No. _____

In the
Supreme Court of the United States

ROYAL TRUCK & TRAILER SALES AND SERVICE, INC.,
Petitioner,

v.

MIKE KRAFT AND KELLY MATTHEWS A/K/A KELLY SCHLIMMER,
Respondents.

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

PETITION FOR WRIT OF CERTIORARI

ANTHONY M. SCIARA
Counsel of Record
ROYAL TRUCK & TRAILER
311 East Cady Street
Suite C
Northville, Michigan 48167
(248) 773-3775
asciara@royaltrailersales.com

Counsel for Petitioner

Becker Gallagher · Cincinnati, OH · Washington, D.C. · 800.890.5001

QUESTION PRESENTED

Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose. See also *Nathan Van Buren v. United States*, 140 S. Ct. 2667 (2020) (petition for a writ of certiorari to the United States Court of Appeals for the Eleventh Circuit granted on the same issue) (Supreme Court Docket Number 18-12024).

PARTIES TO THE PROCEEDING AND RULE 29.6 STATEMENT

1. Royal Truck & Trailer Sales and Service, Inc. – plaintiff-petitioner. No parent or publicly held company owns 10% or more of Royal Truck & Trailer Sales and Service, Inc.'s stock.
2. Mike Kraft – defendant-respondent.
3. Kelly Matthews a/k/a Kelly Schlimmer – defendant-respondent.

STATEMENT OF RELATED PROCEEDINGS

There are no proceedings that are directly related to this case.

TABLE OF CONTENTS

APPENDIX

TABLE OF AUTHORITIES

Cases

Statutes

Rules

OPINIONS BELOW

(1) The United States District Court for the Eastern District of Michigan issued its Opinion and Order Granting Defendants' Motion to Dismiss, Dismissing Without Prejudice Plaintiff's Remaining State Law Claims, and Denying as Moot Defendants' Motion to Stay Discovery on March 11, 2019 ("Decision"). The Decision is not reported. A citation to the Decision is 2019 WL 1112387. The Decision is reproduced in the Appendix at App. 16-25. (2) The United States Court of Appeals for the Sixth Circuit issued its Opinion on September 9, 2020. The Opinion is reported. The citation to the Opinion is 974 F.3d 756 (2020). The Opinion is reproduced in the Appendix at App. 1-15.

STATEMENT OF JURISDICTION

The United States District Court for Eastern District of Michigan had jurisdiction (1) over Counts I and II of the First Amended Complaint pursuant to 28 U.S.C. § 1331; and (2) over Counts III through IX of the First Amended Complaint pursuant to 28 U.S.C. § 1367. The United States Court of Appeals for the Sixth Circuit had jurisdiction over the appeal from the United States District Court for the Eastern District of Michigan pursuant to 28 U.S.C. § 1291. This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

FEDERAL STATUTORY PROVISION INVOLVED

28 U.S.C. § 1030(a)(2)(C)(g):

(a) Whoever--

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(C) information from any protected computer;

shall be punished as provided in subsection © of this section.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.…

STATEMENT OF THE CASE

Royal, Mike, and Kelly

Petitioner-Plaintiff Royal Truck & Trailer Sales and Service, Inc. ("Royal") is a Midwestern supplier and servicer of new and used semi-trailers, trucks, parts, and accessories. (RE 8, Complaint, Page ID #39). Respondents-Appellees Mike Kraft ("Mike") and Kelly Matthews a/k/a Kelly Schlimmer ("Kelly") (collectively "Defendants") were previously employed by Royal. (Id.). Mike was employed as a Service Advisor and Salesperson for Royal. (Id.). Mike was responsible for (a) quoting pricing for the provision of repair and maintenance services on semi-trailers and trucks for potential, and actual, Royal customers; and

(b) managing Shop Technicians to ensure services were properly and timely performed. (Id.). Kelly was employed as an Outside Salesperson in the Parts Division for Royal. (Id. at Page ID #40). Kelly was responsible for maintaining existing business relationships and developing new business relationships on behalf of Royal with potential, and actual, customers interested in purchasing parts from Royal for their semi-trailers, trucks, and related items. (Id.).

Royal's Company Policies

Mike and Kelly were aware of, and familiar with, the policies described in the Employee Handbook. (RE 8, Complaint, Page ID # 40). In early 2018, Mike was provided the Employee Handbook and instructed to review it. (Id.). On February 7, 2018, Mike signed the Employee Handbook Acknowledgement, which is located on the second-to-last page of the Employee Handbook. (Id.). The acknowledgement states: "I have read, understand and agree to all of the above." (Id.). In early 2018, Kelly was provided the Employee Handbook and instructed to review it. (Id.). On February 23, 2018, Kelly sent herself an email from her Royal account to her personal account, which attached an unsigned copy of the Employee Handbook Acknowledgement. (Id.).

The Employee Handbook contains (among others) the following policies:

a. "Examples of prohibited conduct are ... [u]nauthorized removal or use of any company property or that of a customer or coemployee….";

b. "Examples of prohibited conduct are … [w]asting, impairing or altering company property....";

c. "All employees are required to return computers, cell phones, tools, manuals, training manuals, customer and pricing lists, files, keys, uniforms, sales office vehicles, supplies, or any other Company property.";

d. "The Company provides PTO for employees to take time for rest and recuperation.";

e. "Company equipment must be maintained in the best possible manner…. This includes but is not limited to computer equipment and data stored thereon, voice mail, records and employee files…. [T]he use of Company equipment/property for personal activities is strictly prohibited.";

f. "Employees are responsible for items issued to them by the Company or in their possession or control, such as but not limited to … [d]atabase information … [c]ustomer lists … [f]iles and documents … [c]omputers, software, manuals, and informational resources … [c]ell phones.";

g. "Although the Company strives to ensure that each employee has access to the resources needed to perform his/her job, the Company also expects all employees to understand that use of those resources is limited to the performance of their jobs. Any unauthorized use, retention or disclosure of any Company resources or property will be regarded as theft warranting disciplinary action up to and including termination and may prompt various civil and/or criminal legal actions.";

h. "All content created, saved, and/or shared using the Company's traditional and electronic communication and information systems are a form of corporate correspondence, and are subject to the same internal and external regulation, security and scrutiny as any other corporate correspondence.";

i. "Employees shall not attempt to gain access to another employee's personal information systems and messages.";

j. "The Company's electronic information systems are to be used for Company business only.";

k. "Hardware (computers, laptops, tablets, and smart phones) and software (computer files, the e-mail system), furnished to employees are Company property intended for business use.";

l. "The equipment, services, and technology provided to access the Internet remain at all times the property of the Company.";

m. "The following behaviors are examples of previously stated or additional actions and activities that are [considered] prohibited [abuse of the Internet access provided by the Company] and can result in disciplinary action: … [s]ending or posting trade secrets, or proprietary information outside of the organization.";

n. "Company-provided cell phones are intended to be used for business purposes."; and

o. "Upon termination of employment, or at any time upon request, employees may be required to return

> the company-provided cell phone to the supervisor/manager or Human Resources. If company-provided cell phones are lost, damaged due to negligence, or not returned, employees may be responsible for the cost of replacement, unless state or local law require otherwise."

(RE 8, Complaint, Page ID #41-42).

In addition to the above Policies, the Employee Handbook also contains the following "Information Security/Confidentiality" policy:

> **Information Security/ Confidentiality**
>
> Employees have been entrusted with one of our most valuable assets -- information -- and they have the responsibility to protect it and to see that it is used only for its intended business purpose. We use information on a dally basis that could be useful to competitors and others who would misuse it.
>
> Confidential information may include, but is not limited to:
>
> - Computer records
> - Word processing documents
> - Letters and memos
> - Paper reports
> - Electronic Data Storage
> - Conversation

- Passwords and access codes
- Employment records and applications
- Client information (Social Security numbers, phone numbers, account numbers, etc.)

The classified information must be protected from disclosure to competitors and those who would misuse it. Whether employees work With paper records, at a computer terminal, or spend most of their day on the phone, employees are part of the Company's information security systems. This does not include the sharing of information regarding wages, hours, or other terms and conditions of employment.

Remember these rules when employees handle confidential information:

- Do not disclose to anyone outside the company any business-related information relating to the Company that has not been disclosed to the public, without appropriate management approval or as required by law, at any time during or **after** their employment. Don't even share this information with other Employees unless they have a business need to know about it. This does not include employee communication of information regarding wages, hours, or other terms and conditions of employment.

- Routinely take precautions to keep confidential information from being disclosed. This includes making sure such information is not displayed on our desks or in their work area where it can be seen by anyone. Employees should also avoid transmitting information Via a computer or by fax in ways that might make it available to unauthorized people.
- Require third-party recipients of restricted company information to keep such information confidential.
- Do not reveal Company trade secrets or the trade secrets of a previous employer or accept improperly obtained proprietary information about another company.
- Maintain the confidentiality of private information and proprietary information from customers, suppliers and other third parties that comes to our attention under an understanding of confidentiality. We must maintain the proprietary nature of such information and not use or disclose it without proper written authority.
- Logging off from their computer when leaving a work area

- Assuring that hard copies of member, employee or applicant information are kept in a locked area when employees are away from their work area
- Always shred any paperwork that includes any confidential information. Do not throw this into the regular trash cans or bins.
- Be mindful of clearing items from office equipment (fax/copier) and mail stations.
- Staff should never ask employees for their Windows password and sensitive information, in person, over the phone or via email. Unusual requests should be verified in dual with the requestor's manager and the employee's manager.

(RE 8, Complaint, Page ID #43-44).

In addition to the above Policies in the Employee Handbook, Kelly was also aware of, and familiar with, Royal's cellular phone GPS Tracking Policy. (RE 8, Complaint, Page ID #44). Among other things, the policy provides that "[e]mployees may not disable or interfere with the GPS (or any other) functions on a company issued cell phone" and "[e]mployees may not remove any software, functions or apps at any time." (Id.). On November 11, 2017, Kelly signed an acknowledgement that states: "I have received and am required to read and abide by the [Royal] GPS Tracking Policy set forth above." (Id.).

The Resignations and Investigation

On February 22 and 23, 2018, Defendants suddenly resigned from their employment with Royal without any advance notice. (RE 8, Complaint, Page ID #44). Shortly after their resignations, Royal learned Defendants had quickly begun working for a competitor of Royal, T-N-T Trailer Sales L.L.C. ("TNT"). (Id.). In a similar manner to Royal, TNT describes itself as a "full service semi-trailer dealership … located … in the Detroit Michigan area" that "has a full service and parts department to handle all your transportation needs." (Id. at Page ID #45). In an effort to ensure valuable, sensitive, confidential, and/or proprietary company property and information had not been compromised by Defendants, Royal subsequently began investigating Defendants' conduct before their resignations. (Id.).

The investigation revealed a substantial amount of nefarious and illegal conduct:

Date	**Significant Events**
2/14/18 (Wednesday)	(1) 4:39 p.m. – Kelly sends Mike an iMessage from her personal cellular phone stating: "Hey call me as soon as you can." (2) 4:41 p.m. – Kelly sends Mike another iMessage from her personal cellular phone stating: "Don't forget. Very important."
2/17/18 (Saturday)	(1) 4:08 p.m. – Mike receives an SMS message on his company cellular phone from another Royal employee,

	"Brian," which asks: "Hey Mike where is TNT located…" (2) 4:09 p.m. – Mike answers Brian by stating: "Please don't text this number bro" and "Call me at 313 770 7053." The number provided by Mike is his personal cellular phone number. (3) 5:25 p.m. – Mike sends a message to "Brian Cell Xtra" stating: "Call me when you have time bro. I need to talk." Upon information and belief, "Brian Cell Extra" is Brian Bladen, the operations manager for Royal customer, XTRA Lease. (4) 5:29 p.m. – "Brian Cell Xtra" responds by stating: "Ok. I'm in Ann Arbor. I will call you when I get home." (5) 5:54 p.m. – Mike responds with only a " ." (6) 6:34 p.m. – Mike receives a call from "Brian Cell Xtra" and has a conversation for more than fifteen (15) minutes.
2/18/18 (Sunday)	(1) 7:44 a.m. – Mike forwards a quote for a Royal customer, Ryder Livonia, on a CVS Maxon BMR Liftgate, from his Royal email account to his personal email account. (2) 8:32 a.m. – Mike sends an

	iMessage to his manager, Mike Morrison, which states: "I will be not be coming in Monday or Tuesday due a personal family emergency sir." (3) 11:01 a.m. – Mike forwards an email from his Royal email account to his personal email account, which attaches the image of a paystub for another Royal employee, Service Technician, Kerry Young. (4) 12:01 p.m. – Mike forwards an email from his Royal email account to his personal email account, which attaches the image of a paystub for another Royal employee, Parts Salesperson, Samuel Hernandez.
2/19/18 (Monday)	(1) 10:41 a.m. – Mike receives an iMessage stating: It's LB!! Congrats on the new job brother !! Dylan was telling me about it." (2) 10:58 a.m. – Mike receives an iMessage from another Royal employee, "Nick," asking" "Everything alright?. (3) 11:35 a.m. – Mike responds to Nick stating: "Yes just had to get some personal stuff handled."
2/20/18 (Tuesday)	(1) 11:44 a.m. – Mike receives an iMessage from someone named "Sherri," which states: "Love you back congratulations on your job rockstar"

	(2) 11:45 a.m. – Mike sends an iMessage to "Sherri," which states: "Save this other number it's my personal 313 770 7053" (3) 4:23 p.m. – Mike receives a "Happy Birthday" iMessage from someone named "Dave Hase." (4) 5:33 p.m. – Mike responds to "Dave Hase" by stating: "Thanks brother. Save this number it's my personal 313 770 7053 " (5) 7:03 p.m. – Mike sends an iMessage to his manager, Mike Morrison, stating: "Sorry but I'm going to need the rest of the week off. See you Monday morning." (6) 7:09 p.m. – Mike Morrison responds by stating: "I hope you're ok. Take care."
2/21/18 (Wednesday)	(1) 6:37 a.m. – Mike sends an iMessage to a Royal employee, "Nick," which states: "Sorry but I'm taking the week off." (2) 7:40 a.m. – Nick responds stating: "Is everything okay?" (3) 8:15 a.m. – Mike responds stating: "Not really but Its going to get better I hope." (4) 11:06 a.m. – Mike sends an email from his Royal email account to a

	Senior Service Manager at Ryder Truck Rental (a customer of Royal), which states: "Can you send me all the new vendor info , so I can get on board with you. Please make sure its all sent to this email mckraft220@ gmail.com." (5) 8:01 p.m. – Mike forwards a quote for a Royal customer, Gemini Transport LLC, on a Hendrickson Subframe Box, from his Royal email account to his personal email account. (6) Mike deletes and reinstalls the entire operating system on his company provided computer (laptop) at some point this day. The delete and reinstall overwrites everything, which effectively renders all data destroyed and unrecoverable.
2/22/18 (Thursday)	(1) 4:31 p.m. – Mike receives an iMessage from a Royal employee, "Frank," which states: "Checking on you. Things ok?" (2) 4:43 p.m. – Mike responds stating: "As best as the can be buddy." (3) 7:48 p.m. – Kelly sends an email from her Royal account to Mike's personal email account with the words "Here's some", which attaches a "Salesperson Summary Report" that contains confidential and proprietary

	information regarding the month-to-date revenue, profits, and other details relating to eight of the salespeople in Royal's Parts Division. (4) 8:00 p.m. – Mike attempts to send an email to every employee of Royal, but succeeds only in sending the email to Royal's senior leadership, managers, and some other employees, which attaches a resignation letter. The resignation letter states: "Please accept this letter as notice of my resignation from my position as senior service advisor effective immediately. I have received a position at another company and after careful consideration; I realize that this opportunity is too exciting for me to decline."
2/23/18 (Friday)	(1) 10:55 a.m. – Kelly forwards an email from her Royal account to her personal email account, which contains a sales inquiry (containing customer specific pricing information) from seven days earlier (2/13) allocated to Kelly (by her manager) through Royal's sales analytic software system (sales-i), and with a direction for Kelly to "reach out to your contact and try to get our foot in the door with Kitmasters."

	(2) 10:00 a.m. - 12:00 p.m. (approximately) – Royal employees, Mike Morrison and Paul Rodriguez, travel to Mike's home and obtain the return of his company provided computer (laptop) and cellular phone. (3) 10:28 a.m. – Kelly forwards an email from her Royal account to her personal email account, which attaches an unsigned Employee Handbook Acknowledgment and an unsigned Confidentiality Policy and Pledge. (4) 10:29 a.m.-12:08 a.m. – Kelly visits Royal's corporate headquarters, returns her company owned laptop and cellular phone, and immediately resigns. Kelly's cellular phone has been reset to factory settings, which effectively rendered all data on the phone destroyed and unrecoverable. (5) 12:09 p.m. – Kelly shares a link on Facebook to the YouTube video for the Johnny Paycheck song, "You can take this job and shove it," with the statement: "And this is how today went."

(RE 8, Complaint, Page ID #45-49) (bold removed) (underline in original).

In (most) pertinent part, the investigation revealed that, during the days before resigning, Mike and Kelly intentionally accessed their company-owned computers and cellular phones to:

a. forward a quote for a Royal customer, Ryder Livonia, on a CVS Maxon BMR Liftgate, from Mike's Royal email account to his personal email account;

b. forward an email from Mike's Royal email account to his personal email account, which attached the image of a paystub for another Royal employee, Service Technician, Kerry Young;

c. forward an email from Mike's Royal email account to his personal email account, which attached the image of a paystub for another Royal employee, Parts Salesperson, Samuel Hernandez;

d. forward a quote for a Royal customer, Gemini Transport LLC, on a Hendrickson Subframe Box, from Mike's Royal email account to his personal email account;

e. destroy data, programs, systems, and/or information on Mike's company-provided computer by removing and reinstalling the entire operating system;

f. send an email from Kelly's Royal email account to Mike's personal email account with the words "Here's some," which attached a "Salesperson Summary Report" that contained confidential and proprietary information regarding the month-to-

date revenue, profits, and other details relating to eight of the salespeople in Royal's Parts Division;

g. forward an email from Kelly's Royal email account to her personal email account, which contained a sales inquiry (containing customer-specific pricing information) allocated to Kelly (by her manager) through Royal's sales analytic software system (sales-i), and with a direction for Kelly to "reach out to your contact and try to get our foot in the door with Kitmasters"; and

a. destroy data, programs, systems, and/or information on Kelly's company-provided cellular phone by resetting the cellular phone to factory settings.

(Id. at Page ID #45-53).

Litigation History

On April 3, 2018, Royal filed a First Amended Complaint against Defendants. (RE 8, Complaint, Page ID #37). The First Amended Complaint contains nine counts. (Id. at Page ID #49-62). Counts I and II allege Defendants violated Section 1030 (a)(2) of the Computer Fraud and Abuse Act. (Id. at Page ID #49-53). Counts III-IX allege Michigan statutory and common law claims. (Id. at Page ID #54-62).

On April 17, 2018, Defendants filed a combined Motion to Dismiss Under Rule 12(b)(6) for Failure to State a Claim and Under Rule 12(b)(1) for Want of Subject Matter Jurisdiction. (RE 11, Motion, Page ID #70). The motion requested dismissal of Counts I and II of the First Amended Complaint. (Id.). The motion

also asked the Court to decline supplemental jurisdiction over Counts III-IX, if Counts I and II were dismissed. (Id.). The motion did not challenge the legal sufficiency of Counts III-IX. (Id.). On May 8, 2018, Royal filed a Response to the Motion. (RE 13, Response, Page ID #94). On May 22, 2018, Defendants filed a Reply in Support of the Motion. (RE 15, Reply, Page ID #132).

On March 11, 2019, the district court dismissed Counts I and II, declined to exercise supplemental jurisdiction over the remaining claims, and dismissed those remaining claims without prejudice. App. 25.

On March 11, 2019, Royal timely filed a Notice of Appeal. (RE 24, Notice of Appeal, Page ID #335).

On September 9, 2020, the Sixth Circuit affirmed the district court's dismissal of the First Amended Complaint. App. 15.

REASONS FOR GRANTING CERTIORARI

I. THIS COURT SHOULD GRANT CERTIORARI TO RESOLVE A SUBSTANTIAL CONFLICT AMONG NINE UNITED STATES COURTS OF APPEALS ON AN IMPORTANT MATTER: SECTION 1030(a)(2) OF THE COMPUTER FRAUD AND ABUSE ACT

There is a "deep circuit split regarding interpretations and scope of the [Computer Fraud and Abuse Act]." *American Furukawa, Inc. v. Hossain*, 103 F. Supp. 3d 864,871 (E.D. Mich., May 6, 2015). One district court in the Sixth Circuit has aptly summarized the divide:

> The split arises from cases in which an employer brings a CFAA claim against an employee who accesses the employer's computer to misappropriate confidential or proprietary business information to start a competing business venture or join a competitor. Courts around the country struggle with whether the CFAA applies in a situation where an employee who had been granted access to his employer's computers uses that access for an improper purpose.

Ajuba Intern., L.L.C. v. Saharia, 871 F. Supp. 2d 685-86 (E.D. Mich. May 14, 2012). The circuit split "has been cast as a clash between 'broad' and 'narrow' interpretations of the CFAA." *Hossain*, 103 F. Supp. 3d at 871.

A. The "Broad" Approach

The First, Fifth, Seventh, Eighth, and Eleventh Circuits have adopted a "broad" approach to interpreting and applying the phrase "exceeds authorized access." See *E.F. Cultural Travel BV, EF v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010); *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); and *U.S. v. Teague*, 646 F.3d 1119 (8th Cir. 2011). These courts hold an employee granted access to information through a computer for some reasons may nonetheless exceed his authorized access under the CFAA by using the information for prohibited or improper reasons. *Id.*

For example, in *Rodriguez*, the Eleventh Circuit affirmed the conviction of a Social Security Administration ("SSA") employee under the CFAA because he accessed information on a work computer in violation of a use restriction policy. 628 F.3d at 1260. As an employee of the SSA, the defendant was generally permitted to access certain governmental databases containing sensitive personal information about the public. *Id*. In order to protect this information, however, the SSA implemented a policy that prohibited all employees from accessing these databases without a business reason. *Id*. The defendant refused to sign an acknowledgment form after receiving the policy, but he was nonetheless aware of the policy. *Id*. After it was discovered that, in an apparent effort to learn about multiple women the defendant was involved with, he had repeatedly accessed the database without a business reason, he was charged with, and convicted of, exceeding his authorized access to the information under the CFAA. *Id*. at 1261-62.

The defendant appealed. *Rodriguez*, 628 F.3d at 1263. In doing so, the defendant urged the Eleventh Circuit to follow the "narrow" approach to interpreting the CFAA, which had been adopted by the Ninth Circuit one year earlier. *Id*. (citing *LVRC Holdings LLC v. Brekka,* 581 F.3d 1127 (9th Cir. 2009)). The Court declined:

> The Ninth Circuit held that Brekka, an employee of a residential addiction treatment center, had not violated the Act when he emailed documents that he was authorized to obtain to his personal email account. The treatment

> center argued that Brekka obtained the documents he emailed without authorization because he later used them for his own personal interests. The treatment center had no policy prohibiting employees from emailing company documents to personal email accounts, and there was no dispute that Brekka had been authorized to obtain the documents or to send the emails while he was employed. *Brekka* is distinguishable because the Administration told Rodriguez that he was not authorized to obtain personal information for nonbusiness reasons.

Id. (internal citations omitted). In other words, while the Court distinguished *Brekka*, the Court also reasoned that (contrary to *Brekka*) an individual's right to access information for some reasons does not preclude liability under the CFAA when the individual accesses information for prohibited reasons. *Id*. Rather, because a departmental policy informed the defendant he was not allowed to access the information for a "nonbusiness reason," the moment he "obtained personal information for a nonbusiness reason" he also "exceeded his authorized access and violated the [CFAA]." *Id*.[1]

---

[1] See also *John*, 597 F.3d at 271-73 (employee of bank exceeded authorized access to customer account information database she was generally permitted to access by sharing the information with non-employee in violation of company policy and furtherance of illegal scheme); *Teague*, 646 F.3d at 1121-23 (employee of government contractor exceeded authorized access to governmental student loan database he was generally permitted to access by improperly accessing student-loan records of former United States president); *Explorica*, 274 F.3d at 582-84 (former

B. The "Narrow" Approach

The Second, Fourth, Sixth, and Ninth Circuits have adopted a "narrow" approach to interpreting and applying the phrase "exceeds authorized access." See *Brekka*, 581 F.3d 1127; *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2011); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); *U.S. v. Valle*, 807 F.3d 508 (2d Cir. 2015); and *Royal Truck & Trailer Sales and Service, Inc. v. Mike Kraft and Kelly Matthews a/k/a Kelly Schlimmer*, 974 F.3d 756 (6th Cir. 2020). These courts hold an employee granted access to information through a computer for any reason is incapable of violating the CFAA by using his access to the information for a prohibited or improper reason. *Id*.

For example, in *Nosal*, the government indicted a former employee of an executive search firm for, among other things, violating the CFAA. 676 F.3d at 856. Shortly after leaving the company, the defendant persuaded some of his former colleagues – who remained employed by the company – to help him start a competing business. *Id*. The employees used their log-in credentials to download source lists, names, and

---

employee of travel agency exceeded authorized access when he violated a confidentiality agreement by assisting a technology consultant hired by a competitor with developing a program that enabled the extraction of confidential pricing information from his former employer's website); and *Citrin*, 440 F.3d at 418-21 (former employee of real estate business violated CFAA when he erased files from computer before going into business for himself in violation of employment agreement because access to computer was revoked when he acquired interests adverse to his employer).

contact information from a confidential database accessed through a company computer, and then transferred this information to the defendant. *Id*. While the employees were authorized to access the database containing the information, a company policy prohibited them from disclosing the information to the defendant. *Id*. After the government indicted the defendant for aiding and abetting the employees in exceeding their authorized access, the defendant moved to dismiss. *Id*. The district court eventually dismissed the CFAA counts. *Id*. The government appealed. *Id*.

The Ninth Circuit affirmed. *Nosal*, 676 F.3d at 864. In doing so, the Court initially acknowledged the competing approaches to interpreting the phrase "exceeds authorized access":

> This language can be read either of two ways: First, as [the defendant] suggests and the district court held, it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files – what is colloquially known as "hacking." For example, assume an employee is permitted to access only product information on the company's computer but accesses customer data: He would "exceed authorized access" if he looks at the customer lists. Second, as the government proposes, the language could refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information. For example, an employee may be authorized to access customer

> lists in order to do his job but not to send them to a competitor.

Id. at 856-57.

"While the CFAA is susceptible to the government's broad interpretation," the Court continued, "we find [the defendant's] narrower one more plausible." *Nosal*, 676 F.3d at 858. This is because, the Court suggested, the broader approach "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id.* at 857. According to the Court:

> The government agrees that the CFAA was concerned with hacking, which is why it also prohibits accessing a computer "without authorization." According to the government, *that* prohibition applies to hackers, so the "exceeds authorized access" prohibition must apply to people who are authorized to use the computer, but do so for an unauthorized purpose. But it is possible to read both prohibitions as applying to hackers: "[W]ithout authorization" would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and "exceeds authorized access" would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files). This is a perfectly plausible construction of the statutory language that

> maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate.

Id. at 858 (italics in original).

In sum, the Ninth Circuit concluded, the decisions from the circuits applying the "broad" approach have "failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of "exceeds authorized access" and "failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to avoid making criminal law in Congress's stead." *Nosal*, 676 F.3d at 862-63 (internal citations and quotations removed).[2]

C. This Case Presents An Excellent Opportunity For The Court To Resolve The Circuit Split

This case presents an excellent opportunity for the Court to resolve the circuit split. See *Cash v. Maxwell*,

---

[2] See also *WEC*, 687 F.3d at 204 (employee did not exceed authorized access to computer when he downloaded confidential information in violation of company policy and subsequently used the information to assist a competitor because defendant was generally allowed to access the information); *Valle*, 807 F.3d at 508 (former police officer did not exceed authorized access to confidential police database when he searched for an individual's personal information in violation of a policy prohibiting him from using the database without a law enforcement purpose because he was generally allowed to access the database); and *Royal*, 974 F.3d at (employees did not exceed authorized access to company computers when they absconded with sensitive information because they were generally allowed to access the information).

123 S. Ct. 611, 612-13 (2012) (quoting *Caperton v. A.T. Massey Coal Co.*, 556 U.S. 868, 902 (2009) (Scalia, J., dissenting) ("'The principal purpose of this Court's exercise of its certiorari jurisdiction is to clarify the law.'")). First, the issue is *clearly* presented by this case. The case will be before the Court on appeal from the affirmance of a dismissal of the First Amended Complaint pursuant to Fed. R. Civ. P. 12(b)(6). There is thus no dispute (for purposes of appeal) that company polices permitted Defendants to access information on their company computers and telephones for limited purposes; that company policies prohibited Defendants from using the information for other purposes; and that Defendants used the information for improper purposes in violation of company policies. See *Royal*, 974 F.3d at 759.

Second, this case offers the Court an opportunity to resolve a civil case involving the circuit split. This Court has already granted certiorari in *Nathan Van Buren v. United States*, 140 S. Ct. 2667 (2020). *Nathan* is a criminal case presenting the same issue as this case. Granting certiorari in this case will permit the Court to directly resolve the circuit split in both a criminal and civil case. This will allow the Court to eliminate any ambiguity that may result from interpreting the statute in the context of solely a criminal case. Accordingly, this Court should grant certiorari.

CONCLUSION

This Court should grant certiorari to resolve the split among nine United States Courts of Appeals on an important matter: Section 1030(a)(2) of the Computer Fraud and Abuse Act. Accordingly, this Court should grant certiorari.

Respectfully submitted,

ROYAL TRUCK & TRAILER
SALES AND SERVICE, INC.

By: /s/ Anthony M. Sciara
Counsel of Record

ANTHONY M. SCIARA
ROYAL TRUCK & TRAILER
311 East Cady Street
Suite C
Northville, Michigan 48167
(248) 773-3775
asciara@royaltrailersales.com

Counsel for Petitioner