UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA	)	No. 21 CR 177
	)	
v.	)	Violations: Title 18, United States
	)	Code, Sections
ANDREW MAHN	)	1030(a)(2)(C) and 1343
	)	

COUNT ONE

The SPECIAL NOVEMBER 2020 GRAND JURY charges:

1. At times material to this indictment:

a. Company A was a multi-national corporation headquartered in the Northern District of Illinois.

b. Among other products, Company A sold two-way radios worldwide.

c. Company A allowed customers to unlock additional software features on certain radios by paying a fee. Company A referred to these additional features as "entitlements."

d. Company A maintained computer servers in the Northern District of Illinois that were used to support its sales of products in interstate and foreign commerce.

e. Company A restricted access to its computer network to employees, and required a username, password, and multi-factor authentication in order to log in. The multi-factor authentication process typically entailed an employee receiving a text message on his or her cell phone with a unique code or a

push notification to be input during the log in process to Company A's network.

f. Individual B and Individual F were employees of Company A who worked in the Northern District of Illinois.

2. From no later than August 7, 2020, and continuing through no earlier than October 25, 2020, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

ANDREW MAHN,

defendant herein, knowingly devised, intended to devise, and participated in a scheme to defraud Company A, and to obtain money, funds, and property belonging to Company A, by means of materially false and fraudulent pretenses, representations, and promises, which scheme is further described below.

3. It was part of the scheme that defendant ANDREW MAHN sent fraudulent emails, also referred to as spear phishing emails, to Company A employees asking them to click on a link that purported to be an official Company A website, but was in fact a false website designed to appear like a Company A website created by MAHN as a means to steal Company A employees' usernames and passwords. MAHN then contacted certain Company A employees via text messages to obtain additional login information to obtain unauthorized access to Company A's network. Once on the network, MAHN stole or exfiltrated data, including a Company A software tool that allowed him to unlock entitlements on certain Company A radios, valued at up to $175 per radio.

4. It was further part of the scheme that defendant ANDREW MAHN

registered a domain and created a fake website that purported to be Company A's official payroll login website, but was in fact controlled by MAHN and intended to deceive Company A employees into entering their Company A login information, which allowed defendant to unlawfully harvest Company A employees' usernames and passwords without their permission.

5. It was further part of the scheme that defendant ANDREW MAHN sent emails to at least 31 Company A employees, including Individual B and Individual F, which contained a link to the fake Company A payroll website. The email stated that there was a "task awaiting your approval" in the payroll system, and directed employees to click on a link to the fake payroll website. Employees who clicked on the link were asked to provide their Company A username and password, ostensibly to access in Company A's network, when in fact MAHN was electronically collecting those usernames and passwords without permission.

6. It was further part of the scheme that defendant ANDREW MAHN, after obtaining usernames and passwords, sent text messages to at least one Company A employee, Individual B, purporting to be from Company A's multi-factor authentication service, but were in fact from MAHN. MAHN first sent Individual B emails and text messages falsely claiming that Individual B would have to verify information about his two-factor authentication code at some point in the future. MAHN later sent text messages to Individual B requesting that Individual B send his multi-factor authentication code or approve a login through a push notification.

7. It was further part of the scheme that defendant ANDREW MAHN used

the unlawfully obtained username, password, and multi-factor authentication code from Individual B to access Company A's computer network without authorization. MAHN then modified Individual B's Company A account so that future multi-factor authentication codes would be sent to phone numbers controlled by MAHN, not Individual B.

8. It was further part of the scheme that defendant ANDREW MAHN, after accessing Company A's network without authorization, downloaded a Company A software tool that enabled a user to unlock features or entitlements on Company A communication devices. This stolen source code allowed MAHN to unlock entitlements on an unlimited number of Company A radios for nine years (the period of the software license). Company A normally sold these software features at a price of up to $175 per radio.

9. It was further part of the scheme that defendant ANDREW MAHN, during his unauthorized access to Company A's network, unlocked several entitlements on a specific Company A radio with the internal serial number 871TRB0781, which radio MAHN kept in his home.

10. It was further part of the scheme that defendant ANDREW MAHN concealed, misrepresented, and hid, and caused to be concealed, misrepresented and hidden, the existence, purpose and acts done in furtherance of the scheme.

11. On or about August 28, 2020, in the Northern District of Illinois, Eastern Division, and elsewhere,

ANDREW MAHN,

defendant herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce, certain writings, signs, and signals to the State of Massachusetts from the State of New Hampshire, namely, an email to Individual B containing a link to a fake computer login page for Company A;

In violation of Title 18, United States Code, Section 1343.

COUNT TWO

The SPECIAL NOVEMBER 2020 GRAND JURY charges:

1. Paragraphs 1 through 10 of Count One of this indictment are incorporated here. .

2. On or about September 28, 2020, in the Northern District of Illinois, Eastern Division, and elsewhere,

ANDREW MAHN,

defendant herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce, certain writings, signs, and signals to the Northern District of Illinois by way of a location outside of Illinois, namely, a text message to Individual B requesting Individual B's multi-factor authentication code for Company A's network;

In violation of Title 18, United States Code, Section 1343.

COUNT THREE

The SPECIAL NOVEMBER 2020 GRAND JURY charges:

1. Paragraphs 1 through 10 of Count One of this indictment are incorporated here.

2. On or about September 28, 2020, in the Northern District of Illinois, Eastern Division, and elsewhere,

ANDREW MAHN,

defendant herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce, certain writings, signs, and signals to the Northern District of Illinois by way of a location outside of Illinois, namely, an unauthorized login request to Company A's network using Individual B's fraudulently obtained username and password;

In violation of Title 18, United States Code, Section 1343.

COUNT FOUR

The SPECIAL NOVEMBER 2020 GRAND JURY charges:

1. Paragraphs 1 through 10 of Count One of this indictment are incorporated here. .

2. On or about September 30, 2020, in the Northern District of Illinois, Eastern Division, and elsewhere,

ANDREW MAHN,

defendant herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce, certain writings, signs, and signals to the Northern District of Illinois by way of a location outside of Illinois,, namely, an email to Employee S.B. containing a link to a fake computer login page for Company A

In violation of Title 18, United States Code, Section 1343.

COUNT FIVE

The SPECIAL NOVEMBER 2020 GRAND JURY charges:

1. Paragraph 1 of Count One of this indictment is incorporated here.

2. Between on or about August 7, 2020, and on or about October 25, 2020, in the Northern District of Illinois, Eastern Division, and elsewhere,

ANDREW MAHN,

defendant herein, intentionally accessed a protected computer used in interstate and foreign commerce without authorization, and thereby obtained information from a protected computer, namely the computer network of Company A, and the offense was committed for purposes of commercial advantage and private financial gain, and the value of the information obtained exceeded $5,000;

In violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii).

FORFEITURE ALLEGATION ONE

The SPECIAL NOVEMBER 2020 GRAND JURY further alleges:

1. Upon conviction of an offense in violation of Title 18, United States Code, Sections 1343, as set forth in this Indictment, defendant shall forfeit to the United States of America any property that constitutes and is derived from proceeds traceable to the offense, as provided in Title 18, United States Code, Section 981(a)(1)(D) and Title 28, United States Code, Section 2461(c).

2. The property to be forfeited includes, but is not limited to:

a. a personal money judgment in an amount equal to the proceeds derived from the offenses in violation of Title 18, United States Code, Section 1343;

b. the following specific property:

i. Company A source code, software, or other information.

3. If any of the property described above, as a result of any act or omission by a defendant: cannot be located upon the exercise of due diligence; has been transferred or sold to, or deposited with, a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty, the United States of America shall be entitled to forfeiture of substitute property, as provided by Title 21, United States Code Section 853(p).

FORFEITURE ALLEGATION TWO

The SPECIAL NOVEMBER 2020 GRAND JURY further alleges:

1. Upon conviction of an offense in violation of Title 18, United States Code, Section 1030(a)(2)(C), as set forth in this Indictment, defendant shall forfeit to the United States of America:

a. any property constituting and derived from proceeds obtained directly and indirectly as a result of the offense, as provided in Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(B); and

b. any personal property used and intended to be used to commit and to facilitate the commission of the offense, as provided in Title 18, United States Code, Section 1030(i)(1)(A).

2. The property to be forfeited includes, but is not limited to:

a. a personal money judgment in an amount equal to the proceeds derived from the offenses in violation of Title 18, United States Code, Section 1030(a)(2)(C);

b. the following specific property:

i. Company A source code, software, or other information.

3. If any of the property described above, as a result of any act or omission by a defendant: cannot be located upon the exercise of due diligence; has been transferred or sold to, or deposited with, a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty, the

United States of America shall be entitled to forfeiture of substitute property, as provided by Title 21, United States Code Section 853(p).

A TRUE BILL:

_____

FOREPERSON

_____

signed by Steven J. Dollear on behalf of the
UNITED STATES ATTORNEY