No. 19-783

IN THE

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

BRIEF OF THE MANAGED FUNDS ASSOCIATION AS *AMICUS CURIAE* IN SUPPORT OF RESPONDENT

JOSEPH V. DEMARCO
Counsel of Record
DAVID M. HIRSCHBERG
DEVORE & DEMARCO LLP
99 Park Avenue, Suite 1100
New York, NY 10016
(212) 922-9499
(917) 576-2369
jvd@devoredemarco.com

Counsel for Amicus Curiae

September 1, 2020

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF CONTENTS—Continued

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES—Continued

COURT FILINGS Page(s)

OTHER AUTHORITIES

TABLE OF AUTHORITIES—Continued

INTEREST OF *AMICUS CURIAE*[1]

Managed Funds Association ("MFA") is a not-for-profit membership organization representing the global alternative investment industry. MFA is an advocacy, education, and communications organization established to enable advisers to investment funds and managed futures funds to participate in public policy discourse, share best practices, learn from peers, and communicate the industry's contributions to the global economy. MFA's more than 4,200 professional members represent managers of hedge funds, separately managed funds, managed futures funds, and their service providers.

MFA members represent a significant portion of the American economy. MFA's over 200 investment management member firms include many of the nation's largest investment institutions, collectively managing more than $1.1 trillion in capital, a figure which comprises nearly two-thirds of the capital managed by the fifty largest U.S.-based hedge funds. Member firms are headquartered in nineteen states and employ more than 10,000 individuals in addition to tens of thousands of additional employees working at MFA member banks. MFA investment management firms are fiduciaries to their clients. The investors of the client funds of MFA members predominantly include pension plans, university endowments, charitable foundations, and philanthropic trusts. The goal of these investors is to diversify their investments, manage

---

[1] Pursuant to Supreme Court Rule 37.6, no counsel for a party authored this brief in whole or in part. No person or entity other than the Managed Funds Association and its members made any monetary contribution to fund the preparation or submission of this brief. The parties have consented to this filing.

risks, and generate reliable returns over time for retirees, students and other beneficiaries.

MFA members include some of the most intensive computing and data-reliant businesses in the world. Modern financial decision-making relies on massive amounts of data, sophisticated algorithms, and the application of computer processing power — each one an area in which MFA members invest in heavily. Yet while computer-based analyses and trading tools have been a boon to the investment industry, they have also given rise to the unfortunate side effect of data misappropriation and theft of confidential intellectual property. As has been demonstrated in several high-profile instances, the portability of digital information has given unscrupulous employees of financial firms the motivation to steal their employer's digital assets, often with the intent of benefiting themselves or their future employers. MFA members therefore expend substantial resources in securing their digital assets — especially those assets which are proprietary and highly confidential.

Notwithstanding these efforts, it is an unavoidable consequence of conducting an analytical business that certain employees and other third parties must be granted access to sensitive and non-public information residing on MFA member databases and systems. When those individuals are responsible for information theft, victimized financial firms can only rely upon the law — including the Computer Fraud and Abuse Act — to protect themselves. MFA is therefore concerned that Petitioner's narrow reading of the term "authorized" as used in that statute would, if adopted by this Court, substantially weaken MFA member firms' ability to prevent the theft of their highly valuable confidential, non-public proprietary data and intellectual property.

SUMMARY OF ARGUMENT

The Computer Fraud and Abuse Act (Title 18, United States Code, section 1030) ("CFAA") is unquestionably the most important federal statute protecting American computer systems and the data stored on those systems. As digital technology has become ever more central to the economy, the CFAA has, in a corresponding fashion, increased in importance. Adopted in the pre-Internet age, when computer security was in its relative infancy, the CFAA could not have been drafted with precise knowledge of how computers would eventually come to be used, or how those evolving complexities could generate uncertainty concerning the meaning of apparently simple statutory language. Yet Congress' fundamental purpose in enacting the law — which must be reflected in interpreting the statute — was clearly and unambiguously to protect non-public computer systems and confidential data from the threats posed by malicious actors.

At issue in this case is the definition of the words "without authorization," an element of several of the CFAA's enumerated criminal offenses (and, by reference, the statute's civil provision), as well as its statutory companion, "exceeding authorized access." As courts addressing the issue have often remarked, the lack of an explicit definition in the CFAA of what constitutes "authorization," and perhaps more importantly what parameters dictate when authorization is *lacking*, has generated uncertainty as to how the statute should be applied. Interested parties have advanced — or proposed as evils that must be avoided — rather extreme interpretations of the term. Those favoring the narrowest possible scope of the term argue that any activity is "authorized" unless technical measures are deployed specifically to prevent it. Under such a

definition, the CFAA would become essentially an anti-circumvention statute, prohibiting only the conduct of those who "hack" through the security of a computer system. On the other extreme are those who champion an extremely broad interpretation of what constitutes "unauthorized access," reasoning that any violation of the most innocuous contractual terms concerning computer access should qualify, *even if* the data in question is publicly-viewable by anyone with Internet access. Such advocates miss the obvious point that there is an array of activity involving access to *non*-public data that, while not within the conventional view of malicious "hacking" by outside individuals or groups, is nonetheless clearly without authorization under any reasonable, common sense interpretation of that term. MFA submits that among the actions which should be understood as violative of the CFAA are those of employees (and other insiders) which violate plainly communicated, expressly agreed to, unambiguous restrictions on the use of non-public computer systems and non-public data on those systems.

MFA's concerns with Petitioner's (mis)reading of the CFAA are not hypothetical. In particular, our members are keenly aware of, and acutely concerned by, the threat posed by the exploitation of its members computer systems by faithless employees, contractors, vendors, suppliers and other third party "insiders" with permissioned access to member systems. The theft of such intellectual property or proprietary information harms investment managers, fund investors, potentially other market participants and the economic competitiveness of U.S. firms to the extent that such property is exported to a foreign competitor. Indeed, in recent years, financial firms have seen a marked increase in the prevalence of data theft and attempted data theft by such "insiders." These incidents include

not only widely reported-upon events which have given rise to criminal proceedings, but also countless other thefts and attempted thefts which, for various reasons, do not come to the public knowledge. Moreover, the adoption of a narrow reading of the CFAA in certain circuits has served as a deterrent to firms who would otherwise seek to vindicate their rights in federal court.

MFA respectfully submits that adopting the extremely narrow scope of the CFAA advocated by Petitioners belies the ordinary meaning of the word "authorized."[2] It also defies common sense. Such a narrow reading renders the CFAA powerless against the most significant cyber-security threat faced by many financial firms: the threat of insider malfeasance related to trade secrets and other confidential data and IP. Simply put, if the line between authorized and unauthorized activity is *only* defined with reference to technological controls protecting against outside hackers, then it becomes nearly impossible for any user of a computer system with access credentials to that system — such an investment firm employee — to violate the CFAA, *no matter how egregious* his conduct in relation to non-public data on those systems.

MFA believes that a better interpretation of the CFAA is to apply the common, dictionary definition of the term "authorization" when applying the statute. Rather than reading into the CFAA a requirement of circumventing a technological access control — a term conspicuously absent from the statutory text —

---

[2] *See, e.g.*, *Authorized*, MERRIAM-WEBSTER.COM DICTIONARY, https://www.merriam-webster.com/dictionary/authorized (last visited Aug. 26, 2020) (defining "authorized" as "sanctioned by authority: having or done with legal or official approval").

factfinders should instead determine the answer to this straightforward question: "Was the defendant specifically and knowingly prohibited from engaging in the complained-of conduct concerning the non-public systems and non-public data in question?"

ARGUMENT

I. PETITONER'S INTERPRETATION OF THE CFAA, IF ADOPTED, WOULD LIMIT THE APPLICABILITY OF THE CFAA ALMOST ENTIRELY TO THE ACTIONS OF OUTSIDERS, RENDERING IT INEFFECTIVE AGAINST THE OFTEN FAR MORE SIGNIFICANT THREAT POSED BY FAITHLESS INSIDERS TO CONFIDENTIAL COMPUTER SYSTEMS AND INFORMATION

A. Modern Financial Firms Gather, Create, Maintain, and Rely Upon Massive Amounts of Non-Public Data and Proprietary Programs in the Course of Conducting their Business

Without a doubt, investment firms are among the most technologically advanced and technology-reliant businesses in the American economy. While the types of systems and data used by each firm vary substantially in accordance with the nature and character of their investment activities, a high-level overview of the digital assets maintained by such institutions sheds light on the importance and breadth of computerized information used in the field. It also underscores the criticality to member firms' competitive position of being able to keep confidential data and systems that it has expended time and effort creating.

- *Personal Information and Personal Financial Information*. Like all businesses, financial firms maintain non-public personal information, often quite sensitive, concerning their employees and clients. In particular, as a necessary incident to providing investment services, most firms also maintain confidential digital records of their clients' investments, income, tax information, and other financial and sensitive records.
- *Research and Data Analysis*. Firms' research departments typically produce proprietary analyses, often in the form of confidential analyses and White Papers, of markets and investment strategies.
- *Trading Strategies, Platforms, and Source Code*. At the most fundamental level, an investment firm's business is to implement trading strategies that provide clients with the best possible returns on their investments. As such, investment firms often expend considerable resources developing their own confidential trading strategies. Indeed, it is these "secret sauce" strategies which provide much of the value of a firm to a prospective client and which differentiate one firm from another. Although in some cases trading strategies can be written out in human-readable form and executed manually, often the strategies consist of intricately detailed confidential statistical models which operate on real-time feeds of massive amounts of market data. In many instances, the systems which run these models not only assist in making investment decisions, but also *execute* the trades in an automated fashion. Such automated trading systems

require development of software platforms which can quickly and efficiently execute transactions.

- *Data from Diverse Sources.* Financial firms have always relied on traditional forms of market data, including records of stock prices and transactions, financial records of publicly traded companies, broad economic indicators, interest rates, currency exchange rates and similar data inputs. In recent years, however, investment firms have gathered and incorporated into trading strategies an ever-broadening array of data sets from a range of diverse sources. These data sets can include financial data such as credit card data, as well as non-financial data (for example, weather data, satellite imagery, and real-time inventory monitoring). Often, member firms expend substantial resources aggregating, analyzing, and interpreting these new datasets in order to create powerful confidential strategies to maximize client returns.

B. Certain Employees and Third Parties Must Be Granted Access to Valuable Proprietary Data and Systems in Order for Those Systems to Operate Properly

The development of non-public confidential trading strategies and the computing platforms upon which those strategies are executed is, of course, accomplished through the efforts of individual employees of financial firms. For example, an algorithmic trading strategy may be embodied in a complex spreadsheet which takes as its inputs a data feed of trades in a given market and which will execute a trade if certain conditions (embodied in computational formulas embedded within the spreadsheet) become satisfied. These confidential formulas — and by extension the trading

strategy itself — are developed and maintained by analysts and programmers working for the trading firm. Each of these people must have technological access to the spreadsheet in order to develop and implement the strategy. Similarly, in the context of non-automated trading, investment professionals must have access to confidential research materials and analyses — often developed in-house and essentially always maintained in computerized format — in order to use the contents of those materials in making investment decisions.

Notably, however, the personnel who must have access to a firm's computing environment are not limited to investment professionals. Other employees, including sales personnel, compliance, operations and back-office and support staff, will require access to communications and records systems. Moreover, technicians who maintain the computer systems themselves (who may or may not be employees of the firm) will often have "administrator" level permissions, permitting largely unfettered access to stored data. In addition, numerous non-employee personnel, including IT and other contractors, as well as temporary workers, also regularly have access to confidential firm and customer data.

C. Investment Firms Implement Robust Procedures to Secure their Digital Assets

As noted above, financial firms invest heavily in the acquisition of data and the development of analytical tools and reports. Given that firms obtain substantial value from these assets, it is natural that they go to great lengths to secure those confidential materials from loss, corruption, and theft. Crucially, these safe-

guards include both technical as well as *contractual and procedural* elements. Both are described more fully below.

To begin with, investment firms implement some of the most stringent technical access control, employee monitoring, and cybersecurity measures of any private entities. Like other businesses, they typically require individualized computer access credentials, limit access to systems necessary for an individual's job functions, monitor electronic communications, log the dates and times files are accessed by employees, and deploy firewalls with robust Data Loss Prevention ("DLP") controls. Many firms go far beyond those prosaic methods, taking steps such as preventing access to outside email systems and cloud-storage services, disabling corporate systems from being able to connect to external peripherals such as portable hard drives, conducting video surveillance of their offices, and requiring personal electronics (including cellular phones) to be stored outside of the areas where access to computer systems is provided. Importantly, many of these practices limit technical access to data (*e.g.*, limiting users to accessing only job-relevant systems). Under either the broad or narrow interpretations of the CFAA, defeating these protections may be indicative of "unauthorized" activity. Yet many of these protections are expressly designed to prevent individuals who *are* permitted to access proprietary data from removing it from the firm's computing environment (*e.g.*, preventing the connection of portable hard drives to firm systems). The presence of these security measures serves as a clear indication that while firm employees may be permitted to access and use confidential information while at work, they are not authorized to remove that data from the premises.

Another group of data protection safeguards utilized by financial firms consists of *non*-technical limitations on employee conduct. These measures consist primarily of contractual agreements and policies and procedures all of which are often reinforced through training. For example, typically at the outset of employment (and often periodically thereafter), employees of a financial firm will agree to non-disclosure and confidentiality agreements as part of their employment contracts. These agreements are often extremely detailed, with explicit prohibitions against certain actions such as removal of confidential firm data from the employer's computing systems and environment.[3]

Notwithstanding those features, Petitioners and other proponents of the "narrow" interpretation of the CFAA argue that such non-technical policies are entirely irrelevant to the issue of whether an employee exceeds their authorized access when the employee circumvents those non-technical controls and violates the clear and unambiguous terms of his employment contract in connection with non-public, confidential data and IP belonging to the employer. This view is

[3] Notably, this appeal does not implicate the question of restrictions, through terms of service or otherwise, ostensibly related to *publicly accessible* information — for example, data which can be accessed by anyone through public-facing websites. That issue is not before this Court. It is, however, worth noting that MFA member contractual data protection controls related to *non*-public data are entirely dissimilar to a public website's terms of service, which are often vague and often assertedly apply to public data on the site. In contrast, MFA employees' non-disclosure and confidentiality contracts and policies regularly contain provisions which are (1) limited to *non*-public systems and data, (2) consistently and conspicuously monitored, and (3) reinforced through periodic training.

not supported by the plain language of the CFAA. It also makes no sense.

II. INVESTMENT FIRMS ARE UNDER CONSTANT THREAT OF DATA THEFT BY FAITHLESS INSIDERS

The proprietary computerized information generated by investment firms is intrinsically valuable, as many of those data sets, algorithms, and trading platforms are used quite directly to generate revenue for investors. While the vast majority of employees at investment firms are conscientious and trustworthy, it only takes one unscrupulous employee to severely damage and even destroy a well-built investment management business. In the hands of knowledgeable competitors with adequate resources, misappropriated confidential financial intellectual property can be used to set up a competing business without the need to invest in costly research and development.[4] These factors, combined with the frequency with which employees in the field move between competing firms, unfortunately serve as strong incentives for unscrupulous individuals to attempt to transfer proprietary information to their new firms.

[4] Some firms specifically manage their workforce in a manner which does not require complete knowledge of confidential trading strategies by any single individuals (*i.e.*, "siloing" information) to avoid precisely this threat. However, there are limits to how far such efforts can go. Although it is common for researchers to specialize in one area, for portfolios which consist of different kinds of asset classes or securities of companies from different industries, there is benefit in joint research, collaborative idea generation, and data and information sharing so that researchers can have a more full understanding of micro- and macro-economic factors.

These dangers are far from theoretical: the scale of insider threats to financial firms is staggering. According to the 2020 *Cost of Insider Threats Global Report* study by the well-respected Ponemon Institute, the financial services industry (defined to include banking, insurance, investment management and brokerage organizations) has experienced the highest cost of responding to insider threats of any industry.[5] Financial services also experienced the second-fastest increase in the number of insider incidents of any business sector, experiencing a 20.3% increase over two-years.[6] Moreover, the Ponemon study found that incidents involving the criminal or malicious (as opposed to negligent) actions of faithless "insiders" cost organizations an average of $755,760 per incident, and comprised 23% of all reported incidents involving insiders.[7]

Most insider threats to financial firms' confidential computer systems fall within a defined number of patterns. These include:

- *Facilitation of Identity Theft and Fraud.* As required by statute and regulation, financial firms are required to retain records of extremely sensitive confidential personal information concerning their clients, including their names, addresses, account numbers, and tax information, among other sensitive information. In this scenario, corrupt firm employees target the personal information that their employers

[5] PONEMON INSTITUTE, 2020 COST OF INSIDER THREATS: GLOBAL REPORT 22 (2020) (*available* at https://www.observeit.com/2020costofinsiderthreat).

[6] *Id.* at 5.

[7] *Id.* at 4.

maintain concerning firm clients in connection with identity fraud. Sadly, this fact pattern has become increasingly common. The most recent such incident became public earlier this year, when Fifth Third Bank, a $169 billion banking and financial services group, announced that a small number of its former employees accessed and misused consumer data to commit fraud. The bank contacted at least 100 customers possibly impacted.[8] Indeed, in some cases, insiders may simply sell client information to criminal organizations. For example, in *United States v. Persaud*, the defendant, a former employee of JP Morgan Chase Bank abused his access to the bank's systems by obtaining and selling the confidential personal and account information of customers.[9]

---

[8] *Former Fifth Third Staff 'Stole Customer Data', Bank Confirms*, BANKING EXCHANGE (Feb. 19, 2020), https://www.bankingexchange.com/compliance-management/item/8134-former-fifth-third-staff-stole-customer-data-bank-confirms.

[9] *Former JP Morgan Chase Bank Employee Sentenced to Four Years in Prison for Selling Customer Account Information*, U.S. DEP'T OF JUSTICE (Aug. 10, 2018), https://www.justice.gov/usao-edny/pr/former-jp-morgan-chase-bank-employee-sentenced-four-years-prison-selling-customer; *see also* Indictment, *United States v. Persaud*, No. 15-cr-00462 (E.D.N.Y. Sept. 14, 2015). *See also* Lauren Tara LaCapra & Tanya Agrawal, *Morgan Stanley Says Wealth Management Employee Stole Client Data*, REUTERS (Jan. 5, 2015), https://www.reuters.com/article/us-morgan-stanley-data/morgan-stanley-says-wealth-management-employee-stole-client-data-idUSKBN0KE1AY20150106 (discussing a wealth management employee who stole account information of approximately 350,000 clients and attempted to sell it online).

- *Effecting Fraudulent Financial Transactions.* In another scenario, insiders may abuse their access to firm systems to directly steal money. As an example, between April 2014 and May 2017, Dilcia Mercedes, a payment processor employee of a mortgage lender abused her access to the company's computer system to make hundreds of fraudulent wire transfers and steal over $2 million. She was indicted on and pleaded guilty to charges including unauthorized access of a computer with intent to defraud under 18 U.S.C. § 1030(a)(4).[10]
- *Theft of Confidential Business Information.* Business plans and customer lists have also frequently been targeted by corrupt insiders. In one conspiracy, a former employee of an online mortgage broker sold company-employee log-in credentials to another mortgage broker, who subsequently used the company's database to steal thousands of mortgage leads. The conspirators were charged with and pleaded guilty to charges including CFAA violations.[11]

---

[10] *Employee at Mortgage Company Admits Illegally Accessing Computer to Steal $2 Million*, U.S. DEP'T OF JUSTICE (June 21, 2019), https://www.justice.gov/usao-nj/pr/employee-mortgage-company-admits-illegally-accessing-computer-steal-2-million-0; *see also* Information, *United States v. Mercedes*, No. 1:19-cr-00435 (D.N.J. June 21, 2019).

[11] *Former Online Mortgage Broker Employee and Mortgage Broker Conspirator Sentenced to Prison for Computer Theft*, U.S. DEP'T OF JUSTICE (Dec. 15, 2014), https://www.justice.gov/usao-wdnc/pr/former-online-mortgage-broker-employee-and-mortgage-broker-conspirator-sentenced-prison; *see also* Indictment, *United States v. Rosene et al.*, No. 3:12-CR-00369 (W.D.N.C. Nov. 15, 2012).

- *Theft of Algorithmic Trading Code and Trading Platform Source Code.* Perhaps the highest profile incidents of employee theft of investment firm data in recent years have concerned the removal of highly confidential trading algorithms themselves — particularly high frequency trading algorithms — and the source code for the platforms that execute transactions. Given the extreme investment required to develop these assets and the incredible value they represent, such incidents have given rise to protracted litigation, including at the appellate level. Most notable of these cases is *United States v. Aleynikov*, which concerned a former Goldman Sachs computer programmer who was accused of misappropriating source code for the firm's high-frequency trading system.[12] The *Aleynikov* case is particularly notable for present purposes as, prior to trial, the District Court dismissed the CFAA charge against the defendant, reasoning that the "phrases 'accesses a computer without authorization' and 'exceeds authorized access' cannot be read to encompass an individual's misuse or misappropriation of information to which the individual was permitted access."[13]

---

[12] *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012). *See also United States v. Agrawal*, 726 F.3d 235 (2d Cir. 2013) (involving the theft of computer code underlying Société Générale's high-frequency trading platform).

[13] *United States v. Aleynikov*, 737 F. Supp. 2d 173, 192 (S.D.N.Y. 2010).

III. THE READING OF THE CFAA ADVANCED BY PETITIONER UNDERCUTS THE STATUTE'S EFFECTIVENESS AT PREVENTING CYBERCRIME AND IS CONTRARY TO THE PLAIN MEANING OF THE STATUTORY LANGUAGE

In determining the proper understanding of the CFAA, this Court should be cognizant of the practical reality of how access to computer systems is provided by corporations such as MFA members and avoid adopting an extremely constricted reading that focuses solely on technological access controls to the exclusion of all other factors. MFA respectfully submits that a more reasonable approach, and one which comports with the common understanding of "authorization" as a quality which must be granted, would take into consideration *both* technological controls *and* the understanding of the parties as to what actions are (and are not) permitted in relation to confidential data. More particularly, in the context of employee access to confidential data housed on non-publicly accessible, employer-operated computers, a proper and balanced understanding of the statute should take into holistic consideration the (1) clearly communicated and agreed-to understandings of the parties as embodied in employment contracts and policies, (2) training and monitoring, and (3) the facts and circumstances of access as applied in practice.

A. Giving Weight to the Terms of Employment Contracts and Policies Reinforces the Common Understanding that One's Rights Concerning the Property of Another Extend Only as Far as They Are Granted

It is axiomatic to the law of property that, absent a grant of permission, one is not entitled to use the property of another.[14] In the context of employer-provided computer systems and confidential data, this axiom is reinforced by practical considerations: unless and until an employee is issued access credentials to a confidential system or database, she has neither the right nor the ability to use the system or access the data stored thereon.

The analysis does not, however, end there. The next question becomes whether an employer, in granting access credentials to an employee, retains the right to impose conditions upon the use of those credentials. Clearly, they do. In fact, MFA member firms collectively have spent tens of millions of dollars creating, and implementing conditions on data access, use, and misuse. Member firms have likewise collectively spent hundreds of millions of dollars on training employees on these policies and in enforcing policy violations. Moreover, numerous statutory laws and regulations — not to mention fiduciary duties and obligations — affirmatively *require* member firms to proactively safeguard confidential and non-public data through contractual and policy controls. *See, e.g.*, Section 206

---

[14] 2 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND (1ST ED. 1765-69) *2 (defining property as "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe").

of the Investment Adviser Act of 1940 ("Advisers Act")[15] and Commission Interpretation Regarding Standard of Conduct for Investment Advisers (stating that Section 206 imposes a fiduciary duty on an investment adviser);[16] Rule 206(4)-7 under the Advisers Act (requiring investment advisers registered with the Securities and Exchange Commission ("SEC") to adopt and implement written policies and procedures that are reasonably designed to prevent violations of the Advisers Act);[17] Rule 204A-1 under the Advisers Act (requiring investment advisers to adopt a written code of ethics that includes a standard of conduct reflective of its fiduciary obligations, and to require employees to comply with the code of ethics and other legal requirements); Reg S-P[18] (requiring SEC regulated members to adopt written policies and procedures addressing administrative, technical, and physical safeguards for the protection of customer records and information); Reg S-ID[19] (requiring SEC registered investment advisers and broker-dealers to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account); Rule 10b-5 under the Securities Exchange Act of 1934 (regulating trading based on material non-public information).

---

[15] 15 U.S.C. § 80b-6 (2012).

[16] Commission Interpretation Regarding Standard of Conduct for Investment Advisers, Advisers Act Release No. 5248, 17 C.F.R. Part 276 (June 5, 2019).

[17] 17 C.F.R. § 275.206(4)-7 (2007).

[18] 17 C.F.R. § 248.201 (2016).

[19] 17 C.F.R. § 248.201 (2016).

Indeed, an entire compliance industry of lawyers, consultants, and subject-matter experts exists to assist member firms in abiding by these policy requirements. MFA submits that, in light of this bevy of mandates to protect confidential information from theft or misuse by outsiders *and* insiders, it would be anomalous (to say the least) for the CFAA to be interpreted in a manner that renders it wholly ineffective to vindicate these obligations against corrupt insiders.

B. An Interpretation of the CFAA Which Excludes All Actions of Those with Legitimate Access to a Computer System Improperly Limits the Statute in a Manner Inconsistent with the Actual Text of the Statute

Proponents of the narrow interpretation of the CFAA advocate that this Court ignore the plain text of the statute. In effect, they maintain that the statute should be read either by inserting an implied clause — "by circumventing a technological access control mechanism" — into each of the several provisions that include the term "without authorization" *or* by ignoring a portion of the text — "or exceeds authorized access" — which is present. Either option would be an impermissible revision of the actual text of the CFAA.

As a threshold matter, if Congress wished to limit authorization to a purely technological matter, it could have done so. For example, the anti-circumvention provision of the Digital Millennium Copyright Act, Title 17 United States Code, section 1201(a)(1)(A), specifically prohibits the "circumvent[ion] of a technological measure that effectively controls access" to a copyrighted work.[20] Had Congress intended Section

[20] 17 U.S.C. § 1201(a)(1)(A) (2012).

1030 to be limited solely to persons who bypass technological barriers, it could have included similar language.

In addition, adopting a narrow interpretation of "without authorized access" would render another part of the CFAA meaningless. Under Petitioner's reasoning, any time a user accesses a computer either she has done so without authorization, and has violated the CFAA, *or* she was authorized to access the computer and no further inquiry is needed. The problem with this wooden dichotomy is that it renders null the companion phrase "exceeds authorized access." That is because if any activity accomplished following initial authorized access is declared *not* to violate the CFAA, then what function does "exceeds authorized access" serve?[21]

We submit that the only interpretation of the combined phrase "accesses a computer without authorization or exceeds authorized access" which neither inserts language not present in the text nor reads text out of the statute entirely is one which recognizes that "authorization" is not merely a technological concern — it also takes into account contractual and policy restrictions — and that it is possible to violate the CFAA even following "technologically authorized" access to a computer system.

---

[21] 18 U.S.C. § 1030(e)(6) (2012) (defining "exceeds authorized access" as to "access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter").

C. Concerns that a Broad Interpretation of "Without Authorization" under the CFAA Would Require Examination of Defendants' Subjective Motivations Are Not Significant in the Context of Clearly-Communicated, Action-Based Limitations on Authorization

Some courts, in choosing between the "narrow" and "broad" interpretations of the CFAA are significantly concerned with the need to delve into the subjective intentions of a defendant and to rest a determination of whether conduct is unlawful on whether that subjective intent is contrary to the defendant's employer's interests.[22] While this difficulty may sometimes be present, rejecting a broader interpretation on these grounds ignores the fact that in the vast majority of cases, subjective intent is largely irrelevant to the analysis. This is particularly true when an employer has clearly communicated prohibitions on specific actions the employee may take. For example, if an employer informs an employee that she may not run cryptocurrency mining software on firm computer systems, it is clear that if she subsequently does run cryptocurrency mining software then her actions are unauthorized, whether or not her intent was to harm her employer. The inquiry can begin and end with an analysis of the employee's actions.

Similarly, and more relevant to financial firms, communicated limitations on use are not typically limited to the simple statement "you may only use the

---

[22] *See, e.g.*, *Enhanced Recovery Co. LLC v. Frady*, No. 3:13-cv-1262, 2015 WL 1470852, at *4–6 (M.D. Fla. Mar. 31, 2015) (rejecting the broad interpretation of the CFAA because the "analysis focuses on the actions of the employer rather than the subjective motivation of the employee").

computer system for purposes of completing your assigned work." In reality, firms (typically in confidentiality or non-disclosure agreements) explicitly enumerate prohibited actions, including, for example, "you may not copy any data from the firm's computing systems to any storage device or service not controlled by the firm." Yet under the Petitioner's narrow interpretation of the CFAA, an authorized user of firm data could ignore this restriction entirely without risking criminal penalty (or civil liability under the CFAA's civil provision) because the analysis begins and ends with the provision of access. However, taking into consideration the unambiguous "no copying" rule, the broader reading of the CFAA can be imposed without need to consider the defendant's motivations at all.

D. Taking into Consideration Policy and Contract-Based Limitations on Computer System Use in the Context of Employer-Provided Systems Raises No More "Private Criminal Law" Concerns than Does Consideration of Technology-Based Controls

Another concern raised by opponents of a broad interpretation of "without authorization" in the context of the CFAA is that it allows private parties to make criminal laws through imposition of contractual terms.[23] These arguments are often bolstered by rather farfetched examples of "browse-wrap" or "click-wrap" terms of service or use for *public* websites, the minor violation of which sends an unsuspecting web-surfer to a federal penitentiary.[24]

---

[23] Brief for Computer Security Researchers *et al*. as *Amici Curiae* 17.

[24] Brief for the National Association of Criminal Defense Lawyers as *Amicus Curiae* 21-22.

What this argument ignores is that technical restrictions on access to computer systems are every bit as under the control and subject to the supposed whims of system operators as are contractual limitations. There is no natural right to access a computer, nor is the scope of what one can do when accessing a computer subject to any controls other than those which the operator elects to impose. The contractual limitations and the technological limitations are *both* in a sense artificial. Considering that both arise from the decisions and authority of the system operator, treating, for example, a violation of a firewall rule preventing access to an offshore Internet casino as a potentially violative of the CFAA while at the same time treating as entirely irrelevant a clear employee policy against using firm computer systems for gambling should lead to cognitive dissonance. Instead, *both* should be given consideration, in a balanced and holistic manner, as the true issue is whether the firm, as owner and operator of the computing system, is free to place limits on how its employees use their non-public systems and data.

E. Focusing Purely on Technological Access Controls Leads to Plainly Absurd Results

If the only factor given weight in assessing whether a defendant's actions directed toward a computer system is whether he is, as a technical matter, able to access specific systems or data, absurd and nearly contradictory conclusions necessarily follow. Assume, for example, that a financial firm employs Defendant and has granted him access to exactly those computer systems required for his job. At some point, Defendant transfers to another department of the same firm, requiring access to a different set of systems.

- *Case 1*: The firm's IT department inadvertently changes Defendant's technical permissions a day too early. In order to complete his assigned tasks, he uses a coworker's credentials to access the required confidential files. Since Defendant lacked technical access, his action is *unauthorized*.
- *Case 2*: The Defendant's transfer occurs mid-week, but, due to the manner in which the firm's IT department operates, his former permissions will not be revoked until the end of the week. Defendant's supervisor specifically reminds him that, having transferred out of the department, he no longer has permission to access the department's confidential systems and data and should refrain from doing so. The Defendant agrees to this limitation, which aligns with his employment agreement. Later that day, the Defendant accesses the files of his former department and maliciously deletes them. Because his credentials were still valid, his actions for purposes of the CFAA are still ironically *authorized*.
- *Case 3*: Due to a configuration error, the transferred Defendant is inadvertently given access to the firm's human resources system. Although unrelated to his job, and knowing he should not do so, he takes the opportunity to read the confidential HR files of several of his coworkers. Because of the configuration error, his spying on his coworkers is considered *authorized* activity.

Each of these situations results in an unexpected and irrational outcome as a result of an analysis which focuses *exclusively* on technological access controls. In the latter two cases, clearly blameworthy activity, far outside the intent of the employer in granting access, is rendered "authorized" by application of Petitioner's

analysis. On the other hand, an approach which considers additional factors would result in more sensible conclusions — conclusions which would comport with any reasonable observer's expectations and the purposes for which the CFAA was adopted.

CONCLUSION

In light of the increasing threat to investment firms' computerized systems and data posed by faithless insiders, a narrow interpretation of the CFAA which limits the statute's applicability only to the actions of outsiders with no legitimate use of a system would substantially undercut federal criminal law's protection of those systems and simultaneously render ineffective the civil provision of the CFAA for the same purpose. In order to provide redress for victimized firms and to align the application of the CFAA with its common sense interpretation, this Court should imbue the statutory phrases "without authorization" and "exceeds authorized access" their plain meanings in a balanced way, rendering them applicable both to outside "hackers" and to inside wrongdoers who have clearly and explicitly agreed to policy-based limitations on their use of their employers' confidential computer systems and data.

Respectfully submitted,

JOSEPH V. DEMARCO
Counsel of Record
DAVID M. HIRSCHBERG
DEVORE & DEMARCO LLP
99 Park Avenue, Suite 1100
New York, NY 10016
(212) 922-9499
(917) 576-2369
jvd@devoredemarco.com

September 1, 2020 *Counsel for Amicus Curiae*