UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

MATTHEW WEISS,

Defendant.
_____/

Case No: 25-20165

Honorable Nancy G. Edmunds

OPINION AND ORDER DENYING DEFENDANT'S MOTION TO DISMISS COUNTS 11-20 OF THE INDICTMENT [20]

Before the Court is Defendant Matthew Weiss's Motion to Dismiss Counts 11-20 of the Indictment. (ECF No. 20.) The motion argues that the government has improperly charged Defendant with aggravated identity theft under 18 U.S.C. § 1028A(a)(1). Defendant relies on the Supreme Court's recent decision in *Dubin v. United States*, 599 U.S. 110 (2023), which offers a narrower interpretation of § 1028A(a)(1) than some courts have taken in the past. In opposition, the government contends that the indictment describes a set of facts that amount to a violation of § 1028A(a)(1), even after the Supreme Court's clarification in *Dubin*. Because the allegations fall within the scope of the statute's text and pass the test articulated in *Dubin*, the Court DENIES the motion to dismiss.

I. Background

The indictment alleges as follows.[1] From about 2015 to January 2023, Defendant Matthew Weiss accessed the "social media, email, and/or cloud storage accounts" of more than 3,300 users—primarily female college athletes—without the users' authorization. (ECF No. 1, ¶¶1-2.) Defendant obtained access to student-athlete databases maintained by third party Keffer Development Services ("KDS") by "compromising the passwords of accounts with elevated levels of access, such as the accounts of trainers and athletic directors." (*Id.* ¶6.) After accessing the databases, Defendant downloaded various information contained therein, including passwords that student athletes used to access KDS's systems. (*Id.* ¶¶7-8.) He then conducted additional research on certain student athletes to learn other personal details about them, "such as their mothers' maiden names, pets, dates of birth, and nicknames." (*Id.* ¶9.) Using the information from the student-athlete databases and his independent research, Defendant guessed or reset the passwords of over 2,000 targeted athletes' social media, email, and cloud storage accounts, allowing him to access these accounts. (*Id.* ¶10.) He also gained access to social media, email, and cloud storage accounts of "1,300 additional students and/or alumni from colleges around the country," in at least several cases by exploiting vulnerabilities in account authentication processes. (*Id.*, ¶¶12, 14.) Defendant used his access to the over 3,300 total accounts to view and download personal or intimate photographs and videos stored in the accounts. (*Id.* ¶¶11, 13.)

[1] When considering a motion to dismiss, the Court treats the factual allegations in the indictment as true and does not test the evidence supporting the government's claims. *E.g.*, *United States v. Palma*, 58 F.4th 246, 250 (6th Cir. 2023). The reader is reminded, however, that the allegations in the indictment have not been proven, and Defendant will be presumed innocent unless and until the government proves otherwise.

The government filed an indictment in March 2025. Relevant to this motion, counts 1-10 of the indictment allege that Defendant obtained access to the social media, email, and cloud storage accounts of 10 Jane Does "without and in excess of authorization," in violation of 18 U.S.C. §1030(a)(2)(C) and (c)(2)(B)(ii). (*Id.* ¶¶15-17.) Counts 11-20 allege that Defendant committed aggravated identity theft under 18 U.S.C. § 1028A(a)(1) by transferring, possessing, and using the "means of identification" of another person—a "unique identifier" or "login identifier" for each of the 10 Jane Does' accounts—"during and in relation to" the violations alleged in counts 1-10. (*Id.*¶¶18-20.)

Defendant moved to dismiss counts 11-20 of the indictment. (ECF No. 20.) The government responded (ECF No. 23), and Defendant replied (ECF No. 27).

II. Standard of Review

A defendant may move under Federal Rule of Criminal Procedure 12(b)(3)(B)(v) to dismiss an indictment that "fail[s] to state an offense." "An indictment does not state an offense adequately unless it alleges each element of the offense, 'fairly informs a defendant of the charge against which he must defend,' and 'enables him to plead an acquittal or conviction in bar of future prosecutions for the same offense.'" *United States v. Hall*, 261 F. Supp. 3d 812, 815 (E.D. Mich. 2017) (quoting *United States v. Anderson*, 605 F.3d 404, 411 (6th Cir. 2010)). "When assessing the sufficiency of the charge, the examination focuses on the indictment itself, and not on the underlying evidence of the crime." *Id.* (citing *United States v. Landham*, 251 F.3d 1072, 1080 (6th Cir. 2001)).

III. Analysis

Counts 11-20 of the indictment charge Defendant with aggravated identity theft under 18 U.S.C. § 1028A(a)(1). The statute provides:

> Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or 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.

Id. To summarize, the statute acts as a sentence enhancer for a felony enumerated in § 1028A(c) when a defendant (1) "knowingly transfers, possesses, or uses," (2) a "means of identification of another person," (3) "without lawful authority," (4) "in relation to" the predicate felony. *Id.* The enumerated predicate felonies include "any provision contained in this chapter," including § 1030. *See id.* § 1028A(c)(4).

The predicate felonies, counts 1-10, allege unauthorized computer access in violation of the Computer Fraud and Abuse Act ("CFAA"). In relevant part, the CFAA prohibits "intentionally accesse[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." *Id.* § 1030(a)(2)(C). A "protected computer" includes any computer "used in or affecting interstate or foreign commerce or communication," *id.*, § 1030(e)(2)(B), including "all computers that connect to the Internet." *Van Buren v. United States*, 593 U.S. 374, 379 (2021). A website server is a "protected computer" for the purpose of the CFAA. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1195 (9th Cir. 2022).

The motion does not dispute that the indictment adequately alleges predicate violations of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(ii). Defendant also does not meaningfully dispute that the Jane Does' login credentials were a "means of identification of another person" for the purpose of the identity-theft statute. *See United States v. Barrington*, 648 F.3d 1178, 1193 (11th Cir. 2011) (holding that "usernames and passwords, considered together, constituted a 'means of identification'" for the purpose

of § 1028A). The primary disagreement is whether Defendant "use[d]" the digital identifiers of his alleged victims "in relation to" the alleged crime of accessing their accounts without authorization for the purpose of § 1028A(a)(1).[2]

In *Dubin*, the Supreme Court considered what it means to "use" a "means of identification… in relation to" an underlying crime. The defendant in that case, David Dubin, was charged with aggravated identity theft after the company he helped to manage submitted a Medicaid claim that overstated the qualifications of the service provider and listed an incorrect date of service. *Dubin*, 599 U.S. at 114. The government argued that a defendant "use[s]" a "means of identification" for the purpose of § 1028A(a)(1) whenever the means of identification "facilitates or furthers the predicate offense in some way." *Id.* at 117. On this reading, the defendant "use[d]" the patient's identity to commit the underlying billing-fraud offense because the patient's Medicaid reimbursement number was included on the fraudulent claim. *Id.* at 115.

The Court declined to adopt this broad interpretation of the statute, instead ruling that "[a] defendant 'uses' another person's means of identification 'in relation to' a predicate offense when this use is at the crux of what makes the conduct criminal." *Id.* at 131. Under this test, there must be "more than a causal relationship" between the use of another person's identity and the underlying offense. *Id.* The use of the identity must be "at the locus of the criminal undertaking" rather than "passive, passing, or ancillary." *Id.* at 123 (cleaned up). And, at least for predicate crimes involving fraud or deceit, "the means of identification specifically must be used in a manner that is fraudulent or

[2] While the statute also criminalizes "possess[ion]" and "transfer[]" of the means of identification of another in relation to a predicate felony, the parties' arguments (and the cases they cite) focus on the "use[]" prong of the statute.

deceptive." *Id.* at 131-32. The defendant's conduct did not satisfy this test because the "crux" of the underlying fraud was a misrepresentation about an employee's qualifications; the use of the patient's identity in the bill was merely an "ancillary feature" of the crime. *Id.* at 132.

In explaining this standard, the Supreme Court repeatedly cited a heuristic developed by the Sixth Circuit: a defendant "use[s]" a means of identification "in relation" to a billing-fraud crime by "misrepresenting *how* and *when* services were provided to a patient, not *who* received the services." *Id.* at 132; *see United States v. Michael*, 882 F.3d 624, 628-29 (6th Cir. 2018); *United States v. Medlock*, 792 F.3d 700, 707 (6th Cir. 2015). The Sixth Circuit employed this heuristic in *Medlock*, where the defendants falsely claimed that they used stretchers while transporting patients in ambulances to obtain reimbursements from Medicaid. 792 F.3d at 703. The false claims about the stretchers did not amount to identity theft under § 1028A because the defendants "misrepresented *how and why* the beneficiaries were transported, but they did not use those beneficiaries' identities to do so." *Id.* at 707. In *Michael*, on the other hand, the defendant was a pharmacist who allegedly used a doctor and a patient's identifying information "to request reimbursement for a drug the doctor never prescribed and the patient never requested." 882 F.3d at 625. Taking the alleged facts as true, the pharmacist committed aggravated identity theft because misrepresenting who received and who prescribed the medications was "integral" to the predicate felony of healthcare fraud. *Id.* at 629.

The Sixth Circuit recently applied the *Dubin* test in *United States v. O'Lear*, 90 F.4th 519 (6th Cir.), *cert. denied*, 144 S. Ct. 2542 (2024). There, the defendant appealed a conviction for identity theft where the government "alleged that [the defendant] forged

the signatures of a physician and an x-ray technician to make it appear as if these individuals had ordered or conducted the x-rays he billed for." *Id.* at 533. The Sixth Circuit upheld the conviction under *Dubin* because the defendant "used the identities of these professionals in a 'deceptive' way that went to the 'crux' of his scheme to bill for fictitious x-rays." *Id.* (quoting *Dubin*, 599 U.S. at 132). Put another way, the case was different from *Dubin* because the defendant misrepresented *who* ordered and performed the healthcare services, not *what* they were or *when* they were performed.

The government likens this case to *Michael* and *O'Lear*. In both cases, the defendants' uses of third parties' identities were central to committing the underlying billing fraud. In the same way here, the government argues, Defendant's alleged use of victims' usernames and passwords is central to the underlying computer crime. In each of the 10 instances of computer hacking, "a *specific* victim's username and password was necessary to access *that victim's* account and thereby *that victim['s]* personal images." (ECF No. 23, PageID.91.) Thus, "[e]ach victim's means of identification is at the crux of each corresponding count of 18 U.S.C. § 1028A(a)(1)." (*Id.*)

The Court agrees that Defendant's alleged use of victims' identifying information is at the crux of what makes the underlying CFAA violations criminal. *See Dubin*, 599 U.S. at 131. The gist of the charged predicate felony is that Defendant accessed online accounts without permission by obtaining or resetting login credentials, allowing him to essentially impersonate authorized users. This misrepresentation of his digital identity was not merely an "ancillary feature" of the predicate felony, *see id.* at 132, but central to the alleged unauthorized computer access. To borrow the heuristic used in *Dubin*, Defendant accessed the accounts without permission by misrepresenting "*who*" was

logging in, not just "*how* or *when*" he was doing it. *See id.* Accordingly, the indictment sufficiently alleges that Defendant violated § 1028A.

Defendant makes several arguments to the contrary, but none of them establish that the indictment fails to state an offense.

First, Defendant argues that his alleged use of victims' login credentials was "merely an ancillary feature" of the underlying crime because it merely facilitated a separate act of unauthorized computer access. (ECF No. 20, PageID.70 (quoting *Dubin*, 599 U.S. at 114).) Defendant points out that the Sixth Circuit has described violations of § 1030(a)(2) as "digital trespassing." (*Id.* (quoting *Abu v. Dickson*, 107 F.4th 508, 514 (6th Cir. 2024).) So, just as a criminal commits a physical trespass by entering a building unlawfully, not by opening the door, Defendant argues that his alleged unauthorized computer access was complete when he accessed the victims' accounts, not when he entered their passwords. As Defendant puts it:

> Means of identification are not at the crux of criminality of a trespass crime because they merely act as a virtual key that help make the subsequent criminal act possible. The hacker who enters a username and password without permission is like the physical trespasser who inserts a stolen key into a lock protecting a business. Turning the key in the lock, or pressing "enter" on the keyboard, can cause the security door to unlock and remove the technical barrier to entry. With the barriers to entry removed, the crime is enabled. The trespasser can then take the step at the crux of the crime and actually enter the place where he is not supposed to be present.

(*Id.* at PageID.70-71.) Defendant thus distinguishes this case from *O'Lear* because the underlying medical fraud and identity theft in that case were accomplished through the same act—submitting fraudulent claims using falsified signatures—whereas in this case, "unlock[ing] virtual doors" was an act that "allowed a later virtual trespass." (*Id.* at PageID.73.)

The assumption underlying this argument appears to be that identity theft is only at the "crux" of the predicate felony when the identity theft and the predicate crime are completed simultaneously or through the same act. Thus, Defendant argues that the alleged identity theft (logging into a web account with another's credentials) is not at the crux of the underlying crime (accessing and obtaining information from the account) because logging in was only a preliminary step to accessing the information, in the same way that turning a key is a precursor to perfecting a trespass by entering a building. But while *Dubin* requires that identity theft "play[] a key role" in the underlying offense, 599 U.S. at 129, it does not say that both the identity theft and the underlying offense must be completed at the exact same moment. Indeed, the only temporal requirement that the statute imposes is that the "means of identification" must be used "during" the predicate crime. 18 U.S.C. § 1028A(a)(1). A jury could reasonably find that Defendant used the Jane Does' login credentials "during" the process of accessing their accounts. Depending on the structure of the websites at issue, the entry of the passwords and the unauthorized access to private information may have occurred at the same time or merely seconds apart from each other. In any case, the indictment states an offense, notwithstanding that entering another user's password without permission might be construed as a preliminary step to accessing the data protected by that password.

Second, and relatedly, Defendant likens using a stolen password to a stolen key; while a "physical key is a unique means of identification that only the homeowner is supposed to have," "inserting the key and unlocking the door does not steal the homeowner's identity." (ECF No. 20, PageID.67-68.) While this argument has some intuitive appeal, it is inconsistent with the statutory text. For the purpose of § 1028A, a

"means of identification" includes "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual . . . ." 18 U.S.C. § 1028(d)(7). A username or password fits this definition because it is a specific electronic identifier—a "name or number"—assigned to a specific individual. *See Barrington*, 648 F.3d at 1193. A physical house key, meanwhile, is not a "name or number," and it does not necessarily "identify a specific individual." 18 U.S.C. § 1028(d)(7). The fact that using a house key is not identity theft only reflects that the statute was not written to cover house keys—it does not show that using another person's login credentials without permission cannot be part of an identity-theft crime.

Third, Defendant asserts that "[u]nder *Dubin*, the 'means of identification' must be 'used deceptively.'" (ECF No. 20, PageID.67 (quoting *Dubin*, 599 U.S. at 123).) Thus, he argues, "[n]o one could have been deceived" by Defendant's use of other peoples' login credentials because "[n]o person saw the login identifiers or made a decision based on their entry." (*Id.*) In other words, Defendant suggests that he cannot be liable because no natural person was deceived. But the text of § 1028A does not require that a human being be deceived. And, as the government points out, healthcare fraud cases involving identity theft—including *Michael* and *O'Lear*, discussed above—"have not found it necessary to determine whether reimbursements were automated or if there was a 'human in the loop.'" (ECF No. 23, PageID.92.) Requiring a human being to be deceived would add an element to the statute that does not exist and could preclude convictions for identity theft accomplished through electronic means, such as using another person's credit card on an ecommerce website or applying for government benefits online using another person's social security number. It would also be strange for Congress to make unauthorized

computer access a predicate offense to aggravated identity theft if it had intended to limit the identity-theft statute to cases where a human being was deceived. Insofar as the government must prove that Defendant used the identities of the Jane Does deceptively, it could do so by showing that Defendant misrepresented who he was when he logged into the Jane Does' accounts using their login credentials.

Fourth, Defendant invokes the *Dubin* Court's concerns that an overbroad interpretation of § 1028A would cover "generic" or "garden-variety" violations of predicate crimes. In context, the "generic" or "garden-variety" crimes the Supreme Court described were acts that, while technically fraudulent, did not involve identity theft as a central feature. *Dubin*, 599 U.S. at 122, 129. The Court was concerned that if § 1028A was triggered whenever a person's name was included on a bill that misstated the goods or services provided—for instance, a legal invoice containing a client's name that rounded up the lawyer's hours from 2.9 to 3, or a restaurant bill that misstated which cut of meat was served—then the statute could be read to cover relatively minor crimes that "do not sound like identity theft." *Id.* at 123. The Supreme Court addressed this concern by adopting a narrower reading that did not capture such "generic" offenses and instead "targets situations where the means of identification itself plays a key role." *Id.* at 129. For reasons already discussed, the "means of identification" of digital accountholders played a "key role" in the offenses charged here when Defendant allegedly used them to gain unauthorized access to users' accounts. The crimes alleged are not the kind of "generic," "garden-variety," non-identity-theft crimes that the Supreme Court was concerned about.

Fifth, Defendant points to legislative history which, in his view, suggests that "Congress has never considered the possibility that entering a username and password

to enable access to another's account is itself aggravated identity theft." (ECF No. 20, PageID.74.) The Court cannot consider legislative history where the text of a statute is clear. *United States v. Banyan*, 933 F.3d 548, 553 (6th Cir. 2019). "[E]xtrinsic materials like legislative history have a role in statutory interpretation only to the extent they shed a reliable light on the enacting Legislature's understanding of *otherwise ambiguous terms*." *Id.* (quoting *Exxon Mobil Corp. v. Allapattah Servs., Inc.*, 545 U.S. 546, 568 (2005)) (emphasis added in *Banyan*) (internal quotation marks omitted). To the extent that § 1028A was ever ambiguous, the Supreme Court resolved the ambiguity when it provided a test for what constitutes "use" of another's identity "in relation to" another crime in *Dubin*.

Sixth, and finally, Defendant contends that combining § 1028A with a violation of § 1030 as a predicate offense is a "novel" charging strategy that converts an offense usually punished with probation into one with a two-year, mandatory-minimum sentence, creating a maximum penalty of 20 years for the 10 counts of aggravated identity theft charged in the indictment. (ECF No. 20, PageID.62-63.) The government disputes that this charging strategy is novel. (ECF No. 23, PageID.95-97.) But even if it is, the novelty of the charging strategy is ultimately irrelevant at this stage. The only question at this point is whether the allegations in the indictment, taken as true, amount to violations of the offenses charged. For the reasons discussed above, they do.

IV. Conclusion

For the foregoing reasons, the Court DENIES the motion to dismiss counts 11-20 of the indictment (ECF No. 20).

SO ORDERED.

s/ Nancy G. Edmunds
Nancy G. Edmunds
United States District Judge

Dated: December 22, 2025

I hereby certify that a copy of the foregoing document was served upon counsel of record on December 22, 2025, by electronic and/or ordinary mail.

s/ Marlena Williams
Case Manager