TMS: USAO2024R00576

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA

v.

MATTHEW BATHULA,

Defendant

* **CRIMINAL NO.** SAG 26cr159

* **(Unauthorized Access to Protected Computers, 18 U.S.C. §§ 1030(a)(5)(A), 1030(a)(2)(C); Aggravated Identity Theft, 18 U.S.C. § 1028A; Forfeiture, 18 U.S.C. §§ 982, 1030(i), 21 U.S.C. § 853(p), and 28 U.S.C. § 2461(c))**

****

INDICTMENT

COUNT ONE
(Unauthorized Access to Protected Computers – Company A)

The Grand Jury for the District of Maryland charges that:

At all times relevant to this Indictment:

1. **MATTHEW BATHULA** ("**BATHULA**") was a resident of the State of Maryland.

2. Company A was a medical system located in the District of Maryland. As a medical system, Company A had computer networks and systems that were used in and affecting interstate commerce; therefore, Company A's computers were "protected computers" within the definition of Title 18, United States Code, Section 1030. Company A had a policy of monitoring user devices, and prohibited the insertion of removable media with malicious content to Company A's networks and systems.

3. In or around July 2011, Company A hired **BATHULA** as a Pharmacy Clinical Specialist, a position he held until in or around October 2024.

4. Victim-001 through Victim-195 (collectively, "Victims"), whose identities are known to the Grand Jury, were current or former employees of Company A, a family member,

friend, or relative of a current or former employee of Company A, someone in a relationship with a current or former employee of Company A, or someone otherwise affiliated with Company A.

Relevant Terms

5. "Malware" was malicious computer software intended to cause the victim computer to behave in a manner inconsistent with the intention of the owner or user of the victim computer, often unbeknownst to that owner or user.

6. A "keylogger" was a type of software or hardware that kept track of and recorded keystrokes on an electronic device.

7. "Keystroke logging" was the process of recording every stroke made on a keyboard.

8. A "keystroke logging extension" was a tool that recorded what a person typed on a device.

9. A "cookie" was a file containing a string of characters that a website could place onto a user's computer, allowing the website to recognize the same user during future visits to that website.

10. "Browser cookies" were used by web services to record a sign-in session, allowing a user to retain access to their account after authenticating with a username and password.

11. A "cookie manager application" was a program that allowed a user to control and manage cookies, including by exporting browser cookies from an account and then later import the cookies into a browser of choice, to access those cookies without the owner's knowledge or authorization.

12. "Mailbox rule creation" were rules created in an email program where someone caused the email program to automatically employ a specific action or set of actions on an incoming email.

13. "File masquerading" was a technique where an individual manipulated the name or location of a computer file. One example of file masquerading was renaming the file extension of a computer file to make it appear as it if it was a different file type (*e.g.* renaming a Word .docx file to end in .pdf, to make it appear to be an Adobe Acrobat Portable Document Format file).

14. "Spyware" was a computer program that enabled a third party to obtain information from a user's computer or device without that user's knowledge or authorization.

The Defendant's Scheme

15. In or about and between July 2016 and September 2024, in the District of Maryland, the defendant, **BATHULA** intentionally accessed Company A computers without authorization and thereby obtained information from protected computers, and such was committed in furtherance of a criminal or tortious act in violation of the Constitution or laws of the United States or of any State: to wit, the Maryland state law tort of invasion of privacy for intrusion upon seclusion. Through this unlawful access, **BATHULA** obtained Victims' usernames, passwords, cookies, images, videos, and other data belonging to, or containing information about, the Victims.

16. **BATHULA** employed various cyber intrusion techniques such as keylogging, cookie managers, mailbox rule creation, and file masquerading, to obtain access to Victims' personal and professional accounts for services such as Google Photos, iCloud Photos, Gmail, and Microsoft 365, as well as Victims' social media accounts.

17. Internet service providers such as Google and Microsoft used the Internet to allow their users to access their services and, as a result, were instrumentalities of interstate commerce. **BATHULA**'s unlawful accessing of Victims' personal and professional accounts required access to Google, iCloud, Gmail, and Microsoft servers that were located outside the District of Maryland.

18. In furtherance of this scheme, **BATHULA** created a mailbox rule to automatically

delete incoming emails with subject heading *Critical Security Alert*, so that the Victims (and Company A cybersecurity personnel) would not know that their accounts (or network, in the case of Company A) were compromised.

19. On September 25, 2024 and September 27, 2024, while **BATHULA** had a USB flash drive attached to a Company A computer, Company A obtained the contents of **BATHULA**'s flash drive. A preliminary analysis of the contents revealed the following:

a) approximately 247 unique sexually explicit photos;

b) approximately 27 unique sexually explicit videos;

c) 17 exports from a cookie manager tool containing full sets of browser cookies.

d) 12 unique drivers' license photos belonging to one male and 11 females;

e) six browser extensions to include three keyloggers and two cookie managers;

f) three unique compromising photos that "likely depict criminal activity";

g) three unique passport photos belonging to three females; and

h) one video recording depicting a domestic conflict exported from a home video camera installed in a living room;

20. In addition to exfiltrating Victims' personal information onto a USB flash drive, **BATHULA**'s repeated export of browser cookies allowed him to import those cookies into an internet browser, and access Victims' accounts without their knowledge or authorization. This process allowed **BATHULA** to maintain unauthorized access to Victims' accounts in locations outside of Company A's network, such as on **BATHULA**'s personal electronic devices (*e.g.*, cell phone, tablet, laptops).

21. In or about and between July 2016 and September 2024, in the District of Maryland, the defendant, **MATTHEW BATHULA**, did intentionally access computers used by Company A without authorization and thereby obtain information from a protected computers, and caused the

transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to protected computers; and the offense caused: loss to 1 or more persons during a 1-year period aggregating at least $5,000 in value; and damage affecting 10 or more protected computers during a 1-year period.

22. On at least 21 occasions between in or around February 2023 and in or around July 2024, in the District of Maryland, **BATHULA** installed a spyware software program onto Company A's computers. Using that software, **BATHULA** conducted video surveillance of people present at Company A, and video recorded one or more of the Victims, without the victim's knowledge or consent.

23. On or about and between August 2019 and October 2023, **BATHULA** used the means of identification of Victim-001 (then an employee of Company A) to obtain unauthorized access to a protected electronic account belonging to Victim-001, without Victim-001's authorization, in furtherance of **BATHULA**'s unauthorized access to Victim-001's protected computer, as set forth in Count Two of the Indictment. The information accessed from Victim-001's electronic account included sexually explicit videos and images, videos of breastfeeding recorded from a security camera system within Victim-001's home, and a photo of an identification card containing Victim-001's personal identifying information.

24. None of the Victims gave **BATHULA** authorization to access their computers.

18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)

COUNT TWO
(Unauthorized Access to Protected Computers – Victim-001 through Victim-0195)

In or around and between July 2016 and September 2024, in the District of Maryland and elsewhere, the defendant, **MATTHEW BATHULA**, did intentionally access protected computers, and thereby obtained information from protected computers, to wit: the electronic accounts containing information about Victim-001, through and including Victim-195, and such was committed in furtherance of a criminal or tortious act in violation of the Constitution or laws of the United States or of any State: to wit, the Maryland state law tort of intrusion upon seclusion.

18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B)(ii)

COUNT THREE
(Aggravated Identity Theft)

In or about and between August 2019 and October 2023, in the District of Maryland and elsewhere, the defendant,

MATTHEW BATHULA,

during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), did knowingly transfer and possess, without lawful authority, a means of identification of another person, to wit: Victim-001, a person whose identity is known to the Grand Jury, knowing that the means of identification belonged to another person, during and in relation to the commission of the offense of Unauthorized Access to Protected Computers, in violation of 18 U.S.C. § 1030, as set forth in Count Two.

18 U.S.C. §§ 1028A(a)(1), (c)(5)

FORFEITURE ALLEGATION

The Grand Jury for the District of Maryland further finds that:

1. Pursuant to the Federal Rule of Criminal Procedure 32.2, notice is hereby given to the defendant that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Sections 982(b) and 1030(i); Title 21, United States Code, Section 853; and Title 28, United States Code, Section 2461(c), in the event of the defendant's conviction under Counts One and Two of this Indictment.

Computer Fraud Forfeiture

2. Upon conviction of the offenses set forth in Counts One and Two, the defendant,

MATTHEW BATHULA,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i) and Title 21, United States Code, Section 853, any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly, as a result of such offense, including but not limited to, a money judgment representing the proceeds of such offense; and pursuant to all right, title, and interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such offense:

a) Amazon Kindle Model L5383A;
b) Apple One C8 Silver iPad Model A1395, with serial number ("S/N") DQVGCSWADFHW;
c) Asus Transformer Pad Infinity S/N C90KAS024330;
d) Back Up Plus Slim Portable 1TB Model #SRD00F1, S/N: NA9M9P2Q;
e) Cruiser Glide 16GB USB thumb drive (black), S/N: SDCZ60016G;
f) Data Traveler 100 GB Thumb Drive, Samsung 32 GB, Black USB drive;
g) Dell Laptop Model PP41L S/N: GVDDBH1;
h) Dell PowerEdge T30 server S/N: J0JF152 with power cord;
i) Keylogger;
j) Kodak 256MB SD Card (SD256-111M);
k) Lexar 4GB SD card (31284-4GBCSTA);
l) Maxtor D740X-6L hard drive S/N 663221158753;
m) Maxtor hard drive Model 4D040H2; S/N D20SS2SE;

n) Maxtor hard drive Model 6L080M0; S/N L20PTY9G;
o) Maxtor hard drive Model 6L080M0; S/N L20QK1XG;
p) Micro Center USB 3.0 32 GB thumb drive;
q) My Passport 1TB hard drive, S/N: WX71A6801XU;
r) Nano Wifi Pineapple bearing MAC 00C0CA908802 with 64 GB SanDisk ultra micro SD card;
s) Nikon CoolPix P80 camera S/N RB08237121280 with cords and 1.0 GB SD card;
t) Nikon CoolPix 6500 Camera w/ 16 GB SD Card;
u) PHICOOL 128GB Thumb Drive;
v) PNY Elite Portable SSD;
w) Raspberry Pi 3 Model B+ with 16GB SanDisk card bearing Serial Number 0387AVDF20MT;
x) Raspberry Pi Zero W v. 1.1 with SanDisk Ultra SD card 64 GB;
y) Raspberry Pi Camera v. 2.1 with 64GB SanDisk Ultra and power cord;
z) SamData 32 GB USB 2.0 thumb drive (blue);
aa) Samsung cell phone Model SM-S916U, IMEI: 354491411132494;
bb) Samsung 2TB hard drive, model ST2000DL004; S/N: S2H7J9FC309753;
cc) SanDisk SD card;
dd) SanDisk adaptor with 32 GB Samsung Micro SD S/N: MBMPBGVEQFWB;
ee) SanDisk SD card 0387AVDF20MT;
ff) SanDisk thumb drive (SDCZ430-O16G) S/N BL181026454Z;
gg) SanDisk USB Drive (SDCZ43O-064G) S/N BN200657524W;
hh) Seagate 160GB hard drive: Model ST3160023A; S/N: 3LJ0APHY;;
ii) Seagate 250GB hard drive: S/N: 5VGCDJL7; Model: Momentus 7200.4;
jj) Seagate 1TB Barracuda hard drive; ST1000DM010; S/N: ZN10J93L;
kk) Seagate 1TB hard drive: S/N: 5VX0BZHL; Barracuda LP - ST31000520AS;
ll) Seagate 5TB hard drive ST5000DM000; S/N: W4J1YSCJ;
mm) Seagate 5TB hard drive ST5000DM000; S/N: W4J03QJG;
nn) Simpletch 1GB thumb drive (S/N obscured);
oo) Toshiba 1TB hard drive DT01ACA100; S/N: 17QGNNNMSKBE;
pp) USB drive (black);
qq) USB drive with dip switcher and 1 keylogger with SD card Patriot 16GB;
rr) USB-C device and keylogger;
ss) Western Digital One My Passport Portable Hard Drive, 3EKM Black (Product Number: WDBYFT0040BBK-0A) with connecting cord, one Intel NVC S/N: 044A;
tt) Xbox 360 S/N: 611732121302, with DVD Movie PlayBack Kit;
uu) Xbox 360 S/N: 013576632308; and
vv) Xbox 1 S/N: 201540453148.

Substitute Assets

3. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred, sold to, or deposited with a third party;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty

the United States shall be entitled to forfeiture of substitute property of the Defendant up to the value of the above-described forfeitable property, pursuant to Title 21, United States Code, 853(p), as incorporated by Title 18, United States Code, Section 982(b) and Title 28, United States Code, Section 2461(c).

Kelly O. Hayes
United States Attorney

A TRUE BILL:

SIGNATURE REDACTED
Foreperson

04/30/2026
Date