IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

MAKSIM BEREZAN,

Defendant.

Criminal No. 1:20-CR-145

Count 1: Conspiracy to Commit Wire Fraud Affecting a Financial Institution (18 U.S.C. § 1349)

Counts 2-4: Wire Fraud Affecting a Financial Institution (18 U.S.C. §§ 1343 & 2(a))

Count 5: Conspiracy to Commit Access Device Fraud and Computer Intrusions (18 U.S.C. § 371)

Count 6: Access Device Fraud (18 U.S.C. §§ 1029(a)(3), 1029(b)(1) & 2(a))

Forfeiture Notice

Filed Under Seal

INDICTMENT

June 2020 Term – at Alexandria, Virginia

THE GRAND JURY CHARGES THAT:

GENERAL ALLEGATIONS

At all times material to this Indictment,

1. Defendant **MAKSIM BEREZAN** was an Estonian national who has resided in Latvia and elsewhere.

2. From at least July 2009, through at least December 2015,[1] **BEREZAN** was a member of DirectConnection, an exclusive website that provided a secure space through which individuals engaging in computer crimes (*i.e.*, "cybercriminals") could meet and assist each other in planning and carrying out a variety of malicious and fraudulent cyber activities. As explained below, DirectConnection members used the relationships they developed on DirectConnection to further the criminal aims of DirectConnection itself. They also used DirectConnection to devise other criminal ventures, and sometimes would further these criminal agreements outside the auspices of DirectConnection.

3. **BEREZAN** was an active user of DirectConnection. As explained in Count Five, he furthered the operation of DirectConnection and its criminal aims in a variety of ways, such as by vouching for users, paying fees, participating in a dispute resolution mechanism, alerting other DirectConnection users of law enforcement activity, and communicating with other DirectConnection users about certain unlawful services. **BEREZAN** also used DirectConnection to form agreements with other cybercriminals regarding the acquisition and use of stolen payment card information and the movement of fraudulently obtained funds and goods.

A. Background on DirectConnection

4. In order to join DirectConnection, prospective members had to undergo a vetting process. A cybercriminal generally had to have three DirectConnection members vouch for him or her, and provide his or her history of committing cybercrime, reputation for committing cybercrime, and reputation for dealing fairly with other cybercriminals. The vouching members

[1] When the Grand Jury alleges in this Indictment that an event occurred on a particular date, the Grand Jury means to convey that the event was alleged to occur "on or about" or "in or around" that date.

would have to pay an amount of money (usually about $5,000 split among the three vouching members), as insurance in case the applicant failed to honor the agreements the applicant made with other DirectConnection members.

5. The DirectConnection site was organized into a number of sections, and members could post messages on different topics that were viewable to other DirectConnection members. These sections, which were known as forums, covered such topics as news relevant to cybercrime, complaints regarding other DirectConnection members, the commission of financial fraud, and the commission of computer intrusions and use of computer exploits.[2]

6. Within each forum, members of DirectConnection created "threads," that is, posts about particular topics to which other members could respond by posting messages that would be viewable to the creator of the thread and other DirectConnection members.

7. Members of DirectConnection also could send one another private messages through the website. These private messages often led to members exchanging contact information, which often led to DirectConnection members corresponding with one another through such online instant messaging services as Jabber and ICQ.

8. Some members of DirectConnection took on leadership positions. In particular, there were at least two administrators, approximately a dozen moderators, and at least one arbiter. The administrators had authority over the forum as a whole, the moderators were responsible for the discussions of particular forums to which they were assigned, and the arbiter adjudicated disputes among DirectConnection members, as further described below.

[2] When the Grand Jury alleges in this Indictment that there was a particular posting on DirectConnection or a particular communication by a co-conspirator, the Grand Jury means to convey that such posting or communication has been translated from Russian to English.

9. For purposes of building trust among DirectConnection's members and facilitating criminal partnerships among members, DirectConnection had a formal dispute resolution mechanism. If a dispute arose among DirectConnection members regarding a criminal agreement, the aggrieved member could file a complaint for purposes of having the dispute adjudicated by another member of DirectConnection. Members who did not abide by the decisions of DirectConnection's adjudicators in regards to these complaints could be expelled from the website.

B. Background on Carding

10. From at least August 2010, and continuing through the present, **BEREZAN** engaged in "carding," which is a term commonly used by cybercriminals to describe the general concept of unlawfully acquiring and using data associated with debit and credit cards (*i.e.*, "payment cards") for purposes of conducting fraudulent transactions and withdrawals. The types of payment card data of interest to carders include card type (*e.g.*, credit or debit), account number, card verification value (CVV) or card verification code (CVC), card expiration date, and personal identification numbers (PINs).[3]

11. Carders are known to use the terms "dumps" or "dump data" to refer to the unauthorized copying of the information contained on the magnetic stripe of a payment card, such as the card's primary account number (PAN)—which is the 14, 15, or 16-digit number typically embossed on the face of a payment card—and the card's expiration date. The information on magnetic stripes of payment cards sometimes is referred to as "track data."

12. **BEREZAN** specialized in "cashouts" and "drops."

[3] A "PIN" is the set of digits (typically four) that must be inputted at the time a debit card is used at an automated teller machine (ATM) or point-of-sale terminal to request a withdrawal of money from a bank account associated with the debit card.

a. "Cashouts," or "cashing out," refers to using dump data and PINs to make fraudulent purchases or to withdraw money from bank accounts without authorization. Cashouts are achieved by encoding dump data onto the magnetic stripe of a physical card and then inserting or swiping the counterfeit physical card (and if necessary providing the PIN associated with the dump data) at a point-of-sale terminal or ATM.

b. A "drop" refers to a location or individual able to securely receive and forward funds or goods obtained through cashouts or other types of fraud, and typically are used to make it harder for law enforcement to trace fraudulent transactions and to circumvent the fraud detection measures used by banks and credit card companies.

C. Additional Relevant Terms and Definitions

13. The following are definitions for terms used throughout the Indictment:

a. "Malware" is hostile or intrusive software or coding that can be used to compromise computers and computer networks. Although functionality varies, one use of malware is to harvest personally identifiable information and financial data, such as dumps and PINs.

b. "Injects" refers to malicious code that targets web browsers and enables the theft of information inputted into a website field by a user.

c. A "botnet" is a network of compromised internet-connected devices.

14. ICQ was an online, cross-platform instant messaging service. From at least 2009 and continuing through at least 2012, ICQ had servers located within the Eastern District of Virginia. As a result, messages sent and received through ICQ during this time period caused wire communications to be transmitted into and out of servers located in the Eastern District of Virginia.

15. "Financial Institution A" was a U.S. banking entity headquartered in Virginia, within the Eastern District of Virginia, and insured by the Federal Deposit Insurance Corporation (FDIC).

16. "Financial Institution B" was a U.S. banking entity headquartered in North Carolina, and insured by the FDIC.

17. "Financial Institution C" was a U.S. banking entity headquartered in New York, and insured by the FDIC.

COUNT ONE

(Conspiracy to Commit Wire Fraud Affecting a Financial Institution)

THE GRAND JURY FURTHER CHARGES THAT:

18. The general allegations of this Indictment, Paragraphs 1 to 17, are re-alleged and incorporated into this Count as though fully set forth herein.

19. From at least August 2010, and continuing through the present, in the Eastern District of Virginia and elsewhere, the defendant,

MAKSIM BEREZAN,

who will be first brought to the Eastern District of Virginia, did knowingly and unlawfully conspire with other persons, known and unknown to the Grand Jury, to devise and intend to devise a scheme and artifice to defraud and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, such scheme and artifice affecting a financial institution, and for the purpose of executing such scheme and artifice transmitted and caused to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, in violation of Title 18, U.S. Code, Section 1343.

Purpose of the Conspiracy

20. The purpose of the conspiracy was to personally profit from stolen payment card data. **BEREZAN** and his co-conspirators stole payment card data (or obtained stolen payment card data from others), used this data to engage in fraudulent transactions and withdrawals across the United States and in foreign countries, and moved (and helped move) the proceeds of the fraudulent transactions and withdrawals in a manner designed to evade detection. The conspiracy, as a result, defrauded financial institutions and merchants that allowed the fraudulent

transactions and withdrawals to occur based on the false pretense and representation that the stolen payment card data was being used by the authorized users of those payment cards.

Manner and Means of the Conspiracy

21. The manner and means by which **BEREZAN** and his co-conspirators sought to accomplish the purpose of the conspiracy included, but were not limited to, the following:

a. As part of the conspiracy, **BEREZAN** joined DirectConnection and used it to solicit and obtain the assistance of other DirectConnection members in acquiring dumps and PINs and using dumps and PINs to engage in cashouts.

b. It further was part of the conspiracy that **BEREZAN** communicated with co-conspirators through ICQ about acquiring dumps and PINs and using dumps and PINs to engage in cashouts.

c. It further was part of the conspiracy that **BEREZAN** and his co-conspirators used compromised computers to obtain PANs without authorization.

d. It further was part of the conspiracy that **BEREZAN** and his co-conspirators unlawfully enriched themselves by cashing out dumps and PINs.

e. It further was part of the conspiracy that **BEREZAN** had a network of drops in the United States and elsewhere that he used for cashouts and made available to other cybercriminals engaged in fraudulent conduct.

Overt Acts

22. As part of the conspiracy, **BEREZAN** and his co-conspirators committed the following overt acts, among others, in furtherance of and to effect the object of the conspiracy. These overt acts were committed within the Eastern District of Virginia and elsewhere.

23. On February 21, 2009, co-conspirator Aleksei Burkov and another co-conspirator launched DirectConnection, which was accessible from anywhere in the world, including the United States, via an internet connection.

24. On July 15, 2009, **BEREZAN** became a member of DirectConnection and used an account to communicate under a particular moniker.[4]

A. BEREZAN's Recruitment Efforts and Requests for Assistance

25. On August 25, 2010, **BEREZAN** posted a message within the "Cyber security. Programming. Cracking. Cracking, data bases, bot nets. Trojans and scripts. Exploits" forum on DirectConnection in which he requested access to a "botnet" in the United States. **BEREZAN** offered to share the proceeds of cashouts with people in control of large botnets, explaining he would provide the "injects" designed to steal card numbers, CVVs, expiration dates, and PINs.

26. On November 25, 2010, **BEREZAN** posted a message within the "Cyber security. Programming. Cracking. Cracking, data bases, bot nets. Trojans and scripts. Exploits" forum on DirectConnection asking for assistance in extracting dumps from wireless networks in grocery stores and decrypting PINs.

27. On December 8, 2010, **BEREZAN** sent a private message through DirectConnection to another co-conspirator titled "offer for you." The message stated, in relevant part:

> I saw your post about drops. I texted you before, we do professional cash-outs. I've had another idea, so I decided to write you about it, think how this will go. [L]ook, I do cash out of credit cards. [M]y coder made injects for collection of cc, cvv, expiry dates and PINs.

[4] For the remainder of the Indictment, the Grand Jury will allege that the person using this moniker was **BEREZAN** without reference to the specific moniker used.

> I make a dump with this information, and we cash it out. [I]f you have a botnet, I suggest you loading our injects for collection of cc. [T]he traffic will pay off + we'll get something for us. [I]t's just the time now when banks raise limits before new year, so that holders buy expensive gifts :-) [L]et's load our injects, withdraw the material and cash it out. [A]s for %, we'll negotiate that. [I]f you are interested in that matter, contact me . . . .

28. On June 2 and 6, 2011, **BEREZAN** posted messages within the "Real carding. Documents. Real plastic. Equipment, dumps (cashout/sale). Documents. Scans and documents" forum on DirectConnection requesting assistance in decrypting PINs in a particular format. **BEREZAN** explained that much of the dump was valid and asked to be contacted via private message.

29. On January 4, 2012, **BEREZAN** posted a message within the "Real carding. Documents. Real plastic. Equipment, dumps (cashout/sale). Documents. Scans and documents" forum on DirectConnection offering assistance in conducting cashouts of dumps and PINs in the United States.

30. On June 7, 2012, **BEREZAN** posted a message within the "Sale and purchase of cards. Visa, MasterCard, AMEX. COBs, VBV, CVV. Extraction of SSN/DOB and other cardholder information" forum on DirectConnection asking for credit and debit card PANs and PINs in exchange for 30% to 35% of the cashout.

31. On April 30, 2015, **BEREZAN** posted a message within the "Real carding. Documents. Real plastic. Equipment, dumps (cashout/sale). Documents. Scans and documents" forum on DirectConnection requesting assistance "cashing" certain PANs "with PINS."

32. On December 1, 2015, **BEREZAN** sent a private message to a DirectConnection co-conspirator asking where the user wanted to try cashing out dump data without PINs, and the user responded on December 7, 2015, by providing a Jabber address.

B. BEREZAN's Carding Activity with Card Source

33. Since at least November 2010, **BEREZAN** communicated with a co-conspirator, who will be referred to herein as the "Card Source," about dumps and PINs.

34. In particular, on November 25, 2010, **BEREZAN** sent a private message through DirectConnection to Card Source that was titled "hi dump + PIN," stated that **BEREZAN** could "try to withdraw up to 150k via POS-terminal, 20% are yours," and asked Card Source to contact **BEREZAN** if he was interested. Card Source responded the next day that he did not "have those for now" but thought he would have dumps and PINs "in a week" and would "message [**BEREZAN**] once they're available."

35. Subsequently on April 13, 2011, **BEREZAN** posted a message within the "Sale and purchase of cards. Visa, Mastercard, AMEX. COBs, VBV, CVV. Extraction of SSN/DOB and other cardholder information" forum on DirectConnection. The title of the message was "cc + pin," and **BEREZAN** later deleted this posting on June 6, 2011.

36. The next day, on April 14, 2011, Card Source sent a private message through DirectConnection to **BEREZAN** regarding **BEREZAN's** "cc + pin" posting. Card Source provided his Jabber account and stated, in relevant part, "[H]i, I do have that, fresh and on permanent basis. Can I hear more details about the bruteforce? Is it fast/slow, does it kill much, does it only accept debit cards or also credit card, about BoF and so on? Or leave me your Jabber." **BEREZAN** responded on April 18, 2011, writing that he wanted to talk to Card Source via Jabber, and that, "[I]t works with all cards, both credit and debit. [A]s for fast or slow, it

depends on quality of the cc. [I]f the cards are fresh, it is fast. [Y]ou set it up today and cream off in the end of the week."

37. As explained below, at least by June 1, 2011, Card Source agreed to provide **BEREZAN** with dumps and did so.

C. BEREZAN's Carding Activity with the Carding Co-Conspirator

38. On July 4, 2009, a co-conspirator, who will be referred to herein as the "Carding Co-Conspirator," became a member of DirectConnection.

39. On September 21 and 29, 2010, Carding Co-Conspirator sent private messages through DirectConnection to **BEREZAN** that referenced PINs and provided Carding Co-Conspirator's contact information for ICQ.

40. On September 29, 2010, and continuing through at least October 9, 2011, **BEREZAN** and Carding Co-Conspirator communicated with each other through ICQ about carding, which caused wire communications to be transmitted from outside the Commonwealth of Virginia and into the Eastern District of Virginia and vice versa. Through these communications, **BEREZAN** and Carding Co-Conspirator agreed to the following arrangement: **BEREZAN** would send to Carding Co-Conspirator batches of PANs and related information; Carding Co-Conspirator would process the PANS to create dumps needed for cashing out; Carding Co-Conspirator would send dumps to **BEREZAN**, who would then provide the PINs for the dumps; and **BEREZAN** and Carding Co-Conspirator thereafter would engage in cashouts. Examples of these ICQ communications include:

a. On November 5, 2010, **BEREZAN** told Carding Co-Conspirator that he was sending him a batch of PANs "3.5k" in size, and asked Carding Co-Conspirator to "process

them quickly" because although "the material is fresh . . . many of them are pre-2010 . . . ." Carding Co-Conspirator responded that he would process the PANs.

b. On March 18, 2011, **BEREZAN** sent messages to Carding Co-Conspirator offering to conduct cashouts on Carding Co-Conspirator's behalf. **BEREZAN** explained that he could cashout "in the USA" and that his "cashouter takes 19%."

c. On March 28, 2011, Carding Co-Conspirator sent **BEREZAN** 15 PANs, and **BEREZAN** responded the same day with the PINS that corresponded to those PANs.

d. On May 2, 2011, **BEREZAN** told Carding Co-Conspirator that he had successfully cashed out "about 3k" from a batch of PANs that the pair had previously shared.

e. On May 30, 2011, Carding Co-Conspirator sent **BEREZAN** 14 PANs and advised that half of the PANs were for **BEREZAN**, and sent separately another 23 PANS and advised that all of these PANS were for **BEREZAN**. Two days later, on June 1, 2011, **BEREZAN** shared with Carding Co-Conspirator the PINs for each of the 14 PANS that were to be split between **BEREZAN** and Carding Co-Conspirator.

f. Also on June 1, 2011, **BEREZAN** and Carding Co-Conspirator exchanged several messages. **BEREZAN** explained, among other things, that: a "base for 1k" **BEREZAN** had provided previously came from Card Source; that "there won't be any PINs for" Card Source's base; and **BEREZAN** had his own botnet that was collecting PANs

g. On June 20, 2011, Carding Co-Conspirator sent **BEREZAN** a message containing 14 PANs, and **BEREZAN** responded the same day with the PINS that corresponded to 9 of those PANs.

h. Also on June 20, 2011, Carding Co-Conspirator, at **BEREZAN's** request, sent 15 PANs to **BEREZAN** via an ICQ instant message. At least one of the PANs that Carding

Co-Conspirator sent to **BEREZAN** had been issued by Financial Institution B, including a PAN ending in 5127, which had been issued in the name of an individual residing in Massachusetts, and which subsequently was used between June 22, 2011, and July 12, 2011, to conduct more than $2,200 in fraudulent transactions at locations in the United Kingdom and Estonia.

41. On November 28, 2012, **BEREZAN** sent a private message to Carding Co-Conspirator through DirectConnection indicating he had approximately 10,000 PANs to share with Carding Co-Conspirator.

D. BEREZAN's Carding Activity with Burkov

42. **BEREZAN** began privately messaging Burkov on DirectConnection as early as June 13, 2012.

43. In 2013 and 2014, **BEREZAN** sent private messages to Burkov containing **BEREZAN's** Jabber user name and particular email addresses so that the pair could communicate outside of DirectConnection.

44. Sometime on or before April 17, 2015, a co-conspirator provided **BEREZAN** with dumps for several payment cards, and **BEREZAN** sent these dumps to Burkov. On April 18, 2015, **BEREZAN** sent a private message on DirectConnection to Burkov complaining that Burkov had not responded yet about the dumps. **BEREZAN** included in this message dumps for 13 payment cards issued by Financial Institution B and Financial Institution C, including PANs ending in 0532, 2495, 5902, 8509, and 9302 that one or more co-conspirators used between April 17 and 18, 2015, in Miami, Florida, to make fraudulent withdrawals totaling approximately $5,000.

45. On April 22, 2015, **BEREZAN** sent to Burkov another private message through DirectConnection that, again, complained about Burkov's non-response and stated: "[G]et more responsible. [T]he more material you take, the longer you are gone for."

E. BEREZAN's Carding Activity with the Drops Co-Conspirator

46. Since at least February 4, 2014, **BEREZAN** sent private messages through DirectConnection to another DirectConnection co-conspirator interested in drops, who will be referred to herein as the "Drops Co-Conspirator."

47. On July 10, 2015, **BEREZAN** sent a private message through DirectConnection to Drops Co-Conspirator that stated, in relevant part: "[Y]ou know where to go for non-duped drops :-) IE, UK, PT, AT, DE, GR, BG, RO, SL, SK, CZ. [W]e usually pay 40%, or 45% if it works out real nice."

48. Drops Co-Conspirator responded with a private message on July 20, 2015, that stated, in relevant part: "40% is too little, I'm paid as much as 50, therefore I'll agree to 45 with a heavy heart." **BEREZAN** responded shortly thereafter, "deal :-)"

(All in violation of Title 18, U.S. Code, Section 1349.)

COUNT TWO
(Wire Fraud Affecting a Financial Institution)

THE GRAND JURY FURTHER CHARGES THAT:

49. The general allegations of this Indictment, Paragraphs 1 to 17, are re-alleged and incorporated into this Count as though fully set forth herein.

50. From at least September 2010, and continuing through at least November 2012, in the Eastern District of Virginia and elsewhere, the defendant,

MAKSIM BEREZAN,

who will be first brought to the Eastern District of Virginia, did knowingly devise and intend to devise a scheme and artifice to defraud and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, such scheme and artifice affecting a financial institution, and for the purpose of executing such scheme and artifice, and attempting to do so, transmitted and caused to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds.

The Scheme and Artifice

51. Paragraphs 20 and 21 are re-alleged and incorporated here as a description of the scheme and artifice.

Execution of the Scheme and Artifice

52. On May 30, 2011, Carding Co-Conspirator, at **BEREZAN's** request, sent 23 PANs to **BEREZAN** via an ICQ instant message, which caused a wire communication to be transmitted through one or more of ICQ's servers located in the Eastern District of Virginia to a computer located outside the Commonwealth of Virginia.

53. At least two of the PANs that Carding Co-Conspirator sent to **BEREZAN** had been issued by Financial Institution B, including:

a. a PAN ending in 7391, which had been issued in the name of an individual residing in New Mexico, and which subsequently was used on June 2, 2011, to make $186 in fraudulent purchases at an Apple store located in Brooklyn, New York; and

b. a PAN ending in 4578, which had been issued in the name of an individual residing in Pennsylvania, and which subsequently was used between June 20 and 23, 2011, to conduct more than $200 in fraudulent transactions at locations in New Jersey and New York.

(All in violation of Title 18, U.S. Code, Sections 1343 and 2(a).)

COUNT THREE
(Wire Fraud Affecting a Financial Institution)

THE GRAND JURY FURTHER CHARGES THAT:

54. The general allegations of this Indictment, Paragraphs 1 to 17, are re-alleged and incorporated into this Count as though fully set forth herein.

55. From at least September 2010, and continuing through at least November 2012, in the Eastern District of Virginia and elsewhere, the defendant,

MAKSIM BEREZAN,

who will be first brought to the Eastern District of Virginia, did knowingly devise and intend to devise a scheme and artifice to defraud and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, such scheme and artifice affecting a financial institution, and for the purpose of executing such scheme and artifice, and attempting to do so, transmitted and caused to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds.

The Scheme and Artifice

56. Paragraphs 20 and 21 are re-alleged and incorporated here as a description of the scheme and artifice.

Execution of the Scheme and Artifice

57. On June 20, 2011, Carding Co-Conspirator, at **BEREZAN's** request, sent 15 PANs to **BEREZAN** via an ICQ instant message, which caused a wire communication to be transmitted through one or more of ICQ's servers located in the Eastern District of Virginia to a computer located outside the Commonwealth of Virginia.

58. At least one of the PANs that Carding Co-Conspirator sent to **BEREZAN** had been issued by Financial Institution B, including a PAN ending in 5127 that had been issued in

the name of an individual residing in Massachusetts, and that subsequently was used between June 22, 2011, and July 12, 2011, to conduct more than $2,200 in fraudulent transactions at locations in the United Kingdom and Estonia.

(All in violation of Title 18, U.S. Code, Sections 1343 and 2(a).)

COUNT FOUR
(Wire Fraud Affecting a Financial Institution)

THE GRAND JURY FURTHER CHARGES THAT:

59. The general allegations of this Indictment, Paragraphs 1 to 17, are re-alleged and incorporated into this Count as though fully set forth herein.

60. From at least September 2010, and continuing through at least November 2012, in the Eastern District of Virginia and elsewhere, the defendant,

MAKSIM BEREZAN,

who will be first brought to the Eastern District of Virginia, did knowingly devise and intend to devise a scheme and artifice to defraud and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, such scheme and artifice affecting a financial institution, and for the purpose of executing such scheme and artifice, and attempting to do so, transmitted and caused to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds.

The Scheme and Artifice

61. Paragraphs 20 and 21 are re-alleged and incorporated here as a description of the scheme and artifice.

Execution of the Scheme and Artifice

62. On June 1, 2011, **BEREZAN** sent PINs for 14 PANs to Carding Co-Conspirator via an ICQ instant message, which caused a computer located outside the Commonwealth of Virginia to transmit a wire communication through one or more of ICQ's servers located in the Eastern District of Virginia.

63. **BEREZAN** provided PINS to Carding Co-Conspirator that corresponded to PANS, including a PAN ending in 4394 that had been issued by Financial Institution A in the name of an individual residing in Arizona.

(All in violation of Title 18, U.S. Code, Sections 1343 and 2(a).)

COUNT FIVE

(Conspiracy to Commit Access Device Fraud and Computer Intrusions)

THE GRAND JURY FURTHER CHARGES THAT:

64. The general allegations of this Indictment, Paragraphs 1 to 17, are re-alleged and incorporated into this Count as though fully set forth herein.

Illegal Objects of the Conspiracy

65. From at least July 2009, through at least December 2015, in the Eastern District of Virginia and elsewhere, the defendant,

MAKSIM BEREZAN,

who will be first brought to the Eastern District of Virginia, did knowingly and unlawfully conspire with other persons, known and unknown to the Grand Jury, to commit the following offenses against the United States:

a. to knowingly and with intent to defraud, traffic in and use one and more unauthorized access devices during a one-year period, and by such conduct obtain things of value aggregating $1,000 and more during that period, said use in violation of Title 18, U.S. Code, Section 1029(a)(2); and

b. to intentionally access a computer without authorization and exceed authorized access, and thereby obtain information from a protected computer in which such access was for purposes of private financial gain, in furtherance of any criminal and tortious act in violation of the laws of the United States and of any State, and was to obtain information with a value exceeding $5,000, in violation of Title 18, U.S. Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B).

Manner and Means of the Conspiracy

66. The manner and means by which **BEREZAN** and his co-conspirators sought to accomplish the purposes of the conspiracy included, but were not limited to, the following:

a. As part of the conspiracy, co-conspirator Aleksei Burkov and another co-conspirator created DirectConnection so that elite cybercriminals had a secure location to meet

one another and assist each other in committing, among other crimes, access device fraud and computer intrusions.

b. It further was part of the conspiracy that Burkov, **BEREZAN**, and their co-conspirators restricted membership to DirectConnection by requiring new applicants to the website to have the backing of three current members of DirectConnection. The vouching members had to state the applicant's history of criminal conduct, reputation for committing crime, and reputation for fair dealings with other criminals, and they had to pay an amount of money (usually about $5,000 split among the vouchers) as insurance in case the applicant failed to honor agreements made with other DirectConnection members.

c. It further was part of the conspiracy that co-conspirator Burkov appointed a number of co-conspirators to leadership positions within DirectConnection in order to help administer the website and further its criminal aims.

d. It further was part of the conspiracy that Burkov, **BEREZAN**, and their co-conspirators posted advice on how to avoid arrest, monitored possible arrests of DirectConnection members, and removed the access of arrested members in order to prevent law enforcement from using cooperating members to infiltrate DirectConnection.

e. It further was part of the conspiracy that Burkov, **BEREZAN**, and their co-conspirators used DirectConnection to solicit and obtain the assistance of other DirectConnection members in committing, among other crimes, access device fraud and computer intrusions.

f. It further was part of the conspiracy that Burkov, **BEREZAN**, and their co-conspirators posted threads about criminal activity on DirectConnection, responded to comments in threads about criminal activity, and communicated with one another by private

message about criminal activity or to setup another means of communication for discussing criminal conduct.

g. It further was part of the conspiracy that co-conspirator Burkov, **BEREZAN**, and their co-conspirators furthered the administration of DirectConnection and its criminal aims by agreeing to abide by a dispute resolution mechanism in which a DirectConnection co-conspirator adjudicated complaints filed by aggrieved DirectConnection co-conspirators.

Overt Acts

67. As part of the conspiracy, **BEREZAN** and his co-conspirators committed the overt acts set forth in Paragraphs 23 to 36 and 42 to 48, as well as the following overt acts, among others, in furtherance of and to effect the objects of the conspiracy. These overt acts were committed in the Eastern District of Virginia and elsewhere.

68. On October 8, 2009, **BEREZAN** sent a private message to another DirectConnection co-conspirator that stated he had "drops in DE" and provided his ICQ contact information. The recipient of this message responded the next day asking if the drops were "duped or non-duped." **BEREZAN** responded on October 12, 2009: "non-duped!" The pair thereafter agreed to use ICQ in order to further discuss working together on the drops.

69. On September 29, 2010, **BEREZAN** made a "claim" against another DirectConnection co-conspirator. **BEREZAN** alleged, in relevant part:

> I, [**BEREZAN**], am aware of the forum statute[.] I'm responsible for credibility of facts and suggestions provided, and I understand that consideration of my claim can lead to revoking both my and my opponent's membership on this forum Claimant: [**BEREZAN**] Respondent: [redacted] Essence of the claim: This person falsely accused me of scamming without providing any proof. I demand

> proofs on the part of [redacted] or his ban on this site. I request the administrators to address this situation.

70. On October 6, 2010, **BEREZAN** posted a message within the "General section. Skirmishes, complaints, debtors and exposure of scammers" forum of Direct Connection that accused another DirectConnection user of borrowing money from **BEREZAN** and failing to pay it back. **BEREZAN** warned that the other DirectConnection user had "played a dirty trick," asked "the administrators to take measures," and demanded his money back plus "double for such a dirty trick."

71. On August 8, 2011, while in the United States, a DirectConnection co-conspirator posted a message within the "Sale and purchase of cards. Visa, MasterCard, AMEX. COBs, VBV, CVV. Extraction of SSN/DOB and other cardholder information" forum that included his email address and stated: "We're selling US CC with a known available balance. 100% validity. It's possible to pick by the state. Prices: $5 for a CC + $0.5 for every 1K on the balance (that is 1-2K available balance = $5.5, 2-3K = $6.5 etc)"

72. On November 12, 2011, Burkov posted an advertisement on DirectConnection for a website selling stolen payment card data, including data belonging to residents in the Eastern District of Virginia and cards that had been issued by Financial Institution A.

73. On January 30, 2012, **BEREZAN** posted a message within the "Spam. Hosting and traffic. Spam. Downloads and traffic. Hosting, domains and servers" forum on DirectConnection regarding the sale of a database with U.S. data. **BEREZAN** explained that his acquaintance was willing to sell a database consisting of usernames and passwords for more than "7kk" U.S. users and more than 2 million U.K. users.

74. On September 24, 2012, **BEREZAN** posted a message within the "Media. News, publications, journalist articles and everything related to our subject" forum on DirectConnection

regarding Thailand law enforcement's arrest of two Russians for using stolen bank data to engage in unauthorized withdrawals.

75. On October 11, 2012, **BEREZAN** filed a complaint on DirectConnection against another user for referring **BEREZAN** to an individual to whom **BEREZAN** provided dump data and who used the dump data to withdraw cash but did not remit any money to **BEREZAN**.

76. On March 25, 2013, a DirectConnection co-conspirator sent a private message to **BEREZAN** regarding "corporate" and "personal drops" and stated he would give thought to what could be "arranged." **BEREZAN** responded the same day, providing his Jabber address and asking the DirectConnection co-conspirator to contact him to "talk."

77. On June 12, 2014, **BEREZAN** sent to "Support" for DirectConnection the following private message: "I'm vouching for menace. [H]e asked me to write you."

78. On August 10, 2014, **BEREZAN** sent a private message to "Support" for DirectConnection, writing that he was having difficulty paying a "forum fee" of $105 for three months' worth of access to the website.

79. On December 1, 2014, **BEREZAN** posted a message within the "Media. News, publications, journalist articles and everything related to our subject" forum on DirectConnection with a link to a security researcher's online posting about malware being used to hack ATMs and a request for anyone "related to that" (*i.e.*, the hack of ATMs with malware) to contact **BEREZAN**.

80. On November 20, 2015, a DirectConnection co-conspirator posted an advertisement indicating that he wished to sell a database containing the names and dates of birth of over 191 million Americans. This database contained the personal information of American citizens residing in the Eastern District of Virginia.

(All in violation of Title 18, U.S. Code, Sections 371.)

COUNT SIX

(Access Device Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

81. The general allegations of this Indictment, Paragraph 1 to 17, are re-alleged and incorporated into this Count as though fully set forth herein.

82. On April 18, 2015, defendant,

MAKSIM BEREZAN,

who will be first brought to the Eastern District of Virginia, knowingly and with intent to defraud, possessed and attempted to possess fifteen or more devices which were unauthorized access devices—namely, PANs, PINs, expiration dates, and associated information—and said possession affected interstate and foreign commerce.

(All in violation of Title 18, U.S. Code, Sections 1029(a)(3), 1029(b)(1), and 2(a).)

NOTICE OF FORFEITURE

83. The Grand Jury finds that there is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

84. Pursuant to Federal Rule of Criminal Procedure 32.2(a), the United States of America gives notice to the defendant,

MAKSIM BEREZAN,

that, if convicted of any of the offenses set forth in this Indictment, the defendant, shall forfeit to the United States, pursuant to Title 18, U.S. Code, Sections 982(a)(2) and 1030(i)(1)(B), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violation.

85. Pursuant to Federal Rule of Criminal Procedure 32.2(a), the defendant,

MAKSIM BEREZAN,

is hereby notified, that, if convicted of the offense set forth in Count 5 of the Indictment, he shall forfeit to the United States, pursuant to Title 18, U.S. Code, Sections 1029(c)(1)(C) and 1030(i)(1)(A), any personal property that was used or intended to be used to commit or to facilitate the commission of such violation.

86. Pursuant to Federal Rule of Criminal Procedure 32.2(a), the defendant,

MAKSIM BEREZAN,

is hereby notified, that, if convicted of the offense set forth in Count 6 of the Indictment, he shall forfeit to the United States, pursuant to 18 U.S. Code § 1029(c)(1)(C), any personal property used or intended to be used to commit the offense.

87. Pursuant to Title 21, U.S. Code, Section 853(p), the defendant,

MAKSIM BEREZAN,

shall forfeit substitute property, if, by any act or omission of the defendant, the property referenced above cannot be located upon the exercise of due diligence; has been transferred, 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.

(Pursuant to 18 U.S.C. § 982(a)(2); 18 U.S.C § 1030(i); 18 U.S.C § 1029(c)(1)(C); 21 U.S.C. § 853; and Fed. R. Crim. P. 32.2.)

A TRUE BILL:

Foreperson of the Grand Jury

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

Alexander P. Berrang
Assistant United States Attorney

Alison Zitron
Trial Attorney
Computer Crime & Intellectual Property Section
Department of Justice

Laura Fong
Senior Trial Attorney
Computer Crime & Intellectual Property Section
Department of Justice