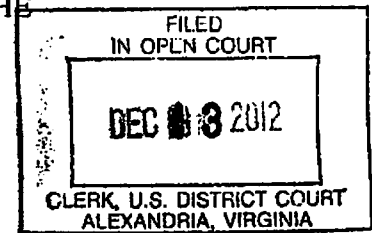


IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

ANDRIY DERKACH and
MIKHAIL RYTIKOV,

Defendants.

CRIMINAL NO.: 1:12-CR-522

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

Counts 2 through 10: Wire Fraud
(18 U.S.C. §§ 1343 and 2)

Count 11: Possession of Fifteen or More
Unauthorized Access Devices
(18 U.S.C. §§ 1029(a)(3) and 2)

Counts 12 through 18: Accessing Protected
Computer in Furtherance of Fraud
(18 U.S.C. §§ 1030(a)(4) and 2)

Count 19: Aggravated Identity Theft
(18 U.S.C. §§ 1028A and 2)

Forfeiture Notice

Filed Under Seal

DECEMBER 2012 TERM – AT ALEXANDRIA, VIRGINIA

INDICTMENT

THE GRAND JURY CHARGES THAT:

Background

At all times material to this Indictment:

1. From as early as January 2009 through as late as June 2009, defendants ANDRIY DERKACH and MIKHAIL RYTIKOV operated an on-line “dumps-checking” service whereby, for a fee, customers could check batches of stolen credit, charge, and debit card numbers

(collectively, "payment card numbers") to confirm which accounts were still active and valid so that further fraudulent transactions and charges could be made to the payment cards belonging to victims.

2. Defendant ANDRIY DERKACH [REDACTED]

[REDACTED] who controlled and operated the computer that offered the dumps-checking service (hereinafter "the dumps-checking server"¹) along with its Internet-based interface located at [REDACTED] among other Internet addresses.

3. Defendant MIKHAIL RYTIKOV [REDACTED]

[REDACTED] who hosted² and serviced the dumps-checking server for defendant ANDRIY DERKACH. Defendant RYTIKOV specialized in "bullet-proof hosting" in which he attempted to evade law enforcement detection and identification through various techniques, including: frequently changing the location of servers; erasing their contents on short notice; using false information to register and lease servers; discouraging Internet Service Providers from disconnecting servers suspected of illegal activity; and locating servers in countries where law enforcement is less likely to interfere with them. At all times relevant to this Indictment, defendant RYTIKOV provided defendant DERKACH with technical support services and advice in relation to the administration and maintenance of the dumps-checking server.

4. From as early as January 2009 through as late as June 2009, defendants ANDRIY DERKACH and MIKHAIL RYTIKOV used the dumps-checking server to check and to store approximately 1,800,000 unique payment card numbers along with victim cardholders' personal

¹ A server is a computer that offers content or a service via the Internet.

² Internet hosting is the business of providing hardware, such as servers, and software for the hosting of Internet sites.

identifying information and addresses, including those of victims residing in the Eastern District of Virginia. These payment card numbers belonged to cards branded with the Visa, MasterCard International Incorporated (“MasterCard”), American Express Company (“American Express”), and Discover Bank credit card logos, and issued by other United States financial institutions and entities including Capital One Bank, headquartered in McLean, Virginia, in the Eastern District of Virginia. To date, fraud losses attributable to the American Express payment card numbers checked and stored by the dumps-checking server have exceeded \$12,000,000.

5. The dumps-checking server contained over 580,000 MasterCard payment card numbers.

6. The dumps-checking server contained over 1,000,000 Visa payment card numbers.

COUNT ONE

7. The factual allegations in Paragraphs 1 through 6 are re-alleged and incorporated here.

The Scheme and Artifice to Defraud

8. From as early as January 2009 through as late as June 2009, in the Eastern District of Virginia and elsewhere, the defendants,

**ANDRIY DERKACH and
MIKHAIL RYTIKOV,**

together with others known and unknown to the Grand Jury, did knowingly conspire to devise and intend to devise a scheme and artifice to defraud, and for obtaining money and property, such scheme affecting a financial institution, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, that is, to knowingly cause computer commands to be transmitted from outside of the Commonwealth of Virginia to computers in the Eastern District of Virginia, in violation of Title 18, United States Code, Section 1343.

Manner and Means

It was part of the scheme that:

9. In a normal payment card transaction, the following steps typically take place:
 - a. When a customer presents a payment card to a merchant for payment of goods or services (or enters such payment card information online), the merchant's computer system transmits information by wire, including the customer's payment card information, the

merchant's identity as represented by a unique merchant ID, and other transaction details to a payment gateway.

b. The payment gateway facilitates the passing of payment card information between merchants and payment processors, checks whether a payment card is still valid and active, and whether funds available to the customer can cover the transaction. During this process, the payment gateway queries various entities, including payment processors, credit card networks, and financial institutions issuing payment cards.

c. As a result of these queries, the payment gateway determines, for example, whether a transaction based on the payment card has been approved or declined, whether the payment card is still valid and active, whether it has sufficient or insufficient funds available, and whether it has expired, or has been reported lost or stolen.

d. The payment gateway transmits this response information back to the merchant's computer system by wire.

e. In a typical transaction, once a merchant's computer system has received the response information, and assuming the transaction has been approved, funds are then wired from the customer's account to the merchant's account through the payment processor. It is this response information from the payment gateway, describing the status of the payment card, which defendants ANDRIY DERKACH and MIKHAIL RYTIKOV fraudulently obtained and sold to their customers in furtherance of additional fraudulent payment card transactions.

10. Defendant ANDRIY DERKACH publicized the dumps-checking services in online advertisements for the Internet-based interface located at [REDACTED] and other Internet addresses. For example, defendant DERKACH posted on an online forum frequented by individuals and groups engaged in large-scale identity theft and payment-card related fraud

the following message indicating that he was willing to bulk-check the validity of hundreds or thousands of payment cards at a time:

[REDACTED]

11. Dumps-checking – checking whether a payment card number is still valid – is important to individuals intending to engage in fraud. An active and valid payment card number belonging to a victim can be used to obtain money, goods, and services, while a payment card number that has been reported lost, stolen, or compromised, has likely been blocked from further transactions, and subsequent attempts to use it may attract the attention of law enforcement.

12. Defendant ANDRIY DERKACH leased the dumps-checking server from defendant MIKHAIL RYTIKOV. To do so, and at all times material to this Indictment, defendants DERKACH and RYTIKOV communicated among other means through a server located in the Eastern District of Virginia and belonging to ICQ, an instant messaging service of America Online, Inc., to coordinate and execute their scheme.

13. Through ICQ, defendants ANDRIY DERKACH and MIKHAIL RYTIKOV discussed how this dumps-checking server could evade detection by law enforcement and others. For example, on or about January 17, 2009, defendants DERKACH [REDACTED] and RYTIKOV [REDACTED] discussed their potential exposure:

[REDACTED]: are you saying that there will be few abuse complaints for sure?
[REDACTED]: yes ... I've been keeping it on hqhoste for 3 years
Not one complaint about abuse
And SpamHaus³ hasn't said anything at all :-)

[REDACTED]: okay
[REDACTED]: you'll have the server today
[REDACTED]: okay
[REDACTED]: it will be in England according to WHOIS

³ SpamHaus is an international nonprofit organization focused on tracking spam and cybercrime.

okay
is it really true what you said that there will be few abuse complaints
because
we have many networks
for completely different tasks
less stable and more abusive
or vice-versa)
bottom line, I think you understand
but this is all in one building)

...
I understand, okay.
so we will accommodate any project of yours)
if you need

...
and by the way so that you know
Unlike other vendors, our colleagues/competitors – we do not give you a
server that we have re-purchased somewhere in a data-center and don't
even put at the co-location.
We have all our own stuff – from the building to optics, in other words
you are getting the service from the primary vendor.
I think that this is also important to some extent.

I see.
in other words, what does everyone usually do? They get a server from
hosters in China, come to an agreement that they will keep the abuse
complaints, and sell these servers to the end clients; one break in the chain
and that's it... nothing works for anyone.)

14. At all times material to this Indictment, the dumps-checking server was located outside the Commonwealth of Virginia.

15. Once customers used the Internet-based interface located at [REDACTED] to upload payment card numbers to the dumps-checking server, defendant ANDRIY DERKACH caused these payment card numbers to be transmitted by wire to payment gateways located in the United States in Florida, Illinois, New Hampshire, and Ohio, to query the status of the payment card numbers. To hide that the requests were actually coming from the dumps-checking server, defendant DERKACH paired the stolen payment card numbers uploaded by customers together with unique merchant IDs he had fraudulently obtained. Defendant DERKACH then sometimes

caused the requests to be routed first through proxy servers⁴ before reaching the payment gateways.

16. Defendant ANDRIY DERKACH's dumps-checking server, in processing queries, connected to various computers and computer systems in the United States, including computer systems owned by Visa Inc., located in Ashburn, Virginia, in the Eastern District of Virginia.

17. Once the payment gateways checked whether victims' payment card numbers were valid, the results of these checks were sent back to a file on the dumps-checking server for storage and use by defendant ANDRIY DERKACH's customers.

18. Because of the illegal nature of their scheme, it was necessary for defendants ANDRIY DERKACH and MIKHAIL RYTIKOV to cooperate and frequently communicate about potential threats to the dumps-checking server, and how to resolve them. For example, on or about February 17, 2009, defendants DERKACH [REDACTED] and RYTIKOV [REDACTED] discussed how to resolve an abuse complaint lodged due to the dumps-checking activity on the server:

[REDACTED]: hi
[REDACTED]: are you there?
[REDACTED]: hi
[REDACTED]: for your information
[REDACTED]: Hello [REDACTED]. We have been notified of the following credit card collection bot site which resolves to a [REDACTED] IP address. This IP address [REDACTED] will be filtered in accordance with the Level 3 Communications Acceptable Use Policy. . . so this is why your IP doesn't work
[REDACTED]: it was LEVEL3 filtered
[REDACTED]: I see well that means we have to turn off the domain
[REDACTED]: these abuse complaints aren't good because the upstream provider is writing to our provider
[REDACTED]: first abuse complaint in 3 years
[REDACTED]: But what a complaint)
[REDACTED]: it looks like it's time to pay there

⁴ A proxy server sits between the server that actually offers the content or service, and the end-user. Proxy servers can be used to, among other things, conceal the location of the actual server.

...
[REDACTED]: how much time is there to change the domain, do you know?
[REDACTED]: I sent the money
[REDACTED]: well a couple of days. Then you'll have to write something to Level3
[REDACTED]: okay

...
[REDACTED]: and because of this, your IP isn't working properly)
[REDACTED]: and can this Level3 sniff traffic?
[REDACTED]: no it can't
[REDACTED]: Level3 is one of the uplinks
[REDACTED]: it is not in [REDACTED]
[REDACTED]: it's in Europe
[REDACTED]: the junction point is in Frankfurt
[REDACTED]: I see. But why didn't they just shut down the domain but blocked the IP
[REDACTED]: like that? It's easier to take down the domain after all
[REDACTED]: well that's the Americans for you))
[REDACTED]: [p
[REDACTED]: who the f*** knows
[REDACTED]: it was the Americans who wrote?
[REDACTED]: well Level3 is an American tier1 provider
[REDACTED]: global
[REDACTED]: I see

(All in violation of Title 18, United States Code, Section 1349.)

COUNTS TWO THROUGH TEN

(Wire Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

19. The factual allegations in Paragraphs 1 through 6 and 9 through 18 are re-alleged and incorporated here.

20. Each of the wire communications set forth below occurred between the dumps-checking server and other computers located outside the Commonwealth of Virginia, and servers belonging to Visa Inc. and America Online, Inc., located in the Eastern District of Virginia.

21. On or about each of the instances set forth below, each instance constituting a separate count, in the Eastern District of Virginia and elsewhere, the defendants,

**ANDRIY DERKACH and
MIKHAIL RYTIKOV,**

having intentionally devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property, such scheme affecting a financial institution, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, knowingly transmitted and caused to be transmitted, by means of wire communication in interstate and foreign commerce, the following writings, signs, signals, pictures, and sounds:

Count	Date	Description
2	1/16/2009	Wire transmission from dumps-checking server confirming validity of Visa payment card ending in 8575
3	1/17/2009	Connect to ICQ server for chat conversation confirming that "there will be few abuse complaints for sure?"
4	2/1/2009	Wire transmission from dumps-checking server confirming validity of Visa payment card ending in 8059
5	2/17/2009	Connect to ICQ server to discuss complaint about dumps-checking server calling it a "credit card collection bot site"
6	2/20/2009	Wire transmission from dumps-checking server confirming validity of

		Visa payment card ending in 4268
7	3/6/2009	Wire transmission from dumps-checking server confirming validity of Visa payment card ending in 5842
8	5/13/2009	Wire transmission from dumps-checking server confirming validity of Visa payment card ending in 7554
9	6/15/2009	Wire transmission from dumps-checking server confirming validity of Visa payment card ending in 9546
10	6/23/2009	Wire transmission from dumps-checking server confirming validity of Visa payment card ending in 7275 issued by Capital One Bank

(All in violation of Title 18, United States Code, Sections 1343 and 2.)

COUNT ELEVEN

(Possession of Fifteen or More Unauthorized Access Devices)

THE GRAND JURY FURTHER CHARGES THAT:

22. The factual allegations in Paragraphs 1 through 6 and 9 through 18 are re-alleged and incorporated here.

23. On or about June 24, 2009, in the Eastern District of Virginia and elsewhere, the defendant,

ANDRIY DERKACH,

knowingly and with intent to defraud, possessed fifteen or more unauthorized access devices, to wit: approximately 1,800,000 unauthorized access devices, including access devices issued by Capital One Bank, headquartered in McLean, Virginia, in the Eastern District of Virginia, and access devices belonging to payment cardholder victims residing in the Eastern District of Virginia, said possession affecting interstate and foreign commerce, in that, among other things, international wire communications were used to facilitate defendant DERKACH's possession of the access devices.

(All in violation of Title 18, United States Code, Sections 1029(a)(3) and (c)(1)(a)(i) and 2.)

COUNTS TWELVE THROUGH EIGHTEEN

(Accessing Protected Computer in Furtherance of Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

24. The factual allegations in Paragraphs 1 through 6 and 9 through 18 are re-alleged and incorporated here.

25. At all times material to this Indictment, Visa Inc. maintained a data center comprised of thousands of servers in Ashburn, Virginia, in the Eastern District of Virginia, that allowed merchants with a merchant ID to determine electronically the validity of payment cards branded with the Visa logo.

26. Defendant ANDRIY DERKACH used stolen merchant IDs to access the Visa servers without authorization.

27. On or about each of the instances set forth below, each instance constituting a separate count, in the Eastern District of Virginia and elsewhere, the defendant,

ANDRIY DERKACH,

knowingly and with intent to defraud, accessed the Visa servers without authorization, and by means of such conduct furthered the intended fraud and obtained something of value, to wit: information regarding the status and validity of payment cards:

Count	Approximate Date	Defendant's Access
12	1/14/2009	Validity of Visa payment card number ending in 0763
13	1/15/2009	Validity of Visa payment card number ending in 3925
14	1/16/2009	Validity of Visa payment card number ending in 1450
15	1/17/2009	Validity of Visa payment card number ending in 4035
16	4/30/2009	Validity of Visa payment card number ending in 9646
17	5/1/2009	Validity of Visa payment card number ending in 8205
18	6/23/2009	Validity of Capital One Bank-issued Visa payment card number ending in 5693

(All in violation of Title 18, United States Code, Sections 1030(a)(4), (c)(3)(A) and 2.)

COUNT NINETEEN

(Aggravated Identity Theft)

THE GRAND JURY FURTHER CHARGES THAT:

28. The factual allegations in Paragraphs 1 through 6 and 9 through 18 are re-alleged and incorporated here.

29. On or about January 16, 2009, in the Eastern District of Virginia and elsewhere, the defendants,

**ANDRIY DERKACH and
MIKHAIL RYTIKOV,**

did knowingly transfer, possess, and use, without lawful authority, means of identification of another person, that is, the payment card information of another person, including but not limited to a Visa payment card number ending in 8575, during and in relation to a conspiracy to commit wire fraud and wire fraud, as alleged in Counts 1 and 2, in violation of Title 18, United States Code, Sections 1349 and 1343.

(All in violation of Title 18, United States Code, Sections 1028A(a)(1), (c)(5), and 2.)

NOTICE OF FORFEITURE

1. Upon conviction of the offenses in violation of Title 18, United States Code, Sections 1349 and 1343, set forth in Counts One through Ten of this Indictment, the defendants,

**ANDRIY DERKACH and
MIKHAIL RYTIKOV,**

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 982(a)(2)(A) and Title 28, United States Code, Section 2461(c), any property, real or personal, constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violations. Specifically, the United States seeks a sum of money equal to at least \$12,000,000 in United States currency, representing the amount of proceeds obtained as a result of such violations.

2. Upon conviction of the offenses in violation of Title 18, United States Code, Sections 1029 and 1030, set forth in Counts Eleven through Eighteen of this Indictment, the defendant,

ANDRIY DERKACH,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(B), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violations; and pursuant to Title 18, United States Code, Sections 1029(c)(1)(C) and 1030(i)(1)(A), any personal property used or intended to be used to commit the offenses. Specifically, the United States seeks a sum of money equal to at least \$12,000,000 in United States currency, representing the amount of proceeds obtained as a result of such violations.

3. If any of the property described above as being forfeitable pursuant to Title 18, United States Code, Sections 982(a)(2)(A); 982(a)(2)(B); 1030(i); and Title 28, United States Code, Section 2461(c), 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 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 divided without difficulty;

it is the intention of the United States of America, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c); Title 18, United States Code, Section 982(b)(1) and 1029(c)(2), and Title 18, United States Code, Section 1030(i)(2), to seek forfeiture of all other property of the defendant up to the value of the property described in paragraphs 1 and 2 above, including but not limited to the following substitute assets:

- a. \$12,000,000 in United States dollars;
- b. Interest in real property located at [REDACTED];
- c. Interest in real property located at [REDACTED];
- d. Interest in real property located at [REDACTED];
- e. Bank of [REDACTED], Account No. ending in 0603, in the name of ANDRIY DERKACH;
- f. Bank of [REDACTED], Account associated with payment card ending in 3661, in the name of ANDRIY DERKACH;
- g. Bank of [REDACTED], Account associated with payment card ending in 8161, in the name of ANDRIY DERKACH;

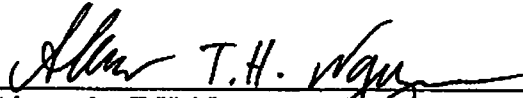
- h. Bank of [REDACTED] Account No. ending in 4882, and associated with Bank Transit No. 83162 and Institution No. 002, in the name of ANDRIY DERKACH;
- i. Bank of [REDACTED], Account associated with payment card ending in 3016, in the name of ANDRIY DERKACH;
- j. TD [REDACTED] Trust, Account No. ending in 2413, in the name of ANDRIY DERKACH;
- k. PayPal Inc., Accounts belonging to ANDRIY DERKACH and associated with [REDACTED] and [REDACTED];
- l. WebMoney, Accounts associated with ID [REDACTED] and ID [REDACTED];
- m. Porsche Cayenne, black;
- n. Porsche 911, black;
- o. The following domain names: [REDACTED]

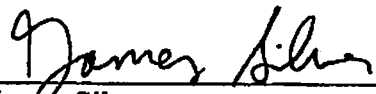
(All pursuant to 18 U.S.C. §§ 982(a)(2)(A); 982(a)(2)(B); 1029(c)(1)(C), and 1030(i), and 28 U.S.C. § 2461(c).)

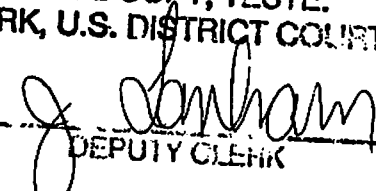
A TRUE BILL:
 Pursuant to the E-Government Act,
 the original of this page has been filed
 under seal at the Clerk's Office.

 Foreperson of the Grand Jury

NEIL H. MacBRIDE
 UNITED STATES ATTORNEY


 Alexander T.H. Nguyen
 Assistant United States Attorney


 James Silver
 Trial Attorney, U.S. Department of Justice
 Computer Crime & Intellectual Property Section

A TRUE COPY, TESTE:
 CLERK, U.S. DISTRICT COURT
 BY 
 DEPUTY CLERK