Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

August 28 20 19

WILLIAM M. McCOOL, Clerk

By _____ Deputy

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff

v.

PAIGE A. THOMPSON,

Defendant.

NO. CR19-159 RSL

INDICTMENT

The Grand Jury charges that:

COUNT 1
(Wire Fraud)

1. Beginning in or before March 2019, and continuing until in or after July 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON, with the intent to defraud, devised and intended to devise, a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises.

A. *Background*

2. The "Cloud Computing Company" is a company that provides cloud-computing services to individuals, companies, and governments. Cloud computing is the practice of using a network of remote servers hosted on the Internet, commonly referred to as "the cloud," rather than a local computer or server, to store, manage, and process

data. The Cloud Computing Company provides services through server farms that are located throughout the world and maintained by the Cloud Computing Company.

3. Capital One Financial Corporation ("Capital One") is a bank holding company that offers credit cards and other services to customers throughout the United States. Capital One supports its services, in part, by renting or contracting for computer servers from the Cloud Computing Company. The servers on which Capital One stores credit card application and other information generally are located in states other than the State of Washington, and they store information regarding customers, and support services, in multiple states. Deposits of Capital One are insured by the Federal Deposit Insurance Corporation.

4. Victim 2 is state agency of a state that is not the State of Washington. Victim 2 supports its services, in part, by renting or contracting for computer servers from the Cloud Computing Company.

5. Victim 3 is a telecommunications conglomerate located outside the United States that provides services predominantly to customers in Europe, Asia, Africa, and Oceania. Victim 3 supports its services, in part, by renting or contracting for computer servers from the Cloud Computing Company.

6. Victim 4 is a public research university located outside the State of Washington. Victim 4 supports its services, in part, by renting or contracting for computer servers from the Cloud Computing Company.

B. The Essence of the Scheme and Artifice

7. The object of the scheme was to exploit the fact that certain customers of the Cloud Computing Company had misconfigured web application firewalls on the servers that they rented or contracted from the Cloud Computing Company. The object was to use that misconfiguration in order to obtain credentials for accounts of those customers that had permission to view and copy data stored by the customers on their Cloud Computing Company servers. The object then was to use those stolen credentials in order to access and copy other data stored by the customers on their Cloud Computing

Company servers, including data containing valuable personal identifying information. The object also was to use the access to the customers' servers in other ways for PAIGE A. THOMPSON's own benefit, including by using those servers for "cryptojacking."

C. *The Manner and Means of the Scheme and Artifice*

8. It was part of the scheme and artifice that PAIGE A. THOMPSON used, and created, scanners that allowed her to scan the publicly facing portion of servers rented or contracted by customers from the Cloud Computing Company, and to identify servers for which web application firewall misconfigurations permitted commands sent from outside the servers to reach and be executed by the servers.

9. It was further part of the scheme and artifice that PAIGE A. THOMPSON then transmitted commands to the misconfigured servers that obtained the security credentials for particular accounts or roles belonging to the customers with the misconfigured servers.

10. It was further part of the scheme and artifice that PAIGE A. THOMPSON then used the accounts for which she had obtained security credentials to obtain lists or directories of folders or buckets of data in the Cloud Computing Company customers' storage space at the Cloud Computing Company.

11. It was further part of the scheme and artifice that PAIGE A. THOMPSON used the accounts for which she had obtained security credentials to copy data, from folders or buckets of data in the Cloud Computing Company customers' storage space at the Cloud Computing Company for which the accounts had requisite permissions, to a server that PAIGE A. THOMPSON maintained at her own residence.

12. It was further part of the scheme and artifice that, in taking these steps, PAIGE A. THOMPSON implicitly represented that commands to copy data that she sent using the accounts for which she had obtained security credentials were legitimate commands sent by users with permission to send such commands, rather than commands sent by a person who had stolen the security credentials and who lacked authority to use the accounts and send the commands.

13. It was further part of the scheme and artifice that, in executing the scheme and artifice, PAIGE A. THOMPSON used virtual private networks ("VPNs"), including a VPN offered by the company IPredator, to conceal PAIGE A. THOMPSON's location and identity from the Cloud Computing Company and from victim companies.

14. It was further part of the scheme and artifice that, in executing the scheme and artifice, PAIGE A. THOMPSON used The Onion Router ("TOR") to conceal PAIGE A. THOMPSON's location and identity from the Cloud Computing Company and from victim companies.

15. It was further part of the scheme and artifice that PAIGE A. THOMPSON copied data to her own server from servers rented or contracted by Capital One from the Cloud Computing Company, including data that contained information, including personal identifying information, from approximately 100,000,000 customers who had applied for credit cards from Capital One.

16. It was further part of the scheme and artifice that PAIGE A. THOMPSON copied and stole data from more than 30 different entities, including Capital One, Victim 2, Victim 3, and Victim 4 that had contracted or rented servers from the Cloud Computing Company.

17. It was further part of the scheme and artifice that PAIGE A. THOMPSON used her unauthorized access to certain victim servers – and the stolen computing power of those servers – to "mine" cryptocurrency for her own benefit, a practice often referred to as "cryptojacking." (Cryptocurrency mining is the process by which cryptocurrency transactions are verified and added to the public ledger, *i.e.,* the blockchain. Persons who verify blocks of legitimate transactions, often referred to as "miners," are rewarded with an amount of that cryptocurrency. Successful mining operations consume large amounts of computing power and hardware.)

C. Execution

18. On or about March 22, 2019, at Seattle, in the Western District of Washington, and elsewhere, PAIGE A. THOMPSON, for the purpose of executing the

scheme and artifice described above, caused to be transmitted by means of wire communication in interstate commerce, from her computer in Seattle to a computer outside the State of Washington, writings, signs, signals, pictures, and sounds, that is, a command to copy data belonging to Capital One from servers, rented or contracted by Capital One from the Cloud Computing Company, to a server belonging to PAIGE A. THOMPSON in Seattle.

All in violation of Title 18, United States Code, Section 1343.

COUNT 2
(Computer Fraud and Abuse)

19. The allegations set forth in Paragraphs 1-18 of this Indictment are realleged and incorporated into this Count, as if fully set forth herein.

20. Between on or about March 12, 2019, and on or about July 17, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON intentionally accessed a computer without authorization, to wit, a computer containing information belonging to Capital One Financial Corporation, and thereby obtained information contained in a financial record of a financial institution and of a card issuer as defined in Section 1602 of Title 15, and information from a protected computer, and the value of the information obtained exceeded $5,000.

All in violation of Title 18, United States Code, Section 1030(a)(2)(A) and (C), and (c)(2)(A) and (B)(iii).

ASSET FORFEITURE ALLEGATION
(Count 1)

The allegations contained in Count 1 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c). Upon conviction of the offense charged in Count 1, the defendant, PAIGE A.

DOCKET ALARM

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.