

*copy*

UNITED STATES DISTRICT COURT

**UNDER SEAL**

for the

Northern District of California

United States of America

v.

DANIL POTEKHIN, a/k/a "crouswar," and DMITRII  
KARSAVIDI, a/k/a Dmitriy Karasavidi

Case No. CR-19-0572-CRB

RECEIVED  
UNITED STATES MARSHAL  
2020 FEB 19 AM 9:37  
NORTHERN DISTRICT  
OF CALIFORNIA

*Defendant*

**ARREST WARRANT**

To: Any authorized law enforcement officer

**YOU ARE COMMANDED** to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) DMITRII KARSAVIDI

who is accused of an offense or violation based on the following document filed with the court:

- Indictment       Superseding Indictment       Information       Superseding Information       Complaint
- Probation Violation Petition       Supervised Release Violation Petition       Violation Notice       Order of the Court

This offense is briefly described as follows:

Defendants are charged with a number of counts associated with a sophisticated phishing campaign targeting users of Poloniex and Binance's virtual currency exchanges, resulting in a loss of at least \$15.7 million worth of cryptocurrency, and the subsequent money laundering of the proceeds of the fraud.

Date: 2/18/2020

**JOSEPH C. SPERO**  
**UNITED STATES MAGISTRATE JUDGE**

*Issuing officer's signature*

City and state: SF, CA

*Chief US Magistrate Judge Spero*  
*Printed name and title*

**Return**

This warrant was received on (date) \_\_\_\_\_, and the person was arrested on (date) \_\_\_\_\_  
at (city and state) \_\_\_\_\_.

Date: \_\_\_\_\_

*Arresting officer's signature*

*Printed name and title*

Copy

UNITED STATES DISTRICT COURT **UNDER SEAL**

for the  
Northern District of California

United States of America  
v.

DANIL POTEKHIN, a/k/a "crouswar," and DMITRII  
KARASAVIDI, a/k/a Dmitriy Karasavidi

Case No. CR-19-0572-CRB

Defendant

**ARREST WARRANT**

To: Any authorized law enforcement officer

**YOU ARE COMMANDED** to arrest and bring before a United States magistrate judge without unnecessary delay  
(name of person to be arrested) DANIL POTEKHIN,  
who is accused of an offense or violation based on the following document filed with the court:

- Indictment
- Superseding Indictment
- Information
- Superseding Information
- Complaint
- Probation Violation Petition
- Supervised Release Violation Petition
- Violation Notice
- Order of the Court

This offense is briefly described as follows:

Defendants are charged with a number of counts associated with a sophisticated phishing campaign targeting users of Poloniex and Binance's virtual currency exchanges, resulting in a loss of at least \$15.7 million worth of cryptocurrency, and the subsequent money laundering of the proceeds of the fraud.

Date: 2/18/2020

JOSEPH C. SPERO  
**UNITED STATES MAGISTRATE JUDGE**  
Issuing officer's signature

City and state: SF, CA

Chief US Magistrate Judge Spero  
Printed name and title

**Return**

This warrant was received on (date) \_\_\_\_\_, and the person was arrested on (date) \_\_\_\_\_  
at (city and state) \_\_\_\_\_.

Date: \_\_\_\_\_

Arresting officer's signature

Printed name and title

RECEIVED  
UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
2020 FEB 19 AM 9:30

United States District Court

FOR THE  
NORTHERN DISTRICT OF CALIFORNIA

UNDER SEAL

VENUE: SAN FRANCISCO

UNITED STATES OF AMERICA,

V.

FILED

FEB 18 2020

SUSAN Y. SOONG  
CLERK, U.S. DISTRICT COURT  
NORTH DISTRICT OF CALIFORNIA

DANIL POTEKHIN, a/k/a "crouswar," and  
DMITRII KARASAVIDI, a/k/a Dmitriy  
Karasavidi

DEFENDANT(S).

**SUPERSEDING INDICTMENT**

18 U.S.C. § 1030(b) – Conspiracy to Commit Computer Fraud & Abuse;  
18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a  
Protected Computer To Obtain Value;  
18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud;  
18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft;  
18 U.S.C. § 1956(h) – Money Laundering Conspiracy;  
18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j), and 981(a)(1)(C) and  
28 U.S.C. § 2461(c) – Forfeiture Allegations



*True Bill*

A true bill.

*[Signature]*  
Foreman

Filed in open court this 18 day of

*February 2020*

*[Signature]*

KAREN L. BOB

JOSEPH C. SPERO Clerk

UNITED STATES MAGISTRATE JUDGE

Bail, \$ no bailment warrants

**DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT**

BY:  COMPLAINT  INFORMATION  INDICTMENT  
 SUPERSEDING

**OFFENSE CHARGED**

PLEASE SEE ATTACHMENT

- Petty
- Minor
- Misdemeanor
- Felony

PENALTY: PLEASE SEE ATTACHMENT

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

**FILED**  
FEB 18 2020

DEFENDANT - U.S.

DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi

DISTRICT COURT NUMBER  
CR-19-0572-CRB

SUSAN Y. SOONG  
CLERK, U.S. DISTRICT COURT  
NORTH DISTRICT OF CALIFORNIA

**UNDER SEAL**

**PROCEEDING**

Name of Complainant Agency, or Person (& Title, if any)

USSS

person is awaiting trial in another Federal or State Court, give name of court

this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

this is a reprosecution of charges previously dismissed which were dismissed on motion of:

U.S. ATTORNEY  DEFENSE

SHOW DOCKET NO.

this prosecution relates to a pending case involving this same defendant

MAGISTRATE CASE NO.

prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person  
Furnishing Information on this form DAVID L. ANDERSON

U.S. Attorney  Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) Cynthia Frey, AUSA, Tax Div.

**DEFENDANT**

**IS NOT IN CUSTODY**

Has not been arrested, pending outcome this proceeding.

1)  If not detained give date any prior summons was served on above charges

2)  Is a Fugitive

3)  Is on Bail or Release from (show District)

**IS IN CUSTODY**

4)  On this charge

5)  On another conviction

Federal  State

6)  Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

Has detainer been filed?  Yes  No

If "Yes" give date filed

DATE OF ARREST

Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY

Month/Day/Year

This report amends AO 257 previously submitted

**ADDITIONAL INFORMATION OR COMMENTS**

**PROCESS:**

SUMMONS  NO PROCESS\*  WARRANT

Bail Amount: \_\_\_\_\_

If Summons, complete following:

Arraignment  Initial Appearance

Defendant Address:

\* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Date/Time: \_\_\_\_\_ Before Judge: \_\_\_\_\_

Comments:

**UNDER SEAL FILED**

**PENALTY SHEET ATTACHMENT:  
DMITRII KARSAVIDI**

**FEB 18 2020**

SUSAN Y. SOONG  
CLERK, U.S. DISTRICT COURT  
NORTH DISTRICT OF CALIFORNIA

**Count 1:** 18 U.S.C. § 1030(b) – Conspiracy to Commit Computer Fraud and Abuse  
**Maximum Penalties:** (1) 10 years imprisonment; (2) Maximum of 3 years of supervised release; (3) \$250,000 fine or twice the gross gain or twice the gross loss; (4) \$100 Special Assessment

**Count 2:** 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer To Obtain Value;  
**Maximum Penalties:** (1) 5 years imprisonment; (2) Maximum of 3 years of supervised release; (3) \$250,000 fine or twice the gross gain or twice the gross loss; (4) \$100 Special Assessment

**Count 3:** 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud  
**Maximum Penalties:** (1) 20 years imprisonment; (2) Maximum of 3 years of supervised release; (3) \$250,000 fine or twice the gross gain or twice the gross loss; (4) \$100 Special Assessment

**Counts 4 & 5:** 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft  
**Maximum Penalties:** (1) 2 years imprisonment (to run consecutive to any other term imposed); (2) Maximum of 3 years of supervised release; (3) \$250,000 fine or twice the gross gain or twice the gross loss; (4) \$100 Special Assessment

**Count 6:** 18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering  
**Maximum Penalties:** (1) 20 years imprisonment; (2) Maximum of 3 years of supervised release; (3) \$250,000 fine or twice the gross gain or twice the gross loss; (4) \$100 Special Assessment

**DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT**

BY:  COMPLAINT  INFORMATION  INDICTMENT  
 SUPERSEDING

**OFFENSE CHARGED**

PLEASE SEE ATTACHMENT

- Petty
- Minor
- Misdemeanor
- Felony

PENALTY: PLEASE SEE ATTACHMENT

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

DEFENDANT - U.S.

**FILED**

▶ DANIL POTEKHIN, a/k/a "crounswar"

**FEB 16 2020**

DISTRICT COURT NUMBER  
CR-19-0572-CRB

SUSAN Y. SOONG  
CLERK, U.S. DISTRICT COURT  
NORTH DISTRICT OF CALIFORNIA

**PROCEEDING**

Name of Complainant Agency, or Person (& Title, if any)

USSS

person is awaiting trial in another Federal or State Court, give name of court

this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

this is a re prosecution of charges previously dismissed which were dismissed on motion of:  
 U.S. ATTORNEY  DEFENSE

SHOW DOCKET NO.

this prosecution relates to a pending case involving this same defendant

MAGISTRATE CASE NO.

prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person Furnishing Information on this form DAVID L. ANDERSON

U.S. Attorney  Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) Cynthia Frey, AUSA, Tax Div.

**DEFENDANT**

**IS NOT IN CUSTODY**

Has not been arrested, pending outcome this proceeding.

- 1)  If not detained give date any prior summons was served on above charges ▶
- 2)  Is a Fugitive
- 3)  Is on Bail or Release from (show District)

**UNDER SEAL**

**IS IN CUSTODY**

- 4)  On this charge
- 5)  On another conviction }  Federal  State
- 6)  Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

Has detainer been filed?  Yes  No

If "Yes" give date filed

DATE OF ARREST ▶ Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY ▶ Month/Day/Year

This report amends AO 257 previously submitted

**ADDITIONAL INFORMATION OR COMMENTS**

**PROCESS:**

SUMMONS  NO PROCESS\*  WARRANT

Bail Amount: \_\_\_\_\_

If Summons, complete following:

Arraignment  Initial Appearance

\* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Defendant Address:

\_\_\_\_\_ Date/Time: \_\_\_\_\_ Before Judge: \_\_\_\_\_

Comments:

PENALTY SHEET ATTACHMENT  
DANIL POTEKHIN

**UNDER SEAL**

**Count 1:** 18 U.S.C. § 1030(b) – Conspiracy to Commit Computer Fraud and Abuse

**Maximum Penalties:** (1) 10 years imprisonment; (2) Maximum of 3 years of supervised release; (3) \$250,000 fine or twice the gross gain or twice the gross loss; (4) \$100 Special Assessment

**Count 2:** 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) – Unauthorized Access to a Protected Computer To Obtain Value;

**Maximum Penalties:** (1) 5 years imprisonment; (2) Maximum of 3 years of supervised release; (3) \$250,000 fine or twice the gross gain or twice the gross loss; (4) \$100 Special Assessment

**Count 3:** 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud

**Maximum Penalties:** (1) 20 years imprisonment; (2) Maximum of 3 years of supervised release; (3) \$250,000 fine or twice the gross gain or twice the gross loss; (4) \$100 Special Assessment

**Counts 4 & 5:** 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft

**Maximum Penalties:** (1) 2 years imprisonment (to run consecutive to any other term imposed); (2) Maximum of 3 years of supervised release; (3) \$250,000 fine or twice the gross gain or twice the gross loss; (4) \$100 Special Assessment

**Count 6:** 18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering

**Maximum Penalties:** (1) 20 years imprisonment; (2) Maximum of 3 years of supervised release; (3) \$250,000 fine or twice the gross gain or twice the gross loss; (4) \$100 Special Assessment

**Forfeiture Allegations:** 18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and (j), and 981(a)(1)(C) and 28 U.S.C. § 2461(c)

**FILED**

**FEB 18 2020**

SUSAN Y. SOONG  
CLERK, U.S. DISTRICT COURT  
NORTH DISTRICT OF CALIFORNIA





1           3.     Poloniex, LLC (“Poloniex”) is a digital currency exchange platform based in  
2 Wilmington, Delaware.

3           4.     Bittrex is a digital currency exchange platform, based in Seattle, Washington.

4           5.     Binance is a digital currency exchange platform that was originally based in Hong Kong,  
5 China, and is currently headquartered in Malta.

6           6.     Bitfinex is a digital currency exchange platform based in the British Virgin Islands.

7           7.     Gemini Trust Company LLC (“Gemini”) is a digital currency exchange platform based in  
8 New York, New York.

9           8.     Bitcoin (“BTC”) is a form of decentralized, convertible digital currency that exists  
10 through the use of an online, decentralized ledger system, referred to as a “blockchain.” While Bitcoin  
11 mainly exists as an Internet-based form of currency, it is possible to “print out” the necessary  
12 information and exchange Bitcoin via physical medium. The currency is not issued by any government,  
13 bank, or company, but rather is generated and controlled through computer software operating via a  
14 decentralized network. Bitcoin is typically acquired by purchasing it from a Bitcoin seller or  
15 “exchanger.” It is also possible to “mine” Bitcoin by verifying other users’ transactions. Bitcoin is just  
16 one form of digital currency, and there are many other varieties of digital currency.

17          9.     Bitcoin exchangers typically accept payments in the form of fiat currency (such as  
18 dollars, euros, or other currency that derives its value from its support by governments), or other  
19 convertible digital currencies. When a user wishes to purchase Bitcoin from an exchanger, the user will  
20 typically send payment in the form of fiat currency, often via bank wire or ACH, or other convertible  
21 digital currency to an exchanger, for the corresponding quantity of Bitcoin, based on a fluctuating  
22 exchange rate. The exchanger, often for a commission, will then typically attempt to broker the  
23 purchase with another user of the exchange that is trying to sell Bitcoin, or, in some instances, will act as  
24 the seller itself. If the exchanger can place a buyer with a seller, then the transaction can be completed.

25          10.    When a user acquires Bitcoin, ownership of the Bitcoin is transferred to the user’s  
26 Bitcoin address. The Bitcoin address is somewhat analogous to a bank account number, and is  
27 comprised of a case-sensitive string of letters and numbers amounting to a total of 26 to 35 characters.  
28 The user can then conduct transactions with other Bitcoin users, by transferring Bitcoin to their Bitcoin

1 addresses, via the Internet. “Bitcoin address clustering” is a process that attempts to de-anonymize a  
2 user by identifying all of the addresses that they control.

3 11. Little to no personally identifiable information about the payer or payee is transmitted in  
4 a Bitcoin transaction itself. Bitcoin transactions occur using a public key and a private key. A public  
5 key is used to receive Bitcoin, and a private key is used to allow withdrawals from a Bitcoin address.  
6 Only the Bitcoin address of the receiving party and the sender’s private key are needed to complete the  
7 transaction. These two keys by themselves rarely reflect any identifying information.

8 12. Digital currencies, including Bitcoin, have many known legitimate uses. However, much  
9 like cash, Bitcoin can be used to facilitate illicit transactions and to launder criminal proceeds, given the  
10 ease with which Bitcoin can be used to move funds with high levels of anonymity. In some  
11 circumstances Bitcoin payments may be traced to accounts at traditional financial institutions using the  
12 blockchain.

13 13. Ethereum (“ETH”) is a digital currency that is open source, public, has a blockchain, and  
14 is distributed on a platform that uses “smart contract” technology. By definition, smart contracts are  
15 computer protocols that automatically enforce a pre-arranged negotiation between individuals  
16 conducting a transaction. These protocols are also sometimes called self-executing contracts.

17 14. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to  
18 track the movement of ETH. Smart contracts allow developers to create markets, store registries of  
19 debts, and move funds in accordance with the instructions provided without any type of middle-man or  
20 counterparty controlling a desired outcome. Smart contract technology is one of Ethereum’s main  
21 selling points and an important tool for companies or individuals executing trades on the ETH  
22 blockchain. The ETH platform allows developers to build and deploy software and decentralized  
23 applications using the blockchain protocol. The ETH blockchain protocol allows smart contracts to  
24 operate without fraud, censorship, or third-party interference.

25 15. Gnosis is a platform built as a decentralized application on the Ethereum network. GNO  
26 is the digital currency token used on the Gnosis platform.

27 16. NEO, formerly called as AntShares, is China’s first open source blockchain platform.  
28 GAS is the digital currency token used to pay the cost of execution on the NEO blockchain.

1 17. Poloniex, Binance, and Gemini are exchanges that offer their users the ability to trade  
2 digital currencies, such as BTC, ETH, GAS, and GNO via the Internet. Users of these exchanges could  
3 access their accounts with their email address and a unique password, and through this account, could  
4 store, access, move, or trade digital currency. Poloniex places transaction limitations on certain  
5 accounts. Where such limitations were in place at Poloniex, the transaction limits could be increased by  
6 linking their accounts to other accounts.

7 18. The computer servers used by Poloniex, Binance, and Gemini in operating their  
8 exchanges and user accounts were used to facilitate interstate and foreign commerce and  
9 communication, including by interstate and foreign electronic signals, and constituted “protected  
10 computers” as defined in Title 18, United States Code, Section 1030(e)(2)(B).

11 The Conspiracy and Scheme to Defraud

12 19. As part of the conspiracy and scheme to defraud, the defendants used the Internet to  
13 launch a sophisticated phishing campaign targeting users of Poloniex, Binance, and Gemini’s digital  
14 currency exchanges. The defendants purchased and deployed multiple websites that appeared to users  
15 to be the legitimate Poloniex, Binance, and Gemini digital currency exchanges. However, when users  
16 would log into these fraudulent websites, the defendants were able to steal their credentials, in the form  
17 of an email address, and their password information, enabling the defendants to control their actual  
18 Poloniex, Binance, and Gemini accounts, withdraw some or all of their digital currency, and manipulate  
19 the market for digital currency. This resulted in losses of digital currencies valued at approximately \$17  
20 million for Poloniex, Binance, and Gemini customers, including customers in the Northern District of  
21 California.

22 COUNT ONE: (18 U.S.C. § 1030(b) – Conspiracy to Commit Computer Fraud and Abuse)

23 20. Paragraphs 1 through 19 of this Indictment are re-alleged and incorporated as if fully set  
24 forth here.

25 21. Beginning at a time unknown to the Grand Jury, but no later than on or about June 8,  
26 2017, and continuing through a date unknown, but at least through on or about April 15, 2018, in the  
27 Northern District of California, and elsewhere, the defendants,

28 DANIL POTEKHIN, and  
DMITRII KARASAVIDI,

SUPERSEDING INDICTMENT

1 did knowingly and willfully conspire and agree with each other and with others, to commit computer  
2 fraud and abuse, namely, with intent to defraud, accessed a protected computer used in interstate and  
3 foreign commerce without authorization and exceeding authorized access, and by means of such conduct  
4 furthered the below-described fraud and obtained something of value, in violation of 18 U.S.C.  
5 § 1030(a)(4).

6 22. In furtherance of the conspiracy, the defendants used the following manner and means to  
7 accomplish the object and purpose of the conspiracy:

8 a. Using fraud, deception, and social engineering techniques to gain access to the  
9 user identification and passwords of victim users of the Poloniex, Binance, and Gemini exchange  
10 platforms;

11 b. Using identification of others without lawful authority, and fictitious identities to  
12 create fictitious Poloniex, Binance, Gemini, and Bittrex accounts to facilitate the fraud scheme;

13 c. Using information obtained from victim customers of the Poloniex, Binance, and  
14 Gemini exchange platforms to access their digital currency addresses and transfer cryptocurrencies  
15 owned by the victims without authority;

16 d. Using unauthorized access to victim customer Poloniex accounts to manipulate  
17 the digital currency markets and take advantage of the immediate increase in digital currency value to  
18 their benefit; and

19 e. Using multiple digital currency addresses and clusters to deposit the stolen digital  
20 currencies and using a layered process for withdrawal and deposits to conceal the nature, source,  
21 location, ownership, or control of the digital currency.

22 23. In furtherance of the conspiracy and to effect its objects, on or about the dates listed  
23 below, in the Northern District of California and elsewhere, POTEKHIN, KARASAVIDI and others,  
24 committed the following overt acts, among others:

25 *Poloniex Theft Attack*

26 a. Between on or about July 17, 2017, and at least on or about October 29, 2017,  
27 POTEKHIN created and controlled at least 13 separate fake Poloniex domains to be used in a fraud  
28 scheme targeting Poloniex and its users.

1           b.       Between on or about July 17, 2017, and at least on or about October 29, 2017,  
2 POTEKHIN induced at least 158 victim customers of the Poloniex exchange platform, including  
3 Poloniex customers in the Northern District of California, to access the fake Poloniex domains, causing  
4 the victim customers to input their user identification and passwords in order to access their Poloniex  
5 account, enabling POTEKHIN and others to obtain the customers' user identification, which is the  
6 user's email address, and passwords without authorization.

7           c.       Between on or about June 8, 2017 and July 17, 2017, POTEKHIN,  
8 KARASAVIDI, and others created five fictitious Poloniex accounts. At least three of those accounts  
9 were in the names of individuals from the United Kingdom: A.C., N.B., and C.A. To create these three  
10 accounts, the defendants fraudulently used the means of identification of A.C., N.B., and C.A.  
11 POTEKHIN and others possessed the means of identification of A.C., N.B., and C.A. prior to the  
12 creation of these fictitious accounts. KARASAVIDI also had access to one of the other fictitious  
13 Poloniex accounts.

14           d.       Between at least on or about August 3, 2017 and August 23, 2017, POTEKHIN,  
15 KARASAVIDI, and others used user identification and passwords obtained without authorization to  
16 gain access to the approximately 155 victim customer Poloniex accounts and withdraw digital currency  
17 without authorization. POTEKHIN, KARASAVIDI, and others also used some of the five fictitious  
18 accounts, described above, along with victim user identification and passwords obtained without  
19 authorization, to link to the victim user accounts, enabling them to withdraw larger sums of digital  
20 currency from victim accounts without authorization. Approximately \$700,000 in BTC was withdrawn  
21 without authorization from victim user accounts, including digital currency from T.S. and J.S., who  
22 resided in the Northern District of California, and deposited into one BTC cluster.

23           e.       Between on or about July 8, 2017 and July 15, 2017, POTEKHIN,  
24 KARASAVIDI and others created three fictitious Bittrex accounts to receive BTC from the fraud  
25 scheme. KARASAVIDI had access to one of the fictitious Bittrex accounts, registered using the email  
26 account \*\*\*\*\*659@yahoo.com, which was the same email account used to register one of  
27 the five fictitious accounts. POTEKHIN had access to the identity of one of these Bittrex accounts.

28 //

1 Between on or about August 10, 2017 and on or about September 19, 2017, approximately 435 Bitcoins  
2 were sent from the Bitcoin cluster to these three fictitious Bittrex accounts.

3 f. Between on or about August 13, 2017 and on or about September 27, 2017, most  
4 of the BTC from the three fictitious Bittrex accounts, including one account also in the name of A.C.,  
5 was converted to approximately 8,816 ETH and through a sophisticated and layered manner was sent  
6 through multiple intermediary accounts, before ultimately being deposited into a Bitfinex account  
7 controlled by KARASAVIDI.

8 *Poloniex Manipulation Attack*

9 g. Between on or about July 18, 2017 and on or about August 13, 2017, POTEKHIN  
10 and others created nine more fictitious Poloniex accounts, each of which provided a residence in  
11 Ukraine or Russia. Eight of those fictitious accounts purchased 300 GAS at relatively low prices (the  
12 “Eight Fictitious Poloniex Accounts”). One of these eight accounts was controlled by POTEKHIN.  
13 One of the eight accounts also purchased GNO. These Eight Fictitious Poloniex Accounts were then  
14 used in a manipulation attack targeting three victim Poloniex customer accounts, with a total holdings of  
15 approximately \$5,243,000 worth of digital currency on or about October 29, 2017.

16 h. Using the same phishing means set forth above, POTEKHIN and others  
17 unlawfully and without authorization obtained the user identification and passwords for these three  
18 victim accounts. On or about October 29, 2017, POTEKHIN and others unlawfully and without  
19 authorization obtained access to the victim accounts. Using digital currency in one victim Poloniex  
20 account, they placed an order to purchase approximately 8,000 GAS, thereby immediately increasing the  
21 market price of GAS from approximately \$18 to \$2,400. POTEKHIN and others then converted the  
22 artificially inflated GAS in their own fictitious Poloniex accounts into ETH and BTC. Using digital  
23 currency in the other two victim Poloniex accounts, POTEKHIN and others purchased GNO. The total  
24 digital currency contained in the Eight Fictitious Poloniex Accounts on October 30, 2017, when  
25 Poloniex froze the accounts, was approximately 15,600 ETH and .16 BTC. Before the Eight Fictitious  
26 Poloniex Accounts were frozen, POTEKHIN and others transferred approximately 759 ETH to nine  
27 digital currency addresses. Through a sophisticated and layered manner, the ETH from these nine

28 //

1 digital currency addresses was sent through multiple intermediary accounts, before ultimately being  
2 deposited into a Bitfinex account controlled by KARASAVIDI.

3 *Binance Theft Attack*

4 i. Between on or about October 16, 2017 and October 31, 2017, POTEKHIN and  
5 others created at least two fictitious Binance accounts using the email accounts of two individuals from  
6 the United Kingdom. POTEKHIN and others possessed the email accounts of these individuals prior to  
7 the creation of these fictitious accounts.

8 j. Between at least on or about at least December 19, 2017, until on or about March  
9 2, 2018, POTEKHIN, KARASAVIDI, and others induced at least 142 victim customers of the Binance  
10 exchange platform, including at least one Binance customer in the Northern District of California, to  
11 access the fake Binance domains, causing the victim customers to input their user identification and  
12 passwords in order to access their Binance account, enabling POTEKHIN and others to obtain the  
13 customers' user identification, which is the user's email address, and passwords without authorization.

14 k. POTEKHIN, KARASAVIDI, and others used the user identification and  
15 passwords obtained without authorization to gain access to approximately 142 victim customer Binance  
16 accounts and withdraw digital currency without authorization. Approximately 566 BTC, with a value of  
17 over \$10 million BTC (valued on December 19, 2017), was withdrawn without authorization, including  
18 digital currency from one victim in the Northern District of California, and deposited into one BTC  
19 cluster, as well as several other intermediary digital currency addresses. BTC from the cluster, as well  
20 as from several other intermediary digital currency addresses, was then deposited into the two fictitious  
21 Binance accounts described above before ultimately being deposited into a Bitfinex account controlled  
22 by KARASAVIDI.

23 *Gemini Theft Attack*

24 l. Between on or about October 24, 2017, and November 1, 2017, POTEKHIN,  
25 KARASAVIDI, and others induced at least 42 victim customers of the Gemini exchange platform,  
26 including at least one Gemini customer in the Northern District of California, to access the fake Gemini  
27 domains. The victim customers input their user identification and passwords, believing they were  
28 accessing their Gemini accounts instead of the fake Gemini domains. In this manner, POTEKHIN and

1 others obtained the customers' user identification, which was the users' email address, and passwords  
2 without authorization.

3 m. POTEKHIN, KARASAVIDI, and others used the user identification and  
4 passwords obtained without authorization to gain access to victim customer Gemini accounts and  
5 withdraw digital currency without authorization. Approximately \$1.176 million in United States dollars  
6 and digital currencies, was withdrawn without authorization from these accounts, including digital  
7 currency from one victim in the Northern District of California. The valuation of the digital currencies  
8 was based upon the average value between October 24, 2017 and November 1, 2017. Some of the  
9 stolen digital currency was intermingled with funds obtained by the co-conspirators in the Poloniex  
10 Market Manipulation Attack. Together, those funds then were moved through several intermediary  
11 digital currency addresses before being deposited into a Bitfinex account controlled by KARASAVIDI.  
12 Still other digital currency that was stolen from the victim Gemini accounts was deposited into a  
13 Binance account that had also received digital currency from the Binance Theft Attack, before it was  
14 ultimately deposited into a Bitfinex account controlled by KARASAVIDI.

15 *Money Laundering from the Poloniex, Binance, and Gemini Attacks*

16 n. In total, at least \$16,876,000 in digital and fiat currency was reported stolen in the  
17 Poloniex, Binance, and Gemini Attacks, which was obtained through the above described fraud scheme  
18 by the co-conspirators. These fraud proceeds were then moved through various accounts, in an effort by  
19 the co-conspirators to promote the fraud and to conceal and disguise the nature, source, ownership, and  
20 control of the funds. Specifically, the digital currency from the Poloniex Manipulation Attack was  
21 intermingled with the digital currency from the Poloniex Theft Attack, as well as digital and fiat  
22 currencies from the Binance Theft Attack and the Gemini Theft Attack. Through a sophisticated and  
23 layered manner, these fraud proceeds were sent through multiple intermediary accounts, before  
24 approximately 19,600 ETH was ultimately deposited on March 11, 2018, March 18, 2018, April 9, 2018,  
25 and April 15, 2018 into a Bitfinex account controlled by KARASAVIDI.

26 All in violation of Title 18, United States Code, Section 1030(b).

27 //

28 //



1 COUNT TWO: (18 U.S.C. § 1030(a)(4) – Computer Fraud)

2 24. Paragraphs 1 through 23 of this Indictment are re-alleged and incorporated as if fully set  
3 forth here.

4 25. On or about June 8, 2017, and continuing through a date unknown, but at least through on  
5 or about April 15, 2018, within the Northern District of California and elsewhere, the defendants,

6 DANIL POTEKHIN, and  
7 DMITRII KARASAVIDI,

8 knowingly and with intent to defraud accessed a protected computer used in interstate and foreign  
9 commerce without authorization and exceeding authorized access, and by means of such conduct  
10 furthered the intended fraud and obtained something of value, specifically digital currency addresses and  
11 passkeys, containing digital currency later withdrawn without authorization by defendants.

12 All in violation of 18 U.S.C. Sections 1030(a)(4) and (c)(3)(A).

13  
14 COUNT THREE: (18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud)

15 26. Paragraphs 1 through 23 of this Indictment are re-alleged and incorporated as if fully set  
16 forth here.

17 27. Beginning at a time unknown to the Grand Jury, but no later than on or about June 8,  
18 2017, and continuing through a date unknown, but at least through on or about April 15, 2018, in the  
19 Northern District of California and elsewhere, the defendants,

20 DANIL POTEKHIN, and  
21 DMITRII KARASAVIDI,

22 and others, did knowingly conspire to devise and intend to devise a scheme and artifice to defraud as to  
23 a material matter and to obtain money and property by means of materially false and fraudulent  
24 pretenses, representations, and promises, and by concealment of material facts, and, for the purpose of  
25 executing such scheme or artifice and attempting to do so, did transmit, and cause to be transmitted, by  
26 means of wire communication in interstate and foreign commerce, certain writings, signs, signals,  
27 pictures, and sounds, in violation of Title 18, United States Code, Section 1343.

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

1 COUNT FOUR: (18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft)

2 28. Paragraphs 1 through 27 of this Indictment are re-alleged and incorporated as if fully set  
3 forth here.

4 29. Between on or about June 8, 2017 and August 23, 2017, in the Northern District of  
5 California and elsewhere, the defendants,

6 DANIL POTEKHIN, and  
7 DMITRII KARASAVIDI,

8 during and in relation to the crime of Conspiracy to Commit Computer Fraud and Abuse, in violation of  
9 18 U.S.C. § 1030(b); Computer Fraud, in violation of 18 U.S.C. § 1030(a)(4); and Conspiracy to  
10 Commit Wire Fraud, in violation of 18 U.S.C. § 1349, did knowingly transfer, possess, and use, without  
11 lawful authority the means of identification of another person, to wit, the username and password of T.S.

12 All in violation of Title 18, United States Code, Section 1028A(a)(1).  
13

14 COUNT FIVE: (18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft)

15 30. Paragraphs 1 through 27 of this Indictment are re-alleged and incorporated as if fully set  
16 forth here.

17 31. Between on or about June 8, 2017 and August 23, 2017, in the Northern District of  
18 California and elsewhere, the defendants,

19 DANIL POTEKHIN, and  
20 DMITRII KARASAVIDI,

21 during and in relation to the crime of Conspiracy to Commit Computer Fraud and Abuse, in violation of  
22 18 U.S.C. § 1030(b); Computer Fraud, in violation of 18 U.S.C. § 1030(a)(4); and Conspiracy to  
23 Commit Wire Fraud, in violation of 18 U.S.C. § 1349, did knowingly transfer, possess, and use, without  
24 lawful authority the means of identification of another person, to wit, the username and password of J.S.

25 All in violation of Title 18, United States Code, Section 1028A(a)(1).  
26 //  
27 //  
28 //

1 COUNT SIX: (18 U.S.C. § 1956(h) – Money Laundering Conspiracy)

2 32. Paragraphs 1 through 27 of this Indictment are re-alleged and incorporated as if fully set  
3 forth here.

4 33. From on or about June 8, 2017, through on or about April 15, 2018, in the Northern  
5 District of California and elsewhere, the defendants,

6 DANIL POTEKHIN, and  
7 DMITRII KARASAVIDI,

8 did knowingly combine, conspire, and agree with each other and with other persons known and  
9 unknown to the Grand Jury to conduct and attempt to conduct financial transactions affecting interstate  
10 and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is,  
11 Conspiracy to Commit Computer Fraud and Abuse, in violation of 18 U.S.C. § 1030(b); Computer  
12 Fraud, in violation of 18 U.S.C. § 1030(a)(4); and Conspiracy to Commit Wire Fraud, in violation of 18  
13 U.S.C. § 1349; knowing the property involved in the financial transactions represented the proceeds of  
14 some form of unlawful activity and knowing the transactions were designed in whole or in part to  
15 conceal and disguise the nature, location, source, ownership, and control of the proceeds, in violation of  
16 Title 18, United States Code, Section 1956(a)(1)(B)(i).

17 All in violation of Title 18, United States Code, Section 1956(h).

18  
19 COMPUTER FRAUD FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(2)(B) and 1030(i) and  
20 (j))

21 34. The allegations contained in this Indictment are re-alleged and incorporated by reference  
22 for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(b) and  
23 1030(i) and (j).

24 35. Upon conviction for the offenses set forth in Counts One and Two in violation of Title  
25 18, United States Code, Section 1030, set forth in this Indictment, the defendants,

26 DANIL POTEKHIN, and  
27 DMITRII KARASAVIDI,

1 shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(b) and  
2 1030(i) and (j), any personal property used or intended to be used to commit or to facilitate the  
3 commission of said violation or a conspiracy to violate said provision, and any property, real or  
4 personal, which constitutes or is derived from proceeds traceable to the offenses, including, but not  
5 limited to:

- 6 a. 15,602 ETH and .016 BTC seized by law enforcement on or about December 14,  
7 2017 (with a value of approximately \$12,623,627 in USD on that date);
- 8 b. 238.32 BTC, \$6,164,994.23 USD, .99 Bitcoin Cash (BCH), 196.13 Bitcoin Gold  
9 (BTG), 1199.99 NEO, and 50,000 EOS seized by law enforcement on or about  
10 August 23, 2019 (with a value of approximately \$8,768,000 USD on that date);  
11 and
- 12 c. a money judgment equal to the total amount of proceeds defendant obtained or  
13 derived, directly or indirectly, from the violation, or the value of the property used  
14 to commit or to facilitate the commission of said violation.

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

- 16 a. cannot be located upon exercise of due diligence;
- 17 b. has been transferred or sold to, or deposited with, a third party;
- 18 c. has been placed beyond the jurisdiction of the court;
- 19 d. has been substantially diminished in value; or
- 20 e. has been commingled with other property which cannot be divided without  
21 difficulty,

22 the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21,  
23 United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1030(i)(2).

24 All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030, and Federal Rule  
25 of Criminal Procedure 32.2.

26 //

27 //

28 //

SUPERSEDING INDICTMENT

1 WIRE FRAUD FORFEITURE ALLEGATION: (18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c))

2 37. The allegations contained in this Indictment are re-alleged and incorporated by reference  
3 for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C) and  
4 Title 28, United States Code, Section 2461(c).

5 38. Upon conviction for the offense set forth in Count Three of this Indictment, the  
6 defendants,

7 DANIL POTEKHIN, and  
8 DMITRII KARASAVIDI,

9 shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and  
10 Title 28, United States Code, Section 2461(c), all property, real or personal, constituting, or derived  
11 from proceeds the defendant obtained directly and indirectly, as the result of those violations; including  
12 but not limited to:

- 13 a. 15,602 ETH and .016 BTC seized by law enforcement on or about December 14,  
14 2017 (with a value of approximately \$12,623,627 in USD on that date);  
15 b. 238.32 BTC, \$6,164,994.23 USD, .99 Bitcoin Cash (BCH), 196.13 Bitcoin Gold  
16 (BTG), 1199.99 NEO, and 50,000 EOS seized by law enforcement on or about  
17 August 23, 2019 (with a value of approximately \$8,768,000 USD on that date);  
18 and  
19 c. A money judgment equal to the total amount of proceeds the defendant obtained  
20 as a result of the offense.

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

- 22 a. cannot be located upon exercise of due diligence;  
23 b. has been transferred or sold to, or deposited with, a third party;  
24 c. has been placed beyond the jurisdiction of the court;  
25 d. has been substantially diminished in value; or  
26 e. has been commingled with other property which cannot be divided without  
27 difficulty,

28 the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21,

1 United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).

2 All pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 28, United States Code,  
3 Section 2461(c), and Federal Rule of Criminal Procedure 32.2.

4  
5 MONEY LAUNDERING FORFEITURE ALLEGATION: (18 U.S.C. § 982(a)(1))

6 40. The allegations contained in this Indictment are re-alleged and incorporated by reference  
7 for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 982(a)(1).

8 41. Upon conviction for the offense set forth in Count Six of this Indictment, the defendant,

9 DANIL POTEKHIN, and  
10 DMITRII KARASAVIDI,

11 shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), all  
12 property, real or personal, involved in said violations, or any property traceable to such property,  
13 including, but not limited to:

- 14 a. 15,602 ETH and .016 BTC seized by law enforcement on or about December 14,  
15 2017 (with a value of approximately \$12,623,627 in USD on that date);  
16 b. 238.32 BTC, \$6,164,994.23 USD, .99 Bitcoin Cash (BCH), 196.13 Bitcoin Gold  
17 (BTG), 1199.99 NEO, and 50,000 EOS seized by law enforcement on or about  
18 August 23, 2019 (with a value of approximately \$8,768,000 USD on that date);  
19 and  
20 c. A money judgment equal to the total amount of funds involved in the offense.

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

- 1 42. If any of the property described above, as a result of any act or omission of the defendant:  
2 a. cannot be located upon exercise of due diligence;  
3 b. has been transferred or sold to, or deposited with, a third party;  
4 c. has been placed beyond the jurisdiction of the court;  
5 d. has been substantially diminished in value; or  
6 e. has been commingled with other property which cannot be divided without  
7 difficulty,

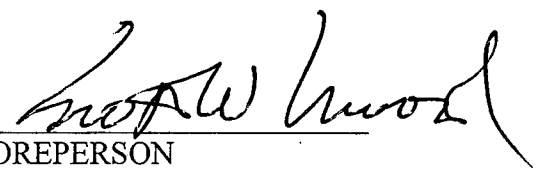
8 the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21,  
9 United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1).

10 All pursuant to Title 18, United States Code, Sections 982(a)(1) and (b)(1) and Federal Rule of  
11 Criminal Procedure 32.2.

12  
13 DATED:

A TRUE BILL.

14  
15 2/18/2020  
16

  
17  
18  
19  
20 FOREPERSON

17 DAVID L. ANDERSON  
18 United States Attorney

  
19  
20 CYNTHIA FREY  
21 Assistant United States Attorney  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

**UNDER SEAL**

**FILED**

**CRIMINAL COVER SHEET**

**FEB 18 2020**

**Instructions:** Effective November 1, 2016, this Criminal Cover Sheet must be completed and submitted along with the Defendant Information Form, for each new criminal case.

SUSAN Y. SCONG  
CLERK, U.S. DISTRICT COURT  
NORTH DISTRICT OF CALIFORNIA

**CASE NAME:**

**CASE NUMBER:**

USA V. DANIL POTEKHIN, a/k/a "crosswar," and DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi

CR 19-0572-CRB

**Is This Case Under Seal?**

Yes  No

**Total Number of Defendants:**

1      2-7       8 or more

**Does this case involve ONLY charges under 8 U.S.C. § 1325 and/or 1326?**

Yes      No

**Venue (Per Crim. L.R. 18-1):**

SF  OAK      SJ

**Is this a potential high-cost case?**

Yes      No

**Is any defendant charged with a death-penalty-eligible crime?**

Yes      No

**Is this a RICO Act gang case?**

Yes      No

**Assigned AUSA**

(Lead Attorney): CYNTHIA FREY, AUSA

**Date Submitted:** 2/18/2020

**Comments:**



**UNDER SEAL**

**FILED**

**FEB 18 2020**

SUSAN Y. SOONG  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

1 DAVID L. ANDERSON (CABN 149604)  
United States Attorney

2 HALLIE HOFFMAN (CABN 210020)  
3 Chief, Criminal Division

4 CYNTHIA FREY (DCBN 475889)  
Assistant United States Attorney

5 450 Golden Gate Avenue, Box 36055  
6 San Francisco, California 94102-3495  
7 Telephone: (415) 436-7200  
8 Fax: (415) 436-7234  
cynthia.frey@usdoj.gov

9 Attorneys for United States of America

10 UNITED STATES DISTRICT COURT  
11 NORTHERN DISTRICT OF CALIFORNIA  
12 SAN FRANCISCO DIVISION

|   |   |  |
|---|---|--|
| 13 UNITED STATES OF AMERICA,              | ) | No.: CR-19-0572-CRB                          |
| 14 Plaintiff,                             | ) | MOTION TO SEAL SUPERSEDING                   |
| 15 v.                                     | ) | INDICTMENT AND [ <del>PROPOSED</del> ] ORDER |
| 16 DANIL POTEKHIN, a/k/a "cronuswar," and | ) | (UNDER SEAL)                                 |
| 17 DMITRII KARASAVIDI, a/k/a Dmitriy      | ) |  |
| Karasavidi                                | ) |  |
| 18 Defendants.                            | ) |  |

19  
20 The government hereby moves the Court for an order sealing the Superseding Indictment, this  
21 motion, and the Court's sealing order until execution of the arrest warrant for defendants DANIL  
22 POTEKHIN, a/k/a "cronuswar," and DMITRII KARASAVIDI, a/k/a Dmitriy Karasavidi. In order to  
23 reduce the chances that the defendants will flee and for reasons of officer safety, the United States  
24 requests that the fact of


25 //  
26 //  
27 //  
28 //

1 the arrest warrant remain under seal until the warrant is executed. The Court's sealing order will be  
2 lifted automatically once the arrest warrant is executed.

3  
4 DATED: February 13, 2020

Respectfully submitted,

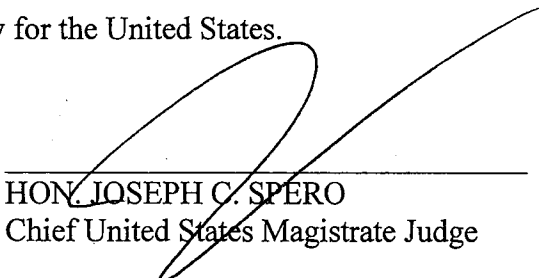
5 DAVID L. ANDERSON  
6 United States Attorney

7  
8   
9 CYNTHIA FREY  
Assistant United States Attorney

10  
11 **[PROPOSED] ORDER**

12 Based upon the motion of the government and for good cause shown, IT IS HEREBY  
13 ORDERED that the Superseding Indictment, this motion, and this sealing order shall be sealed until  
14 execution of the arrest warrant for defendants DANIL POTEKHIN, a/k/a "cronsuswar," and DMITRII  
15 KARASAVIDI, a/k/a Dmitriy Karasavidi or until further order of the Court, whichever occurs first.  
16 This sealing order shall not prevent the Clerk from providing copies of the aforementioned documents to  
17 the United States upon request of an attorney for the United States.

18  
19 DATED: *2/14/2020*

20   
HON. JOSEPH C. SPERO  
21 Chief United States Magistrate Judge  
22  
23  
24  
25  
26  
27  
28