UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

PAIGE A. THOMPSON,

Defendant.

Case No. CR19-159RSL

ORDER DENYING MOTION TO DISMISS COUNTS 2 THROUGH 8

This matter comes before the Court on defendant Paige Thompson's "Motion to Dismiss Counts 2 through 8 of the Second Superseding Indictment" (Dkt. # 123).[1] Defendant faces an upcoming trial for charges of wire fraud, violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), access device fraud, and aggravated identity theft. Dkt. # 166. She contends that Counts 2 through 8 of the indictment, which allege violations of the Computer Fraud and Abuse Act (CFAA), must be dismissed for failure to state a claim. Dkt. # 123 at 1. Defendant also moves to dismiss these counts because, as alleged, they violate her Fifth Amendment right to due process and First Amendment right to free speech and expression. *Id.*

[1] The government introduced a Second Superseding Indictment (Dkt. # 166) after briefing for this motion was submitted. Because the Second Superseding Indictment does not substantively modify Counts 2 through 8, the Court reads the arguments in the present motion as applying equally to both versions of the Superseding Indictment and applies this ruling to the Second Superseding Indictment.

I. Motions to File Overlength Response and Reply

As a threshold matter, the Court grants the government's motion to file an overlength response (Dkt. # 134). The government may file a thirteen-page response. The Court also grants defendant's motion to file an overlength reply (Dkt # 159). Defendant may file a ten-page reply.

II. Counts 2 Through 8: Failure to State a Claim

Defendant argues that Counts 2 through 8 of the Indictment must be dismissed because they fail to allege criminal activity. Dkt. # 123 at 1; Fed. R. Crim. P. 12(b)(3)(B)(v). At this motion to dismiss stage, "the issue in judging the sufficiency of the indictment is whether the indictment adequately alleges the elements of the offense and fairly informs the defendant of the charge, not whether the Government can prove its case." *United States v. Buckley*, 689 F.2d 893, 897 (9th Cir. 1982). On a motion under Federal Rule of Criminal Procedure 12, the failure to allege facts that, if proven, would satisfy an essential element of the offense is a fatal defect requiring dismissal of the indictment. *See United States v. Omer*, 395 F.3d 1087, 1089 (9th Cir. 2005). However, "[t]he Government need not allege its theory of the case or supporting evidence, but only the 'essential facts necessary to apprise a defendant of the crime charged.'" *Id.* (quoting *United States v. Markee*, 425 F.2d 1043, 1047-48 (9th Cir. 1970)). An indictment need not explain all factual evidence to be proved at trial. *United States v. Blinder*, 10 F.3d 1468, 1476 (9th Cir. 1993).

In evaluating a motion to dismiss, the Court accepts the allegations in the indictment as true and is "bound by the four corners of the indictment." *United States v. Boren*, 278 F.3d 911, 914 (9th Cir. 2002). The indictment must be "construed according to common sense, and interpreted to include facts which are necessarily implied." *United States v. Berger*, 473 F.3d 1080, 1103 (9th Cir. 2007) (internal quotation marks and citation omitted). A Rule 12(b)(3)(B) motion is "capable of determination before trial if it involves questions of law rather than fact" and therefore does not intrude upon "the province of the ultimate finder of fact." *United States v. Kelly*, 874 F.3d 1037, 1046-47 (9th Cir. 2017) (quotations omitted).

Here, Counts 2 through 7 charge defendant with violating § 1030(a)(2) of the CFAA. This section prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" and "thereby obtain[ing] . . . information contained in a financial record of a financial institution" or "information from any protected computer." 18 U.S.C. § 1030(a)(2)(A), (C). Count 8 charges defendant with violating § 1030(a)(5)(A), which prohibits causing "the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). Both statutory sections include the element that defendant acted "without authorization."

The indictment alleges that defendant created proxy scanners that allowed her to identify Amazon Web Services (AWS) servers with misconfigured web application firewalls that permitted outside commands to reach and be executed by the servers. Dkt # 166 at ¶ 12. Defendant then sent commands to the misconfigured servers to obtain security credentials for particular accounts or roles belonging to the victims. *Id.* at ¶¶ 11-13, 16-18. Defendant then used these "stolen credentials" to "copy data, from folders or buckets of data" in the victims' cloud storage space and set up cryptocurrency mining operations on the victims' rented servers. *Id.* at ¶¶ 14-15, 21. The indictment further alleges that defendant concealed her location and identity while executing these actions by using VPNs and TOR.[2] *Id.* at ¶¶ 17-18.

Defendant contends that the indictment fails to allege an offense because the government, under the facts alleged, cannot prove that defendant accessed a computer "without authorization.".[3] Dkt. # 123 at 1. In particular, defendant argues that because the victim servers

[2] VPNs (virtual private networks) and TOR (The Onion Router) are both technologies that facilitate online privacy and can be used to conceal a user's identity and/or location.

[3] Counts 2 through 7 are charged under CFAA subsection (a)(2), which requires "intentionally *access[ing] a computer* without authorization." 18 U.S.C. § 1030(a)(2). In contrast, Count 8 is charged under CFAA subsection (a)(5)(A), which requires "intentionally *caus[ing] damage* without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). The Court is cognizant of the need for congruence among these subsections. *See Nosal II*, 844 F.3d at 1033. However, to the extent that defendant's arguments are focused on whether she allegedly *accessed a computer* without authorization,

were misconfigured in such a way that they automatically provided her with credentials in response to certain legitimate commands that she sent, she had received "authorization." Dkt. # 123 at 6. The government, relying on tenets of trespass law,[4] argues the computer system disclosed the credentials by "mistake, not authorization," given defendant misrepresented herself as an authorized user. Dkt. # 135 at 6 (citing to Restatement (Second) of Torts §§ 173-74 (Am. L. Inst. 1977) (explaining that consent is not a valid defense to trespass when consent is obtained by fraud, misrepresentation, or mistake)).

"Without authorization" is not defined in the CFAA. The Ninth Circuit has explained that "'without authorization' is an unambiguous, non-technical term [to be] given its plain and ordinary meaning," *United States v. Nosal (Nosal II)*, 844 F.3d 1024, 1028 (9th Cir. 2016), and has held that "a person is 'without authorization' under the CFAA 'when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission).'" *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016) (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009)). In its only opinion interpreting the CFAA, the Supreme Court explained that the "without authorization" clause "protects computers themselves by targeting so-called outside hackers – those who 'access a computer without any permission at all.'" *Van Buren v. United States*, 141 S. Ct. 1648 (2021) (quoting *Brekka*, 581 F.3d at 1133). The Supreme Court explained that liability "stems from a gates-up-or-down inquiry – one either can or cannot access a computer system." *Id.*

the Court notes that these arguments are not applicable to Count 8, which requires different elements than Counts 2-7.

[4] Notably, the Supreme Court's *Van Buren* decision counseled against reliance on common law principles when interpreting the CFAA. *See* 141 S. Ct. at 1655 n.4 (explaining that "common-law principles 'should be imported into statutory text only when Congress employs a common-law term'—not when Congress has outlined an offense 'analogous to a common-law crime without using common-law terms'" (quoting *Carter v. United States*, 530 U.S. 225, 265 (2000)). In this case, the Court need not resort to trespass law to parse an answer – prior cases interpreting the CFAA provide support for upholding the indictment.

Under this standard, the indictment here adequately states an offense. To reach this conclusion, the Court addresses each of defendant's three main arguments: (1) that authorization was granted to her by the misconfigured servers; (2) that she did not use another person's password; and (3) that she merely accessed publicly available information.

1. Authorization

Turning first to how defendant gained the credentials she used to allegedly copy the data and pursue her cryptomining operation, defendant repeatedly argues that she could not have been an "unauthorized" user because authorization was "automatically granted" to her when the misconfigured servers provided her with the user credentials. Dkt. # 160 at 9. Ultimately, defendant argues, even if authorization was a "mistake," it was "authorization nonetheless." *Id.*

Defendant cites to no case where a user's "authorization" was granted by mistake or by a purely technological process. This argument is undermined by Ninth Circuit precedent, which makes clear that "authorization" is something that only the owner of the computer or similar authority can provide. *See Nosal II*, 844 F.3d at 1028 (explaining that "'without authorization' . . . means accessing a protected computer without permission"); *Brekka*, 581 F.3d at 1133 (defining "authorization" as "permission or power granted by an authority"); *Domain Name Comm'n Ltd. v. DomainTools LLC*, 449 F. Supp. 3d 1024, 1027 (W.D. Wash. 2010) (finding "one is authorized to access a computer when the owner of the computer gives permission to use it"). Here, the indictment clearly alleges that the security credentials were "stolen" and that defendant "lacked authority to use the accounts and roles and send the commands." Dkt. # 166 at ¶ 16. The allegation that they were stolen implies that defendant acted without permission from the owner of the computer, and, therefore, without authorization.

Furthermore, prior cases make clear that there is a difference between the technical ability to access a computer and "authorization" to access a computer. For example, in *Brekka* the Ninth Circuit explained that where a former employee's login credentials had not been deactivated after he left the company, there was "no dispute that if [the employee had] accessed [his former employer's] information on the [traffic monitoring] website after he left the company . . . , [the employee] would have accessed a protected computer 'without authorization'

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**