.S.C. § 2707(e) (Stored Communications Act—Defense)

A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3), section 2702(b)(9), or section 2702(c)(7) of this title permitted the conduct complained of; is a complete

defense to any civil or criminal action brought under this chapter or any other law.

17 U.S.C. § 1201(e) (Digital Millennium Copyright Act)

This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State.

18 U.S.C. § 1833(a) (Defend Trade Secrets Act—Exceptions)

This chapter does not prohibit or create a private right of action for—

(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or

(2) the disclosure of a trade secret in accordance with subsection (b).

28 U.S.C. § 1254(1) (Courts of appeals; certiorari)

Cases in the courts of appeals may be reviewed by the Supreme Court by the following methods:

(1) By writ of certiorari granted upon the petition of any party to any civil or criminal case, before or after rendition of

judgment or decree[.]