No.

IN THE

SUPREME COURT OF THE UNITED STATES

OCTOBER TERM, 2025

GUY CUOMO,
Petitioner,

-v.-

UNITED STATES OF AMERICA,
Respondent.

PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

Andrew Levchuk
Counsellor at Law
69 South Pleasant Street
Suite 203
PO Box 810
Amherst, MA 01004
Tel: 413-461-4530
alevchuk@agllegalnet.com
Attorney for Petitioner

QUESTIONS PRESENTED

1. Whether petitioner knowingly accessed a public computer "without authorization" within the meaning of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2), or conspired to do so, when he accessed a public computer system which anyone could access and use to obtain information, but navigated to a certain area within the computer system that limited access.

2. Whether the evidence was sufficient to establish that appellant a) falsely represented a number to be the social security account number assigned to him, or b) conspired to commit that offense, since the draft applications for unemployment were never submitted.

LIST OF PARTIES

All parties appear in the caption of the case on the cover page.

RELATED CASES

Petitioner is unaware of any related cases pending in this Court.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

OPINION BELOW

The summary order and judgment of the United States Court of Appeals for the Second Circuit, entered January 3, 2025, is reported at 125 F.4th 354 and is found at Appendix A.

JURISDICTION

The court of appeals issued its judgment on March 13, 2025. This Court's jurisdiction is invoked under 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

The Computer Fraud and Abuse Act ("CFAA"), Title 18, United States Code, Section 1030, provides in relevant part:

> (a) Whoever—
> . . .
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
> . . .
>
> (C) information from any protected computer;
>
> . . .
>
> (b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
> . . .
>
> (e)(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an

automated typewriter or typesetter, a portable hand held calculator, or other similar device . . .

(6) the term "exceeds authorized access" means 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 . . . .

Title 42, United States Code, Section 408(a), provides in relevant part:

(7) for the purpose of causing an increase in any payment authorized under this title [42 USCS §§ 401 et seq.] (or any other program financed in whole or in part from Federal funds), or for the purpose of causing a payment under this title [42 USCS §§ 401 et seq.] (or any such other program) to be made when no payment is authorized thereunder, or for the purpose of obtaining (for himself or any other person) any payment or any other benefit to which he (or such other person) is not entitled, or for the purpose of obtaining anything of value from any person, or for any other purpose—
. . .

(B) with intent to deceive, falsely represents a number to be the social security account number assigned by the Commissioner of Social Security to him or to another person, when in fact such number is not the social security account number assigned by the Commissioner of Social Security to him or to such other person . . .

STATEMENT

1. Petitioner Guy Cuomo was charged in a superseding indictment on April 29, 2021, with conspiracy to commit computer fraud, in violation of 18 U.S.C. § 1030(b) (Count 1); accessing a protected computer and obtaining information, in violation of 18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(i) (Count 2); aggravated identity theft, in violation of 18 U.S.C. § 1028A (Counts 7 and 18); conspiracy, in violation of 18 U.S.C. § 371 (Count 12); and misuse of a social security number, in violation of 42 U.S.C. § 408(a)(7)(B) (Count 13). Following a jury trial in the United States

District Court for the Northern District of New York, Cuomo was convicted on all counts. He was sentenced to a total of 45 months' imprisonment, to be followed by three years on supervised release. *See United States v.* Cuomo, 125 F.4th 354, 359 (2d Cir. 2025).

2. As recounted by the court of appeals, the prosecution had its origin in investigations by the United States Department of Labor's Office of the Inspector General ("DOL-OIG") into suspected crimes involving unemployment insurance (or "UI") programs. From 2015 through April 2018 Cuomo, along with codefendant Jason "J.R." Trowbridge, was involved with Paymerica Corporation and a sister company called Ameripay Corporation ("Ameripay") (collectively "Paymerica") that engaged in debt collection. "Skip tracing" (or "skiptracing") refers generally to a process of finding information about a judgment debtor, such as his or her address, telephone number, and place of employment (or "POE"). 125 F.4th at 360.

Paymerica Corporation and Ameripay shared office space and had substantial financial and employee overlap. In their skip tracing operations, Paymerica employees obtained debtors' POE information by entering the debtors' names and personal information in commencing uncompleted online applications for unemployment insurance in the states where the debtors lived. *Id.*

When Paymerica's customers provided Paymerica with the names, social security numbers, and addresses of debtors whose POE information the customers sought to purchase, Paymerica employees initially verified this personal-identifying information--including social security numbers--for the debtors by using TLO, a

commercial database. From there, Paymerica employees obtained the requested POE information for the debtors from state workforce agencies by starting electronic unemployment applications in each debtor's name and with each debtor's personal-identifying information. Among other things, Paymerica employees created online accounts in the debtors' names with the states--for instance, a NY.gov account in New York--and then used the online accounts to start unemployment applications in the debtors' names by submitting, *inter alia*, the debtor's name, date of birth, and social security number. *Id.*

Cuomo personally entered debtors' personal information in starting New York State unemployment applications, including C.C. and S.A., the respective victims of the substantive identity theft counts against him. In March 2018, Cuomo logged on to the New York State unemployment website and initiated unemployment insurance applications in the names of C.C. and S.A. in order to learn their POEs; in response to the website requests for personal information to identify the person inquiring, Cuomo provided C.C.'s and S.A.'s respective social security numbers, which Paymerica had been given by its customers. C.C. and S.A. testified that they did not apply for unemployment insurance in March 2018, had not heard of Paymerica, did not know Cuomo or Trowbridge, and had not authorized anyone to use their names or social security numbers to apply for unemployment insurance for them. 125 F.4th at 360-61.

There was no evidence that Cuomo or his coconspirators actually filed an unemployment insurance application for any debtor they impersonated. They

initiated applications because merely starting that process gave them access to the debtor's most recent employer; none of the applications was completed. Once Paymerica obtained the POE information, it was sold to the requesting third parties. 125 F.4th at 361.

3.a. The court of appeals affirmed Cuomo's substantive and conspiracy convictions under the CFAA. The court rejected Cuomo's contention that his computer searches for debtors' POEs were not "without authorization" within the meaning of § 1030(a) because he used a website that was available to the public. Cuomo argued that if he committed a violation of Section 1030(a)(2), he at most "exceeded authorized access" to a public site, a charge not contained in the indictment. The court of appeals failed to acknowledge or discuss the two-pronged structure of Section 1030(a)(2) and how the "without authorization" and "exceeding authorized access" provisions relate to each other. The court of appeals found it insignificant that any member of the public could create a ny.gov account, or that Ny.gov could be used to access a host of public services, or that there was no password or other gate blocking entry to ny.gov except for certain areas of the network. 125 F.4th at 363-65.

The court also resorted to a technological *non-sequitur*: "Cuomo's argument mistakenly conflates websites and computers. Section 1030(a)(2) refers to accessing 'computer[s],' not accessing websites." 125 F.4th at 364. This statement reflects a misunderstanding of the workings of the Internet and of the trial testimony, because accessing a website is necessarily accessing a computer, as explained below. The

court further found that because part of the ny.gov required entry of personal information – which Cuomo admittedly entered – entry of information of a judgment debtor amounted to accessing the ny.gov network "without authorization." But the court of appeals simply misread the broad definition of "computer" in Section 1030(e)(1) to limit a public computer system to one discrete computer among many comprising the ny.gov network, a public site.

b. The court also affirmed Cuomo's substantive and conspiracy convictions under 18 U.S.C. 371 and 42 U.S.C. 408(a)(7)(B). Section 404(a)(7) makes it a felony for any person to, *inter alia*, "for the purpose of obtaining anything of value from any person, or for any other purpose-- . . . (B) with intent to deceive, falsely represent[] a number to be the social security account number assigned by the Commissioner of Social Security to him or to another person, when in fact such number is not the social security account number assigned by the Commissioner of Social Security to him or to such other person."

Cuomo argued that he did not make false representations about the social security numbers, which he legally possessed in an attempt to collect judgments. In using social security numbers to obtain POE information, Cuomo was not acting with intent to deceive anyone. He accordingly sought a jury instruction requiring a showing that he "intended to deceive *someone* for any purpose," and that "[t]o 'act with intent to deceive' simply means to act deliberately for the purpose of misleading *someone*." (Cuomo's Proposed Jury Charge at 4 (emphases added); *see* Trial Tr. 755-58.)

The court of appeals rejected Cuomo's claim. It stated that:

> Section 408(a)(7)(B) does not require that the defendant's social-security-number misuse with "intent to deceive" have been successful. And the court found that there was sufficient evidence to show that Cuomo intended to deceive New York State. 'New York State required that a user seeking to access employment records stored on the New York State computer provide the user's own social security number; the gate was "put into place to prevent people from seeing records of other people' ([Trial] Tr. 156; *see id.* at 151-52; *see also id.* at 278 (Paymerica employees skip traced in some 15-20 states, all of which required user-identity verification through social security numbers).) . . . [T]o circumvent New York's identity verification requirement, Cuomo falsely created ny.gov accounts in the names of debtors whose POE information he wanted to get for his customers; and when, as the user, he was asked for his social security number he entered not his own social security number but the numbers of the debtors.

125 F.4th at 367-68. The court of appeals thus concluded that the evidence was sufficient to allow the jury to find that Cuomo, with intent to deceive state governments, provided debtors' social security numbers, falsely claiming they were his own—and conspired to do so—in order to obtain access to and sell debtors' POE information to Paymerica's customers, in violation of 42 U.S.C. § 408(a)(7)(B) and 18 U.S.C. § 371

REASONS FOR GRANTING THE PETITION

1. The court of appeals' decision erroneously expands the meaning of "without authorization" in Section 1030(a)(2) to include public computers or computer networks that limit access to certain areas or information. This is a misreading of the statute. The court of appeals limited alternative the "exceeds authorized access" provision of Section 1030(a)(2) to "defendants who concededly

had authorization to access the relevant computer but did so for *improper purposes*." 125 F.4th at 363 (emphasis added). That is flatly contrary to the definition in the statute, which defines the term "exceeds authorized access" to mean "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." 18 U.S.C. § 1030(e)(6). If Cuomo committed a CFAA offense, he "exceed[ed] authorized access," but that was neither charged in the indictment nor presented to the jury. This Court should grant certiorari to correct the court of appeals manifest error and to resolve a conflict with *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1199 (9th Cir. 2022) (concept of "without authorization" does not apply to public websites).

Judge Kearse's opinion asserted that Cuomo "mistakenly conflates websites and computers. Section 1030(a)(2) refers to accessing 'computer[s],' not accessing websites." *United States v. Cuomo*, 125 F.4th 354, 363 (2025). This statement reflects a fundamental misunderstanding of how one remotely accesses a "computer." A website coded in HTML or otherwise is a tool to access information stored on a computer. The government's expert testified that a "website" is simply a tool to facilitate interaction with the computer system behind it (Trial Tr. 157-58). It makes no sense to posit that someone using a web browser who navigates to ssa.gov or amazon.com is not accessing computers maintained by the Social Security Administration or Amazon.

The Computer Fraud and Abuse Act, Section 1030(a)(2) of Title 18, proscribes accessing a protected computer "without authorization" or "exceed[ing] authorized access." *Van Buren v. United States*, 593 U.S. 374, 390 (2021), reasoned that the "gates-up-or-down" structure of 18 U.S.C. § 1030(a)(2) "treats the 'without authorization' and 'exceeds authorized access' clauses consistently." *United States v. Cuomo*, 125 F.4th 354, 363 (2025). "Without authorization" refers to whether "one either can or cannot access a computer system," and "exceeds authorized access" refers to whether "one either can or cannot access *certain areas* within the system." *Id.*, citing *Van Buren*, 593 U.S. at 390 (emphasis added).

The question for purposes of Section 1030(a)(2), the offense charged in this case, is whether the user is accessing a protected computer such as ny.gov with authorization, or either 1) without authorization, or 2) exceeding authorized access. When Cuomo or his colleagues navigated their way through web pages at ny.gov, they were accessing the ny.gov computers *with* authorization, as the undisputed testimony of the government's witnesses established. Ny.gov could be used to access a host of services, including searching for jobs, creating a JobZone profile, getting assistance with employment-related activities, like resume writing, cover letters, and interview skills; or exploring careers, training opportunities, apprenticeship opportunities, and other job seeker resources, and accessing services for veterans. *See* C.A. App. A99. These computer-based services were available to the public and off limits to no one. There was no "gate" blocking entry to ny.gov. Trial Tr. 141.

If Cuomo committed a crime, it was by exceeding his authorized access to obtain information protected by a "gate" requiring the entry of sensitive personal information. In the words of *Van Buren*, Cuomo accessed "*certain areas* within the system" that were off limits to him. *See Van Buren*, 593 U.S. at 390 (emphasis added). Trial Tr. 152. As the court of appeals put it, "[w]hen the website's host computer introduces 'gates' for areas of the website that require authorization to access, those parts of the website and the computer or computers hosting them are not freely available to the public." 125 F.4th at 364. But Cuomo was not charged with "exceeding authorized access" to "those parts of the website and the computer or computers hosting them [that] are not freely available to the public"; he was instead charged solely with accessing a computer system entirely "without authorization." C.A. App. A85. This was the only theory on which the jury was charged. Trial Tr. 722. Therefore, Cuomo was charged under the wrong subsection of Section 1030(a)(2), and the substantive and conspiracy convictions based on Section 1030(a)(2) should have been reversed.

Recognizing this defect in its case, the government focused on one mainframe computer accessible from ny.gov. But "computer" is defined broadly under the CFAA to include not just individual devices like the mainframe but "any data storage facility or communications facility directly related to or operating in conjunction with" a discrete computing device. *See* 18 U.S.C. § 1030(e)(1). Thus the "computer" at issue in this case was the data storage facility pictured on Government Exhibit 10, which contained multiple individual computing devices.

See Gov't C.A. App. 9. This Court recently confirmed that the question of one's "authorization" under Section 1030(a) is whether "one either can or cannot access a computer *system*." *Van Buren*, 593 U.S. at 390 (2021) (emphasis added). This was a computer data facility with "multiple systems" and the mainframe containing the sensitive information was only part of that system. Trial Tr. 151, 159. The network of devices on Government Exhibit 10 (*see* Gov't C.A. App. 9) fell within the definition of "computer" for purposes of Section 1030(e)(1). Cuomo and the public at large had access to many areas of the system, but the area containing place-of-employment information at issue in this case required the entry of certain personal data. When Cuomo entered this information, he may have been exceeding authorized access to the computer system behind ny.gov, but it is simply wrong to find that he accessed a "computer," as defined in 18 U.S.C. Section 1030(e)(1), without authorization.

The court of appeals failed to consider that a recent post-*Van Buren* Ninth Circuit decision confirms this approach. In *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1197-98 (9th Cir. 2022), the Ninth Circuit observed:

> the CFAA contemplates the existence of three kinds of computer systems: (1) computers for which access is open to the general public and permission is not required, (2) computers for which authorization is required and has been given, and (3) computers for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed).

Ny.gov was the of the third variety, where no authorization was required for parts of the system, but was required for certain areas in the system.

> *Van Buren*'s distinction between computer users who "can or cannot access a computer system," . . . suggests a baseline in which there are "limitations on access" that prevent some users from accessing the system (*i.e.*, a "gate" exists, and can be either up or down). The Court's "gates-up-or-down inquiry" thus applies to the latter two categories of computers we have identified: if authorization is required and has been given, the gates are up; if authorization is required and has not been given, the gates are down. As we have noted, however, a defining feature of public websites is that their publicly available sections lack limitations on access; instead, those sections are open to anyone with a web browser. In other words, applying the "gates" analogy to a computer hosting publicly available webpages, that computer has erected no gates to lift or lower in the first place. *Van Buren* therefore reinforces our conclusion that the concept of "without authorization" does not apply to public websites.

hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1199 (9th Cir. 2022). The court of appeals analysis in this case is in conflict with *hiQ Labs*. Unlike the court of appeals in this case, the Ninth Circuit did not labor under the confusion that accessing a website is somehow different from accessing a computer.

Finally, the court of appeals stated that "the gate at issue here is code-based." 125 F.4th at 364. But there was no "gate" for the system as a whole—only, at most, for that part of the system that contained place-of-employment information. Cuomo may have exceeded his otherwise authorized access to the computer system when accessing this information on the mainframe. But again, he was not charged, and the jury was not instructed, on the "exceeding authorized access" prong of Section 1030(a)(2).

In conclusion, the court of appeals' flawed distinction between "computers" and "websites" will, if left unaddressed, lead to perverse outcomes. If a malefactor defaces this Court's website by altering the code, can he defend against a Section

1030(a) prosecution by claiming that he only exceeded authorized access to the Court's "website"—and not a "computer"? If a hacker uses stolen credentials to access someone's AWS database on the web, Section 1030(a)(2) may not apply because she has accessed a mere "website" without authorization. And the court of appeals also erred in interpreting "computer" in the superseding indictment to mean just the mainframe, rather than the public computer system of which it was only a part. In sum, the Court's opinion is fundamentally flawed and re-writes Section 1030(a)(2).

2. Under Title 42, United States Code, Section 408(a)(7)(B), it is a crime if a defendant "with intent to deceive, falsely represents a number to be the social security account number assigned by the Commissioner of Social Security to him or to another person, when in fact such number is not the social security account number assigned by the Commissioner of Social Security to him or to such other person." The government's theory was that Cuomo and his colleagues violated this section by "impersonating" judgment debtors.

"Intent to deceive" means to act for the purpose of misleading someone. The government failed to prove that Cuomo intended to deceive anyone. Rather than deceiving anyone, Cuomo used information legally in his possession to discover non-confidential facts, *i.e.*, finding out where judgment debtors worked. No "intent to deceive" was involved.

The applications were never submitted and therefore never reviewed by anyone at the NYS Department of Labor. Trial Tr. 140-42. And violation of

computer use restrictions does not involve an intent to deceive. A contrary ruling would, in effect, give computer algorithms a status of victims.

This prosecution is unlike other Section 408 violations considered by the Second Circuit and other courts, all of which involved defendants acting with intent to deceive to obtain tangible benefits such as student loans or access devices. *United States v. Wilson*. 709 F.3d 84 (2d Cir. 2013) (access device fraud); *United States v. Fiore*, 169 F.3d 104 (2d Cir. 1999) (fraudulent claim for workers compensation benefits); *United States v. Gibson*, 770 F.2d 306 (2d Cir 1985) (student loans). The individual judgement debtors were hardly victims, given that they were under court orders to repay the debts in question, and the only information about them that was obtained through the alleged scheme was where they worked. New York State was not a defrauded "victim" in any real sense of the offenses charged.

To support a finding of guilt, the government needed to prove that the social security number was falsely represented to someone with intent to deceive. Again, given that the unemployment applications were never submitted, the social security numbers were never falsely "represented" to anyone, nor did anyone conspire to falsely represent social security numbers. And in any event, there was no intent to deceive anyone or conspiracy to do so. The convictions on Counts Twelve and Thirteen are based on a flawed interpretation of Section 408(a)(7)(B).

The government's theory under Section 408(a)(7)(B) was that Cuomo and his colleagues violated this section by impersonating judgment debtors. But

impersonation means more than simply using identification information in an attempt to assist in the collection of a civil judgment. *See* Oxford English Dictionary (1971) (defining "impersonate" as "to invest with an actual personality; to embody.") Black's defines "deceit" as "[t]he act of leading someone to believe something that is not true . . . ." Black's Law Dictionary, p. 491 (10th ed. 2014). Deceit must be directed at someone, and the government failed to prove that Cuomo intended to deceive anyone, including New York State. Cuomo used information legally in his possession (Trial Tr. 176, 205, 275-76, 355, 409-10, 451-53) to discover non-confidential facts, *i.e.*, finding out where judgment debtors worked. This Court should grant certiorari to correct his very fundamental misinterpretation of Section 408(a)(7)(B).

CONCLUSION

The Court should grant the petition for a writ of certiorari on both questions presented.

Dated: June 4, 2025

Respectfully submitted,

/s/Andrew Levchuk

Andrew Levchuk
Counsellor at Law
69 South Pleasant Street
Suite 203
PO Box 181
Amherst, Massachusetts 01002
alevchuk@agllegalnet.com
Attorney for Petitioner

APPENDIX A

United States v. Guy Cuomo, **Page**

United States v. Cuomo

United States Court of Appeals for the Second Circuit

February 12, 2024, Argued; January 3, 2025, Decided

Docket No. 22-1799

Reporter
125 F.4th 354 *; 2025 U.S. App. LEXIS 80 **; 2025 WL 21435

UNITED STATES OF AMERICA, Appellee, - v. - GUY CUOMO, a.k.a. John Monaco, Defendant-Appellant.*

Prior History: Appeal from a judgment entered in the United States District Court for the Northern District of New York, following a jury trial before Thomas J. McAvoy, Judge, and sentencing by Mae A. D'Agostino, Judge, convicting defendant of conspiracy to commit computer fraud, in violation of *18 U.S.C. §§ 1030(b)*, *1030(a)(2)(C)*, and *1030(c)(2)(B)(iii)*; accessing a protected computer and obtaining information without authorization, in violation of *18 U.S.C. §§ 1030(a)(2)(C)* and *1030(c)(2)(B)(i)*; two counts of aggravated identity theft, in violation of *18 U.S.C. § 1028A(a)(1)*; misuse of a social security number, in violation of *42 U.S.C. § 408(a)(7)(B)*; and conspiracy to misuse social security numbers, in violation of *18 U.S.C. § 371*; and sentencing him principally to a total of 45 months' imprisonment, to be followed by a total of three years' supervised release. On appeal, defendant contends principally that his convictions should be reversed on the grounds that his conduct did not violate the *Computer Fraud and Abuse Act, 18 U.S.C. § 1030*, and *Social Security Act § 206, 42 U.S.C. § 408* **[**1]** ; that the court's instructions to the jury were deficient with respect to the counts relating to computer fraud and social-security-number misuse; and that the evidence was insufficient to support his convictions relating to identity theft and social-security-number misuse. Finding no merit in these contentions, or in his challenges to the calculation **[**2]** of his sentence, we affirm.

Core Terms

authorization, website, social security number, employees, sentencing, misuse, user, district court, convictions, counts, identity theft, enhancement, conspiracy, accessing, unemployment insurance, Guidelines, aggravated, customers, gate, contends, skip, intent to deceive, impersonated, challenges, records, personal information, computer fraud, social-security-number, quotation, deceived

Case Summary

Overview
Key Legal Holdings

- The evidence was sufficient to support the jury's findings that Cuomo accessed a computer without authorization and thereby obtained information from a protected computer in violation of the Computer Fraud and Abuse Act (CFAA).
- Cuomo's conduct of providing debtors' social security numbers, falsely claiming they were his own, to obtain access to and sell debtors' employment information violated the Social Security Act.

* The Clerk of Court is instructed to amend the official caption to conform with the above.

- The evidence was sufficient to support Cuomo's convictions for aggravated identity theft under *18 U.S.C.S. § 1028A(a)*.

Material Facts

- Cuomo operated a skip tracing company that obtained debtors' employment information by impersonating the debtors and starting fraudulent unemployment insurance applications using their personal information.
- To bypass New York State's authentication requirements for accessing employment records, Cuomo falsely created accounts in debtors' names and provided their social security numbers.
- Cuomo was convicted of computer fraud, misuse of social security numbers, aggravated identity theft, and related charges.

Controlling Law

- *Computer Fraud and Abuse Act (CFAA), 18 U.S.C.S. § 1030*.
- *Social Security Act, 42 U.S.C.S. § 408*.
- Aggravated Identity Theft statute, *18 U.S.C.S. § 1028A*.

Court Rationale

The evidence showed that New York State's computer system had authentication requirements that Cuomo bypassed to obtain employment records without authorization, in violation of the Computer Fraud and Abuse Act (CFAA). Cuomo's provision of debtors' social security numbers while falsely claiming they were his own demonstrated the intent to deceive required for a Social Security Act violation. Cuomo's use of debtors' personal information was integral to the fraud offenses, satisfying the requirements for aggravated identity theft under Dubin v. United States.

Outcome
Procedural Outcome Section 408(a)(7)(B)

The Second Circuit affirmed Cuomo's convictions and sentence.

LexisNexis® Headnotes

Criminal Law & Procedure > ... > Standards of Review > De Novo Review > Sufficiency of Evidence

Governments > Legislation > Interpretation

Evidence > Inferences & Presumptions > Inferences

HN1[] **De Novo Review, Sufficiency of Evidence**

The standard of review for issues of statutory interpretation is de novo. For sufficiency of evidence challenges, although the ultimate legal question is reviewed de novo, the standard of review is exceedingly deferential to the jury's factual determinations. Evidence is viewed in the light most favorable to the government, crediting every

credibility determination and inference that could have been drawn in the government's favor. A sufficiency challenge fails if any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.

Criminal Law & Procedure > ... > Standards of Review > Plain Error > Definition of Plain Error

Criminal Law & Procedure > ... > Standards of Review > Plain Error > Jury Instructions

HN2 **Plain Error, Definition of Plain Error**

Challenges to jury instructions that have been properly preserved are reviewed de novo. Unpreserved challenges to instructions are reviewed only for plain error. Under plain-error review, there is discretion to reverse only if the instruction contains error that is plain and affects substantial rights. If these conditions are met, the error may be corrected only if it seriously affected the fairness, integrity, or public reputation of judicial proceedings.

Business & Corporate Compliance > Computer & Internet > Criminal Offenses > Data Crimes & Fraud
Computer & Internet Law > Criminal Offenses > Data Crimes & Fraud

Computer & Internet Law > Criminal Offenses > Computer Fraud & Abuse Act

Criminal Law & Procedure > ... > Fraud > Computer Fraud > Elements

HN3 **Criminal Offenses, Data Crimes & Fraud**

The Computer Fraud and Abuse Act (CFAA) provides that it is unlawful to intentionally access a computer without authorization or exceed authorized access, and thereby obtain information from any protected computer, or to conspire to do so. *18 U.S.C.S. 1030(a)(2)(C)* and *18 U.S.C.S. 1030(b)*. The CFAA defines protected computer as one used in or affecting interstate or foreign commerce or communication. *18 U.S.C.S. 1030(e)(2)(B)*. Exceeds authorized access means 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. *18 U.S.C.S. 1030(e)(6)*.

Computer & Internet Law > Criminal Offenses > Computer Fraud & Abuse Act

Governments > Legislation > Interpretation

Criminal Law & Procedure > ... > Fraud > Computer Fraud > Elements

HN4 **Criminal Offenses, Computer Fraud & Abuse Act**

The word "authorization" is not defined in the Computer Fraud and Abuse Act, and courts have viewed it as a word of common usage, without any technical or ambiguous meaning. It thus suggests permission or power granted by authority.

Business & Corporate Compliance > Computer & Internet > Criminal Offenses > Data Crimes & Fraud
Computer & Internet Law > Criminal Offenses > Data Crimes & Fraud

Computer & Internet Law > Criminal Offenses > Computer Fraud & Abuse Act

Criminal Law & Procedure > ... > Fraud > Computer Fraud > Elements

HN5 **Criminal Offenses, Data Crimes & Fraud**

The Supreme Court treats the Computer Fraud and Abuse Act's without authorization and exceeds authorized access clauses as coordinated elements of the computer-context understanding of access as entry. It reasoned that the gates-up-or-down statutory structure treats the without authorization and exceeds authorized access clauses consistently, as without authorization refers to whether one either can or cannot access a computer system, and exceeds authorized access refers to whether one either can or cannot access certain areas within the system. The court suggested that such gates might consist of a specific type of authorization, that is, authentication, which turns on whether a user's credentials allow him to proceed past a computer's access gate, rather than on other, scope-based restrictions.

Criminal Law & Procedure > Trials > Jury Instructions > Requests to Charge

HN6 **Jury Instructions, Requests to Charge**

A defendant is not entitled to have the court give a proposed instruction to the jury unless it is legally correct.

Criminal Law & Procedure > Criminal Offenses > Fraud

Public Health & Welfare Law > Social Security > Disability Insurance & SSI Benefits > Social Security Act Interpretation

Criminal Law & Procedure > ... > Acts & Mental States > Mens Rea > Specific Intent

HN7 **Criminal Offenses, Fraud**

42 U.S.C.S. 408(a)(7)(B) does not require that the defendant's social-security-number misuse with intent to deceive have been successful.

Criminal Law & Procedure > Criminal Offenses > Fraud

HN8 **Criminal Offenses, Fraud**

With fraud or deceit crimes, the means of identification specifically must be used in a manner that is fraudulent or deceptive.

Criminal Law & Procedure > ... > Appeals > Standards of Review > Abuse of Discretion

Criminal Law & Procedure > ... > Appeals > Standards of Review > De Novo Review

Criminal Law & Procedure > Appeals > Standards of Review > Abuse of Discretion

HN9 **Standards of Review, Abuse of Discretion**

The reasonableness of sentencing decisions is reviewed for abuse of discretion, a standard incorporating de novo review of questions of law, including interpretation of the Sentencing Guidelines, and clear error review of questions of fact.

Criminal Law & Procedure > ... > Sentencing Guidelines > Adjustments & Enhancements > Aggravating Role

Criminal Law & Procedure > ... > Inchoate Crimes > Conspiracy > Penalties

HN10[] Adjustments & Enhancements, Aggravating Role

The Sentencing Guidelines recommend a four-step increase in offense level for a defendant who was an organizer or leader of a criminal activity that involved five or more participants, including the defendant. U.S. Sentencing Guidelines Manual § 3B1.1(a). Whether a defendant is considered a leader depends upon the degree of discretion exercised by the defendant, the nature and degree of participation in planning or organizing the offense, and the degree of control and authority exercised over the other members of the conspiracy. A defendant may be a leader of a crime even if it was planned, financed, and orchestrated by another participant.

Criminal Law & Procedure > ... > Sentencing Guidelines > Adjustments & Enhancements > Aggravating Role

Criminal Law & Procedure > Sentencing > Imposition of Sentence > Findings

HN11[] Adjustments & Enhancements, Aggravating Role

A district court's conclusion that a defendant met the criteria for a leadership enhancement under U.S. Sentencing Guidelines Manual § 3B1.1(a) is reviewed de novo, but the court's findings of fact supporting its conclusion are reviewed for clear error. Sentencing judges are given latitude concerning their supervisory role findings, even when their findings are not as precise as they might have been, so long as their findings are sufficient to permit meaningful appellate review.

Criminal Law & Procedure > ... > Appeals > Standards of Review > Clear Error Review

Criminal Law & Procedure > Sentencing > Imposition of Sentence > Findings

Criminal Law & Procedure > ... > Standards of Review > Clearly Erroneous Review > Sentences

HN12[] Standards of Review, Clear Error Review

A sentencing court's findings as to the defendant's role in the offense will be overturned only if they are clearly erroneous. Where there are two permissible views of the evidence, the factfinder's choice between them cannot be clearly erroneous.

Criminal Law & Procedure > ... > Sentencing Guidelines > Adjustments & Enhancements > Aggravating Role

HN13[] Adjustments & Enhancements, Aggravating Role

The Sentencing Guidelines recommend a two-step increase in offense level if the defendant was convicted of an offense under 18 U.S.C.S. 1030, and the offense involved an intent to obtain personal information. U.S. Sentencing Guidelines Manual § 2B1.1(b)(18)(A).

Criminal Law & Procedure > ... > Standards of Review > Harmless & Invited Error > Harmless Error

Criminal Law & Procedure > Sentencing > Ranges

Criminal Law & Procedure > ... > Sentencing Guidelines > Departures From Guidelines > Judicial Review

HN14[] **Harmless & Invited Error, Harmless Error**

An error in Sentencing Guidelines calculation is harmless if correcting the error would result in no change to the Guidelines offense level and sentencing range. The Guidelines provide that appropriate offense-characteristic enhancements are to be applied before the application of adjustments on account of the defendant's role. *U.S. Sentencing Guidelines Manual § 1B1.1(a)*.

Counsel: STEVEN D. CLYMER, Assistant United States Attorney, Syracuse, New York (Carla B. Freedman, United States Attorney for the Northern District of New York, Joshua R. Rosenthal, Assistant United States Attorney, Syracuse, New York, on the brief), for Appellee.

ANDREW LEVCHUK, Amherst, Massachusetts, for Defendant-Appellant.

Judges: Before: KEARSE, PARK, and PÉREZ, Circuit Judges.

Opinion by: KEARSE

Opinion

[*359] KEARSE, *Circuit Judge*:

Defendant Guy Cuomo appeals from a judgment entered in the United States District Court for the Northern District of New York, following a jury trial before Thomas J. McAvoy, *Judge*, and sentencing by Mae A. D'Agostino, *Judge*, convicting him of conspiracy to commit computer fraud, in violation of *18 U.S.C. §§ 1030(b)*, *1030(a)(2)(C)*, and *1030(c)(2)(B)(iii)* (Count 1); accessing a protected computer and obtaining information without authorization, in violation of *18 U.S.C. §§ 1030(a)(2)(C)* and *1030(c)(2)(B)(i)* (Count 2); aggravated identity theft, in violation of *18 U.S.C. § 1028A(a)(1)* (Counts 7 and 18); misuse of a social security number, in violation of *42 U.S.C. § 408(a)(7)(B)* (Count 13); and conspiracy to misuse social security numbers, in violation of *18 U.S.C. § 371* (Count 12); and sentencing him principally to a total of 45 months' imprisonment, to be followed by a total of three years' supervised release. On appeal, **[**3]** Cuomo contends principally that his convictions should be reversed on the grounds that his conduct did not violate the *Computer Fraud and Abuse Act, 18 U.S.C. § 1030*, and *Social Security Act § 206, 42 U.S.C. § 408*; that the court's instructions to the jury were deficient with respect to the counts relating to computer fraud and social-security-number misuse; and that the evidence was insufficient to support his convictions relating to identity theft and social-security-number misuse. He also contends that the court erred in calculating his sentence. Finding no merit in any of his contentions, we affirm.

I. BACKGROUND

The present prosecution had its origin in investigations by the United States Department of Labor's Office of the Inspector General ("DOL-OIG") into suspected crimes involving unemployment insurance (or "UI") programs. DOL-OIG Special Agents zeroed in on conduct from 2015 through April 2018 by Cuomo who, along with codefendant Jason "J.R." Trowbridge, operated both a "skip tracing" company called Paymerica Corporation and a sister company called Ameripay Corporation ("Ameripay") that ostensibly engaged in debt collection but also performed skip tracing. "Skip tracing" (or "skiptracing") refers generally to a process of finding information about a person--often **[**4]** a debtor--such **[*360]** as his or her address, telephone number, and place of employment (or "POE").

The trial evidence leading to Cuomo's conviction of the above offenses, taken in the light most favorable to the government, is described in detail in a Decision and Order of the district court dated July 13, 2022 ("D.Ct. Op."), denying motions by Cuomo for a judgment of acquittal. (*See* Cuomo brief on appeal at 3 ("The district court, as required by law, summarized the facts in the light most favorable to the verdicts." (footnote omitted)).) Under the same standard, we summarize the evidence as follows.

A. *The Evidence of Deceptive Practices*

Paymerica Corporation and Ameripay shared office space and had substantial financial and employee overlap; here, as in the district court proceedings, they will generally be referred to collectively as "Paymerica," D.Ct. Op. at 5-6. In their skip tracing operations, "Paymerica employees obtained debtors' POE information by impersonating the debtors" in commencing for them "online applications for unemployment insurance ('UI') in the states where the debtors lived." *Id.* at 6.

> [W]hen Paymerica's customers provided [Paymerica] with the names, social security numbers, **[**5]** and addresses of debtors whose POE information the customers sought to purchase, Paymerica employees initially verified this personal-identifying information--including social security numbers--for the debtors by using TLO, a commercial database. From there, *Paymerica employees obtained the requested POE information for the debtors from state workforce agencies by starting false UI applications in each debtor's name* and with each debtor's personal-identifying information. Among other things, *Paymerica employees created online accounts for the debtors* with the states--for instance, a NY.gov account in New York--and then *used the online accounts to start fraudulent UI applications in the debtors' names* by submitting, *inter alia*, the debtor's name, date of birth, and social security number.

Id. (record citations omitted) (emphases added). In addition,

> *Paymerica employees routinely created and used fraudulent email accounts . . . to circumvent identity-verification measures* implemented by New York and other state governments. *Four cooperating witnesses . . . testified that the entire process was about impersonating debtors*. According to the witnesses, this was done so that the states would **[**6]** falsely recognize Paymerica employees as the target debtors and provide restricted POE information meant only for those debtors to Paymerica.

Id. at 6-7 (record citations omitted) (emphases added); *see id.* at 6 (the "[f]our cooperating witnesses" were "Paymerica employees who . . . admittedly commit[ed] Computer Fraud, Misuse of a Social Security Number, or Aggravated Identity Theft").

"Paymerica employees took steps to avoid detection and cover up their actions. . . . The skip tracers always used aliases when making verification calls to victims' places of employment." *Id.* at 7 (record citations omitted). Cuomo himself, "for his skiptracing activities," used the alias "John Monaco." (Trial Transcript ("Tr.") 328-29.)

Cuomo also "personally impersonated numerous debtor-victims [in starting] New York State UI applications, including C.C. and S.A., the respective victims of the [identity theft] counts against [him]." D.Ct. Op. at 8. In March 2018, Cuomo logged on to the New York State UI website and initiated unemployment insurance applications **[*361]** in the names of C.C. and S.A. in order to learn their POEs; in response to the website requests for personal information to identify the person **[**7]** inquiring, Cuomo provided C.C.'s and S.A.'s respective social security numbers, which Paymerica had been given by its customers, *see, e.g., id.* at 12. C.C. and S.A. testified that they did not apply for unemployment insurance in March 2018, had not heard of Paymerica, did not know Cuomo or Trowbridge, and had "never authorized anyone to use their names or social security numbers to apply for unemployment insurance for them." D.Ct. Op. at 23-24.

In addition to the use of aliases, impersonations, and "phony email accounts,"

> Paymerica employees employed other means to evade the states' security measures. For example, when the state governments blocked an internet protocol ("IP") address associated with Paymerica's offices, Paymerica employees used a virtual private network ("VPN") *to mask their true IP address*. They also used untraceable,

internet-based phone systems that were paid for with *anonymous retail gift cards to further conceal their true identities*. In addition, when the states added additional identity verification questions in response to Paymerica's fraudulent activities, *the skip tracers used information from TLO to answer highly personal questions about the debtors they impersonated* ***[**8]*** .

Id. at 7-8 (record citations omitted) (emphases added).

Cuomo performed skip tracing himself, and when Trowbridge was not available he supervised the other Paymerica employees, including those engaged in skip tracing. *See id.* at 8. Cuomo also administered and maintained the TLO account--a subscription to a database maintained by TransUnion that contained public, proprietary, and personal information. Trowbridge could not be associated with that account because he had a prior felony conviction. *See id.* Cuomo "was . . . aware that Trowbridge and other[Paymerica employees] used VPNs and other measures to avoid detection by law enforcement." *Id.* (citing Tr. 559-60 (DOL-OIG Special Agent's testimony as to Cuomo's description to interviewing agents of his co-conspirators' use of various measures "'to hide from the states'" (other record citations omitted))). (*See* Part II.A.2. below with respect to confidentiality measures taken by New York State.)

There was no evidence that Cuomo or his coconspirators actually filed an unemployment insurance application for any debtor they impersonated. They initiated applications because merely starting that process gave them access to the debtor's most **[**9]** recent employer; none of the applications was completed. *See* D.Ct. Op. at 11-12.

"Once [Paymerica] obtained[] the POE information[, it] was sold to the requesting third parties for approximately $90 per debtor." *Id.* at 7 (citing Tr. 595-97). Paymerica had received requests from customers to research approximately 200,000 persons, and all 50 states were represented in those requests. (*See* Tr. 597.) In the period from mid-December 2015 to early April 2018, for its largest customer, Paymerica found POE information on some 11,294 individuals, for which it billed the customer $1,013,220. (*See id.* at 595-97.)

B. *The Verdict and Judgment*

The jury found Cuomo guilty of accessing a protected computer and obtaining information, in violation of *18 U.S.C. §§ 1030(a)(2)(C)* and *(c)(2)(B)(i)*, and of conspiracy to commit computer fraud, in violation of *18 U.S.C. §§ 1030(b)*, *(c)(2)(B)(i)*, and *(c)(2)(B)(iii)*, and found that those offenses had been committed "for purposes **[*362]** of commercial advantage or private financial gain." (Verdict Form at 1-2.) It found that the value of the information thereby obtained exceeded $5,000. (*See id.*) The jury also found Cuomo guilty of misuse of a social security number, in violation of *42 U.S.C. § 408(a)(7)(B)*; conspiring to misuse social security numbers, in violation of *18 U.S.C. § 371*; and **[**10]** two counts of aggravated identity theft (victimizing C.C. and S.A.), in violation of *18 U.S.C. § 1028A(a)(1)*.

Cuomo was sentenced principally to a total of 45 months' imprisonment. On Counts 1, 2, 12, and 13 (relating to computer fraud and misuse of social security numbers), he received four 21-month prison terms to be served concurrently with each other, based on calculations under the advisory Sentencing Guidelines ("Guidelines"). (*See* Part III below.) On Counts 7 and 18 (aggravated identity theft), Cuomo was sentenced--as mandated by *18 U.S.C. § 1028A(a)(1)*--to prison terms of 24 months, to be served consecutively to the 21-month prison terms on Counts 1, 2, 12, and 13. As allowed by *§ 1028A(b)*, the court ordered that the two 24-month terms for aggravated identity theft be served concurrently with each other.

II. CUOMO'S CHALLENGES TO HIS CONVICTIONS

On appeal, Cuomo contends principally that his convictions should be reversed on the grounds that his conduct did not violate either the Computer Fraud and Abuse Act of 1986 ("CFAA") or the Social Security Act. He also argues that the trial court's instructions on the counts charging violations of those statutes were erroneous or deficient, and that the evidence was insufficient to support his convictions of **[**11]** aggravated identity theft and misuse of, or conspiracy to misuse, social security numbers.

HN1[] As to issues of statutory interpretation, our standard of review is *de novo. See, e.g., United States v. Gu, 8 F.4th 82, 86 (2d Cir. 2021)* ("*Gu*"), *cert. denied*, *142 S. Ct. 1186, 212 L. Ed. 2d 49 (2022)*. And although we review

de novo the ultimate legal question of sufficiency of the evidence to support a conviction, our "standard of review is exceedingly deferential to the jury's apparent determinations" of facts. United States v. Flores, 945 F.3d 687, 710 (2d Cir. 2019) ("Flores") (internal quotation marks omitted), *cert. denied*, *141 S. Ct. 375, 208 L. Ed. 2d 97 (2020)*; *see* Gu, 8 F.4th at 86. We view the evidence in the light most favorable to the government, crediting every credibility determination and every inference that could have been drawn in favor of the government. *See, e.g.,* Flores, 945 F.3d at 710; Gu, 8 F.4th at 86. "A sufficiency challenge must fail if '*any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.'" Flores, 945 F.3d at 710 (quoting Jackson v. Virginia, 443 U.S. 307, 319, 99 S. Ct. 2781, 61 L. Ed. 2d 560 (1979) (emphasis in Jackson)).

HN2[⬆] We also review *de novo* challenges to the propriety of the trial court's instructions to the jury, if those challenges have been properly preserved. *See, e.g.,* United States v. Botti, 711 F.3d 299, 307 (2d Cir. 2013) ("Botti"); United States v. Bahel, 662 F.3d 610, 634 (2d Cir. 2011). Unpreserved challenges to instructions are reviewed only for plain error. *See, e.g.*, Fed. R. Crim. P. 30(d) and 52(b). Under plain-error review, we have "discretion to reverse only if the instruction contains **[**12]** '(1) error, (2) that is plain, and (3) affect[s] substantial rights'"; and if these three conditions are met, we may "exercise [our] discretion to correct the error only if the error 'seriously affect[ed] the fairness, integrity, or public reputation of judicial proceedings.'" Botti, 711 F.3d at 308 (quoting Johnson v. United States, 520 U.S. 461, 467, ***[*363]*** 117 S. Ct. 1544, 137 L. Ed. 2d 718 (1997)).

A. *The CFAA*

Cuomo contends that his convictions on Counts 1 and 2--computer fraud and conspiracy to commit computer fraud--should be reversed, arguing that his conduct did not violate the CFAA, that the evidence was insufficient to show that he accessed the computer without authorization, and that the district court erroneously instructed the jury as to the meaning of "without authorization." We reject all of these contentions.

1. *Statutory Construction*

HN3[⬆] The CFAA, dealing with fraud and related activity in connection with computers, provides in part that it is unlawful for a person (a) to "*intentionally access[] a computer without authorization* or exceed[] authorized access, *and thereby obtain*[] . . . *information from any protected computer*," or (b) to "conspire[]" to do so. 18 U.S.C. §§ 1030(a)(2)(C) and (b) (emphases added). The CFAA defines "protected computer" in part as a computer "which is used in or affecting interstate or **[**13]** foreign commerce or communication." *Id.* § 1030(e)(2)(B). "[T]he term 'exceeds authorized access' means 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." *Id.* § 1030(e)(6).

HN4[⬆] The word "authorization" is not defined in the CFAA, and we have viewed it as "a word of 'common usage, without any technical or ambiguous meaning,'" United States v. Valle, 807 F.3d 508, 524 (2d Cir. 2015) ("Valle") (quoting United States v. Morris, 928 F.2d 504, 511 (2d Cir.) ("Morris"), *cert. denied*, *502 U.S. 817, 112 S. Ct. 72, 116 L. Ed. 2d 46 (1991)*). It thus suggests "'permission or power granted by authority.'" Valle, 807 F.3d at 524 (quoting *Random House Unabridged Dictionary* 139 (2001)). Both Valle and Morris were prosecutions for alleged violation of the "exceeds authorized access" clause, by defendants who concededly had authorization to access the relevant computer but did so for improper purposes.

HN5[⬆] The Supreme Court has treated the CFAA's "without authorization" and "exceeds authorized access" clauses as coordinated elements of "the computer-context understanding of access as entry." Van Buren v. United States, 593 U.S. 374, 390, 141 S. Ct. 1648, 210 L. Ed. 2d 26 (2021). It reasoned that the "gates-up-or-down" statutory structure "treats the 'without authorization' and 'exceeds authorized access' clauses consistently," as "without authorization" refers to whether "one either can or cannot access a computer **[**14]** *system*," and "exceeds authorized access" refers to whether "one either can or cannot access *certain areas within* the system." Id. at 390 (emphases added). The Court suggested that such "gates" might consist of "a specific type of authorization--that is, authentication, which turns on whether a user's credentials allow him to proceed past a computer's access gate, rather than on other, scope-based restrictions." Id. at 390 n.9 (internal quotation marks omitted).

2. *Sufficiency of the Evidence*

Cuomo contends chiefly that his (and his cohorts') computer searches for debtors' POEs were not "without authorization" within the meaning of § 1030(a) because he (and they) used a website that is available to the public:

> To obtain place-of-employment information, Paymerica employees used ny.gov. All that was needed to create an account was a username and email address. Any **[*364]** member of the public could create a ny.gov account. . . .
>
> Ny.gov could be used to access a host of services, including searching for jobs, creating a JobZone profile, getting assistance with employment-related activities, like resume writing, cover letters, and interview skills; or exploring careers, training opportunities, apprenticeship opportunities, and other **[**15]** job seeker resources, and accessing services for veterans. . . . These services were available to any member of the public and off limits to no one. There was no gate blocking entry *to ny.gov*.

(Cuomo brief on appeal at 18-19 (emphasis added).) These arguments do not, however, reflect the scope of the CFAA or the structure of the gates on ny.gov.

First, Cuomo's argument mistakenly conflates websites and computers. Section § 1030(a)(2) refers to accessing "computer[s]," not accessing websites. As explained at trial by an Information Technology Services manager who had helped to design and develop the New York State process for filing online applications for unemployment insurance ("NYS-ITS Manager"), the website is not the computer itself. The computer "host[s]" the website; information on a website is housed on a computer; and on the website, a person can "look[] at something that's been compiled by a computer and displayed for" a "customer to look at." (Tr. 146; *see id.* at 144-47.) The "website is just a[n] interface" between the user and the computer (*id.* at 146); "the website cannot exist without a computer" (*id.* at 157); if the computer were turned off, "the website would disappear" (*id.* at 146).

Second, **[**16]** some parts of websites are "outward facing," *i.e.*, "they are exposed to the public" (*id.* at 145); but other parts are not (*see, e.g., id.* at 155). *See generally* ("[A] defining feature of public websites is that their *publicly available sections lack limitations on access*; instead, those sections are open to anyone with a web browser." (emphasis added)). When the website's host computer introduces "gates" for areas of the website that require authorization to access, those parts of the website and the computer or computers hosting them are not freely available to the public. *See id.* at 1198-99, 1199 n.17.

While Van Buren left open the question of whether the "gates-up-or-down inquiry" into authorization "turns only on *technological* (or 'code-based') *limitations on access*, or instead also looks to limits contained in contracts or *policies*," 593 U.S. at 390 n.8 (emphases added), we need not resolve that question because the gate at issue here is code-based. The NYS-ITS Manager testified that in 2017-2018, users could obtain information as to an individual's place of employment through ny.gov by taking two steps. To begin, users would have to create an ny.gov account, which merely required them to provide a name and a verifiable email address. (*See* Tr. 147.) **[**17]** To continue, the user could start an application for unemployment insurance; but in order to proceed further--and obtain information from the mainframe--the user was "required to put in a valid social security number and an address, mailing address[,] *to verify they are who they say they are*." (*Id.* at 151 (emphasis added); *see id.* at 161 (a person "ha[s] to enter . . . specific information *to access specific portions of the mainframe*" (emphasis added))). "When you fill out that application with the unemployment insurance area, it would go to the mainframe to actually pull records out for work history of a person *if they put in the proper social and address for that person*." (*Id.* at 152 (emphasis added).)

[*365] In sum, the trial record includes evidence that "[t]he mainframes at issue [in the NYS] Department of Labor" "host a lot of data. There's *no publicly facing website*," but it performs "a lot of" services including "providing data to someone who requests it" (*id.* at 158 (emphasis added))--and shows authorization to get it:

> [Y]ou can get into a web page but you might *not have access to records unless* you [have] *actually proven who you say you are*. . . . When you fill out that application with the unemployment **[**18]** insurance area, it would

> go to the mainframe to actually pull records out for work history *of a person* if they put in the proper *social and address for that person*.

(Tr. 151-52 (emphases added).) These controls were "put into place to prevent people from seeing records of other people." (*Id.* at 156.)

This evidence as to the New York State computer gates, along with the evidence described in Part I.A. above--as to Cuomo's and other Paymerica employees' impersonations and subterfuges to circumvent those gates and obtain POE information for Paymerica customers--was sufficient to support the jury's findings that Cuomo, in violation of *18 U.S.C. §§ 1030(a)(2)* and *(b)*, accessed, and conspired to access, a computer without authorization and thereby obtained information from a protected computer "for purposes of . . . private financial gain."

3. *The CFAA Instruction as to "Authorization"*

On appeal, Cuomo argues that the trial court gave the jury an erroneous instruction as to the meaning of "without authorization" in *18 U.S.C. § 1030(a)(2)*. He challenges the following instruction:

> "A computer's user accesses a computer without authorization if the user bypasses an authentication requirement that requires the user to demonstrate that the user **[**19]** is a person authorized to access the information [on] another computer. A password is an example of an authentication requirement but authentication requirements may take other forms."

(Cuomo brief on appeal at 31-32 (quoting Tr. 722).) Cuomo contends that this was erroneous because it "failed to acknowledge that Cuomo had a valid ny.gov account" (Cuomo brief on appeal at 32), and allowed the jury to believe "it could convict based on" "terms of service or contractual limitations imposed by a website" (*id.* at 32, 33), and that "[t]he jury should have been instructed, consistent with *Valle*, that to find that Cuomo acted without authorization, it had to find that Cuomo had no permission *at all* to access the ny.gov site" (*id.* at 33 (emphasis in original)).

Cuomo made no objection in the district court to the instructions on the CFAA counts. (*See, e.g.*, Tr. 747-58.) Thus, his present challenge to this instruction is reviewable only for plain error. He cannot meet that test because, *inter alia*, the instruction given by the court was not erroneous.

First, his complaint that the instruction did not acknowledge that he "had a valid ny.gov account" again conflates the computer with the website. Cuomo's **[**20]** access to the public-facing aspects of the website did not give him authorization to access the private POE information, stored on the mainframe, which he sought to obtain for Paymerica's customers.

Nor has Cuomo shown error or plain error by arguing that the jury should have been instructed that in order to find that he accessed the computer without authorization in violation of the CFAA, it needed to find that he had no permission **[*366]** at all to access the ny.gov site. In fact, the instruction fragment challenged by Cuomo as erroneous was preceded by the more appropriate instruction--omitted by Cuomo--that "*[a]ccess without authorization* means to *access a computer* without the permission of the computer's owner." (Tr. 722 (emphases added).)

Finally, as discussed in Part II.A.1. above, *Van Buren* indicated that identity "authentication, which turns on whether a user's *credentials* allow him to proceed past a computer's access gate," constitutes "a specific type of authorization." *593 U.S. at 390 n.9* (internal quotation marks omitted (emphasis ours)). The instruction here that a user who accesses a computer by bypassing the authentication requirement can be found to have accessed the computer "without authorization" was **[**21]** not error, much less an error that was "plain."

B. *Social-Security-Number Misuse*

Cuomo contends that his convictions on counts 13 and 12--misuse of a social security number and conspiracy to misuse social security numbers, respectively--should be reversed on the grounds that the district court gave an

erroneous instruction as to the elements of such misuse and erred in failing to instruct the jury as to the theory of his defense, and that under his proposed instructions the evidence was insufficient to support his convictions on those charges. These arguments are meritless.

The *Social Security Act, 42 U.S.C. § 301 et seq.*, makes it a felony for any person to, *inter alia*,

> for the purpose of obtaining anything of value from any person, or for any other purpose--
>
> . . . .
>
> (B) *with intent to deceive, falsely represent[] a number to be the social security account number assigned by the Commissioner of Social Security to him* or to another person, *when in fact such number is not the social security account number assigned by the Commissioner of Social Security to him* or to such other person.

42 U.S.C. § 408(a)(7)(B) (emphases added). The district court instructed the jury that the government was required to prove beyond a reasonable doubt that Cuomo, *inter alia*, **[**22]** "knowingly *represented to New York State* that the social security number described in" Count 13 "had been assigned to him by the Commissioner of Social Security." (Tr. 738 (emphasis added).) As to the "intent to deceive" element, the court instructed that

> [t]o act with intent to deceive means to act with the intention of misleading or giving false information. However, it is *not necessary for the government to prove that anyone was actually deceived or misled*.

(*Id.* at 740 (emphasis added).)

Cuomo objected to these instructions; he had requested that the jury be instructed that it needed to find that his claimed ownership and use of the debtor's social security number constituted a misrepresentation to "someone"--presumably a live person (*see generally* Cuomo brief on appeal at 36-37). His proposed change to the "represented to New York State" part of the court's instruction would have replaced "New York State" with "someone"; and as to the "intent to deceive" element, his proposed substitute would have told the jury that it needed to find that Cuomo "intended to deceive *someone* for any purpose," and that "[t]o 'act with intent to deceive' simply means to act deliberately for the purpose of misleading **[**23]** *someone*." (Cuomo's Proposed Jury Charge at 4 (emphases added); *see* Tr. 755-58.)

[*367] Cuomo's rationale is that these changes would have supported his "defense theory," which was "that the intent to defraud required by *Section 408* must be directed at someone, *a victim deceived by the fraud*" (Cuomo brief on appeal at 36 (emphasis added)), a "victim" who was a natural person. Thus, Cuomo argued to the district court that he was entitled to his proposed "someone" language because the government had "brought no one in who said I worked for the department of labor as a claim examiner and I was looking at this" (Tr. 757). And his attorney in summation pursued this line, asking "'who is Mr. Cuomo intending to deceive? The website? The computer? That was not his intention. His intention was to get the POE information and sell it.'" (Cuomo brief on appeal at 36 (quoting Tr. 817).)

HN6[↑] A defendant is not entitled to have the court give his proposed instruction to the jury unless it is, *inter alia*, legally correct. *See, e.g., United States v. Prawl, 168 F.3d 622, 626 (2d Cir. 1999)*. Cuomo's proposed language would not have been a correct instruction.

To begin with, his theory that to violate *§ 408* there must have been "*a victim deceived by the fraud*" (Cuomo brief on appeal at **[**24]** 36 (emphasis added)) finds no support in the language of the statute. ***HN7***[↑] *Section 408(a)(7)(B)* does not require that the defendant's social-security-number misuse with "intent to deceive" have been successful. The court's instruction that "it was not necessary for the government to prove that anyone was actually deceived or misled" was correct.

Second, Cuomo's repeated proposed references to "someone"--along with defense counsel's rhetorical questions "who is Mr. Cuomo intending to deceive? The website? The computer?" (Tr. 817), and his request to omit the reference to "New York State"--were apparently intended to imply that one could not be prohibited from, or

punished for, acting with intent to deceive or defraud a government. Such an implication would have been misleading and of course is fallacious, *see generally* 31 U.S.C. § 3729 (prohibiting frauds, or conspiracy to defraud, the United States Government); *see also* United States v. Yermian, 468 U.S. 63, 73 n.12, 104 S. Ct. 2936, 82 L. Ed. 2d 53 (1984) (to "[d]eceive is to cause to believe the false or to mislead" (internal quotation marks omitted)); N.Y. Penal Law § 195.20(a)(i) (McKinney 2024) (prohibiting schemes to defraud the State of New York or any of its political subdivisions or instrumentalities by means of, *inter alia*, "false . . . pretenses [or] representations"). The district **[**25]** court was not required to instruct the jury in accordance with Cuomo's erroneous legal theories.

Nor, with § 408(a)(7)(B) properly interpreted, as it was by the court, is there any merit in Cuomo's contention that the evidence was insufficient to support his convictions with respect to social-security-number misuse. As described in Part II.A.2. above, New York State required that a user seeking to access employment records stored on the New York State computer provide the user's own social security number; the gate was "put into place to prevent people from seeing records of other people" (Tr. 156; *see id.* at 151-52; *see also id.* at 278 (Paymerica employees skip traced in some 15-20 states, all of which required user-identity verification through social security numbers).) As described in Part I.A. above, to circumvent New York's identity verification requirement, Cuomo falsely created ny.gov accounts in the names of debtors whose POE information he wanted to get for his customers; and when, as the user, he was asked for his social security number he entered not his **[*368]** own social security number but the numbers of the debtors. (*See id.* at 582-92.) And, as Cuomo's attorney summarized at trial, Cuomo's **[**26]** "'intention was to get the POE information and sell it.'" (Cuomo brief on appeal at 36 (quoting Tr. 817 (his attorney's summation).)

In sum, the evidence was ample to allow the jury to find that Cuomo, with intent to deceive state governments, provided debtors' social security numbers, falsely claiming they were his own--and conspired to do so--in order to obtain access to and sell debtors' POE information to Paymerica's customers, in violation of 42 U.S.C. § 408(a)(7)(B) and 18 U.S.C. § 371.

C. *Aggravated Identity Theft*

Cuomo was convicted on two counts (Counts 7 and 18) of aggravated identity theft under 18 U.S.C. § 1028A(a). That subsection provides, in relevant part, that any person who

> *during and in relation to any felony violation enumerated in* subsection (c), knowingly . . . *uses, without lawful authority, a means of identification of another person* shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

18 U.S.C. § 1028A(a)(1) (emphases added). Subsection (c) defines the predicate "felony violation[s]" to include two categories applicable to Cuomo's conduct: "section 208 . . . of the Social Security Act (42 U.S.C. § 408(l)]," *see* 18 U.S.C. § 1028A(c)(11), and most provisions in Chapter 47 of Title 18 "relating to fraud," which include §§ 1030(a)(2) and (b), *see* 18 U.S.C. § 1028A(c)(4).

Cuomo contends that the evidence was insufficient to support **[**27]** his convictions for aggravated identity theft, arguing principally that there was insufficient evidence of the predicate felonies, *i.e.*, of computer fraud in violation of 18 U.S.C. § 1030 for Count 7, and of social-security-number misuse in violation of 42 U.S.C. § 408 for Count 18. These contentions lack merit. As discussed in Parts II.A. and B. above, the evidence to support the verdicts that Cuomo engaged in, respectively, computer-fraud offenses in violation of §§ 1030(a) and (b), and offenses relating to social-security-number misuse in violation of 42 U.S.C. § 408(a)(7)(B) and 18 U.S.C. § 371, was ample.

We are unpersuaded by Cuomo's contention that a different result is required by the Supreme Court's recent decision in Dubin v. United States, 599 U.S. 110, 143 S. Ct. 1557, 216 L. Ed. 2d 136 (2023). Dubin involved an aggravated-identity-theft prosecution premised on the defendant's "'us[ing]' a patient's means of identification 'in relation to' healthcare fraud," a federal offense under 18 U.S.C. § 1347. Dubin, 599 U.S. at 116-17. The fraud, however, was that the defendant claimed Medicaid reimbursement for psychological testing by a licensed psychologist when the employee who actually performed the testing was only a licensed psychological associate.

The Supreme Court held that this fraud was not a proper predicate for aggravated identity theft under § 1028A(a)(1) because the

> use of the patient's **[**28]** name was not at the crux of what made the underlying overbilling fraudulent. The crux of the healthcare fraud was a misrepresentation about the qualifications of [defendant's] employee. The patient's name was an ancillary feature of the billing method employed.

599 U.S. at 132. HN8[] "[W]ith fraud or deceit crimes like the one in this case, the *means of identification* specifically must be *used in a manner that* is **[*369]** fraudulent or deceptive." Id. at 131-32 (emphases added).

This interpretation of 18 U.S.C. § 1028A(a)(1) and its appropriate felony predicates affords no relief for Cuomo, whose use of the social security numbers of debtors was both fraudulent and deceptive: As "cooperating witnesses . . . testified[,] . . . the entire process was about impersonating debtors," and "was done so that the states would falsely recognize Paymerica employees as the target debtors and provide [to Paymerica] restricted POE information meant only for those debtors," D.Ct. Op. at 6-7.

In sum, Cuomo's contentions provide no basis for setting aside the jury's verdicts.

III. SENTENCING CHALLENGES

As indicated in Part I.B. above, Cuomo's sentence to 45 months' imprisonment included 21 months for the computer-related and social-security-number-misuse counts. In calculating **[**29]** the Guidelines-recommended sentences for these offenses, the district court adopted the fact descriptions and recommendations of the presentence report ("PSR") for several increases in his Guidelines offense level. (*See* Sentencing Transcript, August 11, 2022 ("S.Tr."), at 3.) Cuomo's base offense level was 6. His total offense level was 16, resulting from (A) three enhancements for specific offense characteristics, *i.e.*, (1) two steps under § 2B1.1(b)(2)(A)(i) because the offense involved 10 or more victims, (2) two steps under § 2B1.1(b)(10)(C) because it involved sophisticated means, and (3) two steps under § 2B1.1(b)(18) because it involved an intent to obtain personal information, and (B) a four-step upward adjustment under § 3B1.1(a) because of his leadership role in the criminal activity. On appeal, Cuomo challenges the increases with respect to personal information and leadership role.

HN9[] We review the "reasonableness of sentencing decisions for abuse of discretion, a standard incorporat[ing] *de novo* review of questions of law, including . . . interpretation of the Guidelines, and clear error review of questions of fact." United States v. Taylor, 961 F.3d 68, 74 (2d Cir. 2020) (internal quotation marks omitted).

A. *Cuomo's Role*

HN10[] The Guidelines recommend a four-step increase in offense level for **[**30]** a "defendant [who] was an organizer or leader of a criminal activity that involved five or more participants," Guidelines § 3B1.1(a)--including the defendant, *see, e.g., UNITED STATES v. PACCIONE, 202 F.3d 622, 625 (2d Cir.)* ("Paccione"), *cert. denied*, *530 U.S. 1221, 120 S. Ct. 2232, 147 L. Ed. 2d 261 (2000)*. "Whether a defendant is considered a leader depends upon the degree of discretion exercised by him, the nature and degree of his participation in planning or organizing the offense, and the degree of control and authority exercised over the other members of the conspiracy." United States v. Beaulieau, 959 F.2d 375, 379-80 (2d Cir. 1992). A defendant may be a leader of a crime even if it was planned, financed, and orchestrated by another participant. *See, e.g.,* United States v. Williams, 23 F.3d 629, 635 (2d Cir.), *cert. denied*, *513 U.S. 1045, 115 S. Ct. 641, 130 L. Ed. 2d 547 (1994)*.

HN11[] We review the district court's conclusion that a defendant met the criteria for "a leadership enhancement under U.S.S.G. § 3B1.1(a) *de novo*, but review the court's findings of fact supporting its conclusion for clear error." *See, e.g., Paccione, 202 F.3d at 624*. Sentencing judges are "given latitude concerning their supervisory role findings, even when their findings were not as precise as they might have been," United States v. Napoli, 179 F.3d 1, 14 (2d Cir. 1999) ("Napoli") (internal quotation **[*370]** marks omitted), *cert. denied*, *528 U.S. 1162, 120 S. Ct. 1176, 145 L. Ed. 2d 1084 (2000)*, so long as their findings are sufficient to permit meaningful appellate review, *see,*

e.g., United States v. Ware, 577 F.3d 442, 451-52 (2d Cir. 2009), *cert. denied*, 562 U.S. 995, 131 S. Ct. 432, 178 L. Ed. 2d 344 (2010).

The district court, in addressing Cuomo's role, stated as follows:

> I've **[**31]** looked at the nature and scope of the illegal activity, the degree with which this defendant oversaw this illegal conspiracy. And I find that based upon the fact that *this defendant incorporated and was president of Ameripay*; that *this defendant established the account with TLO* which allowed him to get information about debtors and that *this defendant used both Ameripay and Paymerica to get the identity of debtors*; also that *he managed co-conspirators* . . .; that *his employees characterize this defendant as a manager when Mr. Trowbridge was not present*; . . . [and] *this defendant was very involved with a number of these supposed debtors*.

(Sentencing Tr. 6-7 (emphases added).)

Cuomo challenges the sufficiency of the court's findings, stating principally that the TLO account was a "legitimate business expense for anyone involved in pursuing judgment debtors," that "[t]he employees were not Cuomo's employees," and that "[t]here were no 'supposed debtors' in this case. Ameripay pursued debtors who had *court judgments* against them." (Cuomo brief on appeal at 42 (emphasis in original).) He also argues that the district court ignored "ample evidence that Trowbridge was the sole manager and **[**32]** leader." (*Id.*) These arguments are wide of the mark.

The test for reviewing the court's findings is not whether there were legitimate aspects of the business of Ameripay and Paymerica, or whether the individuals who did most of the skip-tracing were employees of Cuomo personally, rather than of the company he incorporated and its affiliate, or even whether there was evidence from which the court could have ruled differently. ***HN12***[↑] Rather, the "sentencing court's findings as to the defendant's role in the offense will be overturned only if they are clearly erroneous." Napoli, 179 F.3d at 15 (internal quotation marks omitted). And "[w]here there are two permissible views of the evidence, the factfinder's choice between them cannot be clearly erroneous." Anderson v. City of Bessemer City, 470 U.S. 564, 574, 105 S. Ct. 1504, 84 L. Ed. 2d 518 (1985).

The district court's findings that Cuomo was Ameripay's founder and president and that he managed other coconspirators are supported by testimony and documents in the trial record. Ameripay's corporate documents showed Cuomo as its founder and president. Multiple witnesses who worked at Paymerica also testified that Cuomo was "second in command" to Trowbridge (*e.g.*, Tr. 354, 389), and that Cuomo supervised the skiptracers (*id.* at 460), "audited" their time and attendance **[**33]** (*id.* at 559) and the quality of their performance (*id.* at 463), and reported to Trowbridge on their productivity or on their "goofing off" (*id.* at 433). As summarized in the PSR, whose factual descriptions the sentencing judge expressly adopted, Paymerica employees characterized Cuomo as being in charge when Trowbridge was not present, and Trowbridge traveled "a lot."

We see no clear error in the sentencing court's findings as to Cuomo's leadership role in the conspiracy, which demonstrate that Cuomo was intimately involved in organizing and planning the conspiracy and that he exercised direct authority over most of his coconspirators. We thus affirm **[*371]** the imposition of the four-step enhancement based on Cuomo's leadership role.

B. *Personal Information*

HN13[↑] The Guidelines recommend a two-step increase in offense level if "the defendant was convicted of an offense under 18 U.S.C. § 1030, and the offense involved an intent to obtain personal information." Guidelines § 2B1.1(b)(18)(A). "'Personal information'" is defined to

> mean[] sensitive or private information involving an identifiable individual (including such information in the possession of a third party), *including* (A) medical records; (B) wills; (C) diaries; (D) private correspondence, including e-mail; (E) financial **[**34]** records; (F) photographs of a sensitive or private nature; or (G) similar information.

Guidelines § 2B1.1, Application Note 1 (emphasis added).

Cuomo contends that "[t]his enhancement is inapplicable" because "places of employment are not listed in the definition." (Cuomo brief on appeal at 44.) But we need not reach this issue. ***HN14***[↑] "An error in Guidelines calculation is harmless if correcting the error would result in no change to the Guidelines offense level and sentencing range." *United States v. Cramer, 777 F.3d 597, 603 (2d Cir. 2015)*. The Guidelines provide that appropriate offense-characteristic enhancements are to be applied before the application of adjustments on account of the defendant's role, *see Guidelines § 1B1.1(a)*; and without the personal-information enhancement, the two-step increases for each of the other two offense-characteristic enhancements (number of victims and sophisticated means) would have increased Cuomo's offense level from 6 to level 10. However, the guideline establishing the sophisticated-means enhancement--whose applicability Cuomo does not challenge on appeal--(*see* Government brief on appeal at 75; Cuomo reply brief on appeal at 21)--while initially providing for a two-step enhancement, dictates that "[i]f the resulting offense level is less than level 12, *increase **[**35]** to level 12*," *see Guidelines § 2B1.1(b)(10)(C)* (emphasis added). Accordingly, even if Cuomo's challenge to the application of the personal-information enhancement were successful, the sophisticated-means enhancement would increase his enhanced offense level to level 12. The four-step adjustment for his leadership role increases his offense level to level 16, leaving his total offense level and sentencing range unchanged.

CONCLUSION

We have considered all of Cuomo's contentions on this appeal and have found them to be without merit. The judgment of the district court is affirmed.

End of Document

UNITED STATES COURT OF APPEALS
FOR THE
SECOND CIRCUIT

At a Stated Term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 6th day of March, two thousand twenty-five,

Before: Amalya L. Kearse,
Michael H. Park,
Myrna Pérez,
Circuit Judges.

United States of America,

Appellee,

v.

Guy Cuomo, AKA John Monaco,

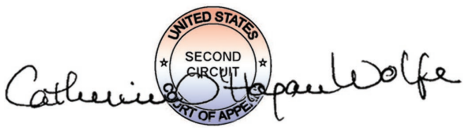
Defendant - Appellant.

ORDER
Docket No. 22-1799

Appellant having filed a petition for panel rehearing and the panel that determined the appeal having considered the request,

IT IS HEREBY ORDERED that the petition is DENIED.

For The Court:
Catherine O'Hagan Wolfe,
Clerk of Court



MANDATE

UNITED STATES COURT OF APPEALS
FOR THE
SECOND CIRCUIT

At a Stated Term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 3rd day of January, two thousand twenty-five.

Before: Amalya L. Kearse,
Michael H. Park,
Myrna Pérez,
Circuit Judges.

United States of America,

Appellee,

v.

Guy Cuomo, a.k.a. John Monaco,

Defendant - Appellant.

JUDGMENT

Docket No. 22-1799

The appeal in the above captioned case from a judgment of the United States District Court for the Northern District of New York was argued on the district court's record and the parties' briefs.

IT IS HEREBY ORDERED, ADJUDGED and DECREED that judgment of the district court is AFFIRMED.

For the Court:
Catherine O'Hagan Wolfe,
Clerk of Court

A True Copy
Catherine O'Hagan Wolfe, Clerk
United States Court of Appeals, Second Circuit

MANDATE ISSUED ON 03/13/2025