

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

UNITED STATES OF AMERICA

§
§
§
§
§
§
§
§

v.

NO: 6:22-CR- 32-JCB-JDL
JUDGE

IGOR DEKHTYARCHUK,

a/k/a "Igor Dehtyarchuk"

a/k/a "Igor Dekhtiarchuk"

a/k/a "Floraby"

INDICTMENT

THE UNITED STATES GRAND JURY CHARGES:

General Allegations

At all times relevant to this Indictment:

1. Defendant **Igor Dekhtyarchuk** was a resident of Kamensk-Uralsky in Sverdlovsk Oblast, Russia.
2. An "access device" was any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access, that can be used alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument). Access devices included usernames, passwords, answers to recovery questions, cookies, and other data used to access websites and other electronic communications systems.

3. Personally identifiable information (“PII”) was a term that refers to people’s names, social security numbers, dates of birth, addresses, phone numbers, bank account numbers, bank routing numbers, bank account information, and online account usernames and passwords.

4. A “cookie” was a small piece of text sent to a user’s internet browser when visiting websites that were used to verify the user on future visits to the same website. Most online financial institutions and retailers use internet cookies to verify return usage. The account’s website automatically sends a cookie to the user during a successful login, which is stored by the user’s browser. When the user returns to the website, the cookie serves as verification that the login attempt is from the same user as the last successful login.

5. Telegram was an end-to-end encrypted electronic messaging service that can be used to transmit text, links, or files electronically in interstate or foreign commerce between devices such as cellular phones and computers.

6. Marketplace A was an online cybercriminal marketplace dedicated to the sale of unlawfully obtained access devices offered without the permission of the actual owners, including stolen login credentials that enable access to online accounts, such as accounts provided by financial institutions, online payment providers, and retailers. Marketplace A specialized in the sale of unlawfully obtained access devices for compromised Companies A, B, C, D, and E; and credit card accounts, including providing the data associated with those accounts such as name, home addresses, login

credentials, and payment card data for the victims, who are the actual owners of those accounts.

7. Company A, whose identity is known to the Grand Jury, was an online payment processing company headquartered in California.

8. Company B, whose identity is known to the Grand Jury, was an online auction company headquartered in California.

9. Company C, whose identity is known to the Grand Jury, was an online retail company headquartered in California.

10. Company D, whose identity is known to the Grand Jury, was an online retail company headquartered in Arkansas.

11. Company E, whose identity is known to the Grand Jury, was an online retail company headquartered in Massachusetts.

12. **Dekhtyarchuk** was the administrator of Marketplace A and was a Russian hacker who first appeared in hacker forums in November 2013 under the alias “floraby.”

Dekhtyarchuk began advertising the sale of compromised account data in Russian-language hacker forums in April 2018 and opened Marketplace A in May 2018.

Dekhtyarchuk immediately began advertising Marketplace A and the products it sold in May 2018. As of May 2021, **Dekhtyarchuk**, through Marketplace A, publicly advertised that he has sold over 48,000 compromised email accounts, 25,000 compromised Company B accounts, and 19,000 compromised Company A accounts. **Dekhtyarchuk** also prominently advertised the locations of the owners of the compromised accounts,

including the United States and Australia. Around March 2022, and according to site statistics, Marketplace A averaged approximately 5,000 daily visitors.

13. A potential customer who visited Marketplace A to purchase access devices for compromised accounts could select different products just as in a legitimate web store. The options included various combinations of Company A, Company B, Company C, and credit card accounts for the same victim. For example, one option was “[Company A] + CC/[Company B],” meaning the customer could purchase the information sufficient to unlawfully access the Company A, credit card, and Company B accounts for the same victim. Some options were broken down by known account balances, which were sold at different price points.

14. **Dekhtyarchuk** also sold the usage, in seven-day rental increments, of a program called “[Company A] Auth 1.0,” which was a downloadable software program that the customer could use to input the stolen access devices, and using the provided cookie, to access the compromised Company A accounts.

15. Once a customer selected an access device to purchase, clicking on the purchase link brought a customer to a page providing specifics of the selected option. Marketplace A listings regularly advertised that the sale includes the login cookie, which is a kind of access device used to access the compromised accounts.

16. All access devices advertised on Marketplace A were advertised in Russian rubles. Once a customer completed a transaction by paying through the Marketplace A’s payment screen, **Dekhtyarchuk** or his associate, sent the customer the access devices via Telegram text message.

17. Beginning in March 2021 and ending in July 2021, the FBI through an online covert employee (OCE) made thirteen purchases of access devices from **Dekhtyarchuk** while accessing Marketplace A from the Eastern District of Texas. Each purchase varied in number of accounts, ranging from three to twenty accounts, resulting in access devices purchased for a total of 131 accounts. The OCE received the purchased access devices via Telegram messenger service shortly after completing each purchase.

COUNT ONE

Violation: 18 U.S.C. §§ 1343 and 2
(Wire Fraud and Aiding and Abetting)

18. The General Allegations section of this indictment is realleged and incorporated by reference as though fully set forth herein.

19. Between about May 2018 and at least July 2021, the exact dates being unknown, in the Eastern District of Texas and elsewhere, the defendant, **Igor Dekhtyarchuk**, knowingly devised and intended to devise, and aided and abetted others in devising, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises.

20. It was the purpose of the scheme and artifice for the defendant to unlawfully and unjustly enrich himself by transmitting and causing to be transmitted, by means of wire communications in interstate and foreign commerce, the writings, signs, and signals which transmitted, from computers outside the United States to a computer in the United States; that is, **Igor Dekhtyarchuk** sold and transmitted 131 sets of login

credentials and other PII related to online accounts provided by Companies A, B, and D to an FBI online covert employee located in the Eastern District of Texas.

In violation of 18 U.S.C. § 1343.

COUNT TWO

Violation: 18 U.S.C. §§ 1029(a)(2) and
(c)(1)(A)(i)
(Access Device Fraud – Trafficking in
Unauthorized Access Devices)

21. The General Allegations section of this indictment is realleged and incorporated by reference as though fully set forth herein.

22. Between March 29, 2021 and July 7, 2021, in the Eastern District of Texas and elsewhere, defendant **Igor Dekhtyarchuk**, knowingly and with the intent to defraud, and in a manner affecting interstate and foreign commerce by the use of interstate and foreign wire transmissions, trafficking one or more unauthorized access devices, that is, login credentials, including usernames, associated passwords, PII, and cookies for access to accounts provided by Companies A, B, and D, by possessing with intent to sell and by selling said access devices, and by such conduct, between July 9, 2020 and July 7, 2021, in a period of less than one year, obtained anything of value aggregating \$1,000.00 or more.

All in violation of 18 U.S.C. § 1029(a)(3), (c)(1)(A)(1) and (2).

COUNT THREE

Violation: 18 U.S.C. §§ 1029(a)(3) and
(c)(1)(A)(i)
(Access Device Fraud – Possession of
Fifteen or More Counterfeit or
Unauthorized Access Devices)

23. The General Allegations section of this indictment is realleged and incorporated by reference as though fully set forth herein.

24. Between March 29, 2021 and July 7, 2021, in the Eastern District of Texas and elsewhere, defendant **Igor Dekhtyarchuk**, knowingly and with the intent to defraud, possessed fifteen or more unauthorized access devices, that is, login credentials, including usernames and associated passwords, for access to online accounts provided by Companies A, B, and D, said possession affecting interstate and foreign commerce by use of interstate and foreign wire transmissions.

All in violation of 18 U.S.C. § 1029(a)(3), (c)(1)(A)(1) and (2).

COUNT FOUR

Violation: 18 U.S.C. §§ 1029(a)(6) and
(c)(1)(A)(1)
(Access Device Fraud – Unauthorized
Solicitation)

1. The General Allegations section of this indictment is realleged and incorporated by reference as though fully set forth herein.

2. Between March 29, 2021 and July 7, 2021, in the Eastern District of Texas and elsewhere, defendant **Igor Dekhtyarchuk**, without the authorization of the issuer of access devices belonging to the customers of Companies A, B, and D, to wit, account

names, user names, passwords, and cookies used to obtain money, goods, services, or any other thing of value, knowingly and with the intent to defraud, did aid and abet soliciting buyers through the Marketplace A platform with the purpose of offering and selling information regarding said access devices, said conduct affecting interstate and foreign commerce.

All in violation of 18 U.S.C. § 1029(a)(6) and (c)(1)(A)(i).

COUNTS FIVE - THIRTY

Violation: 18 U.S.C. §§ 1028A
(Aggravated Identity Theft)

32. The General Allegations section of this indictment is realleged and incorporated by reference as though fully set forth herein.

33. On or about the dates specified as to each count below, in the Eastern District of Texas and elsewhere, the defendant **Igor Dekhtyarchuk**, without lawful authority, knowingly used means of identification of other persons, that is, account holders' PII, as specified below, during and in relationship to a felony enumerated in 18 U.S.C. § 1028A(c), that is, access device fraud, a violation of 18 U.S.C. § 1029:

Count	Account Holder	Type of PII Used	Date of Possession by the Defendant
5	A.Q.	Name, address, email address, Company A account username	March 29, 2021
6	L.P.	Name, address, email address, Company A account username	April 18, 2021
7	A.G.	Name, address, email address, Company A account username	April 18, 2021

8	C.C.	Name, address, email address, Company A account username	April 18, 2021
9	C.H.	Name, address, email address, Company A account username	April 18, 2021
10	Z.M.	Name, address, email address, Company A account username	April 18, 2021
11	L.M.	Name, address, email address, Company A account username	April 18, 2021
12	G.K.	Name, address, email address, Company A account username	April 19, 2021
13	V.C.	Name, address, email address, Company A account username	April 22, 2021
14	D.H.	Name, address, email address, Company A account username	April 22, 2021
15	S.A.	Name, address, email address, Company A account username	April 22, 2021
16	L.D.	Name, address, email address, Company A account username	April 30, 2021
17	E.J.	Name, address, email address, Company A account username	June 3, 2021
18	B.S.	Name, address, email address, Company A account username	June 3, 2021
19	D.S.	Name, address, email address, Company A account username	June 3, 2021
20	S.A.	Name, address, email address, Company A account username	June 9, 2021
21	J.F.	Name, address, email address, Company A account username	June 9, 2021

22	S.C.	Name, address, email address, Company A account username	June 9, 2021
23	S.F.	Name, address, email address, Company A account username	June 21, 2021
24	C.C.	Name, address, email address, Company B account username	June 25, 2021
25	J.Q.	Name, address, email address, Company B account username	June 25, 2021
26	K.S.	Name, address, email address, Company B account username	June 25, 2021
27	A.B.	Name, address, email address, Company D account username	July 15, 2021
28	B.M.	Name, address, email address, Company D account username	July 15, 2021
29	K.B.	Name, address, email address, Company D account username	July 15, 2021
30	J.J.	Name, address, email address, Company D account username	July 15, 2021

All in violation of 18 U.S.C. § 1028A.

NOTICE OF INTENT TO SEEK CRIMINAL FORFEITURE
Pursuant to 18 U.S.C. §§ 1028(b), 1029(c)(1)(C), and 982(a)(2) and (a)(2)(B)

As a result of committing the offenses as alleged in this Indictment, defendant shall forfeit to the United States pursuant to 18 U.S.C. §§ 1028(b), 1029(c)(1)(C), and 982(a)(2) and (a)(2)(B) any and all property, real or personal, involved in or traceable to property involved in the offense, including proceeds obtained directly or indirectly from the offense, and the following:

Cash Proceeds

A sum of money equal to \$200,000.00 in United States currency, and all interest and proceeds traceable thereto, representing the amount of proceeds obtained by defendant as a result of the offenses alleged in this Indictment, for which the defendant is personally liable.

Substitute Assets

If any property subject to forfeiture, as a result of any act or omission by defendant:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or 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 subdivided without difficulty,

it is the intent of the United States, pursuant to 21 U.S.C. § 853(p), to seek forfeiture of any other property of defendant up to the value of the above forfeitable property, including but not limited to all property, both real and personal, owned by defendant.

By virtue of the commission of the felony offenses charged in this Indictment, any and all interest defendant has in the above-described property is vested in the United States

and hereby forfeited to the United States pursuant to 18 U.S.C. §§ 1028(b), 1029(c)(1)(C), and 982(a)(2) and (a)(2)(B).


A TRUE BILL

3-16-2022
Date:



GRAND JURY FOREPERSON

BRIT FEATHERSTON
UNITED STATES ATTORNEY



D. RYAN LOCKER
Assistant United States Attorney
Texas Bar No. 24046307
110 N. College, Suite 700
Tyler, Texas 75702
(903) 590-1400
(903) 590-1439 Fax

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

UNITED STATES OF AMERICA

§
§
§
§
§

v.

NO: 6:22-CR- 32-JCB-JDL
JUDGE

IGOR DEKHTYARCHUK

NOTICE OF PENALTY

COUNT ONE

VIOLATION:

18 U.S.C. § 1343 – Wire Fraud

PENALTY:

Imprisonment of not more than twenty (20) years; the greater of a fine not to exceed \$250,000, a fine not to exceed two times the gross gain to the Defendant, or a fine not to exceed two times the loss to the victim, or both such imprisonment and fine; and a term of supervised release of not more than three (3) years.

SPECIAL ASSESSMENT:

\$100.00

COUNTS TWO – FOUR

VIOLATION:

18 U.S.C. § 1029 – Access Device Fraud

PENALTY:

Imprisonment of not more than ten (10) years; the greater of a fine not to exceed \$250,000, or both such imprisonment and fine; and a term of supervised release of not more than three (3) years.

SPECIAL ASSESSMENT:

\$100.00 each count

COUNTS FIVE - THIRTY

VIOLATION:

18 U.S.C. § 1028A – Aggravated Identity Theft

PENALTY:

Imprisonment of not less than two (2) years and a fine of \$250,000 to be followed by not more than one (1) year of supervised release. This sentencing is to run

consecutively to any other sentence imposed. A person convicted of a violation of this section shall not be placed on probation.

SPECIAL ASSESSMENT: \$100.00 each count