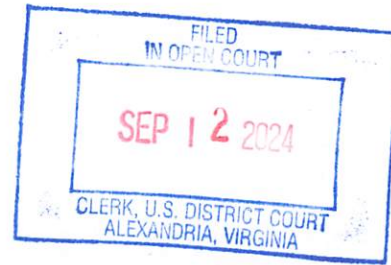


IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division



UNITED STATES OF AMERICA

v.

SERGEY SERGEEVICH IVANOV
a/k/a Taleon
a/k/a UAPS

and

TIMUR KAMILEVICH
SHAKHMAMETOV
a/k/a JokerStash
a/k/a Vega
a/k/a v1pee
a/k/a vip
a/k/a ViperSV

Defendants.

Criminal No. 1:24-CR-205

Counts 1 and 2: 18 U.S.C. § 1349
Conspiracy to Commit Bank Fraud

Count 3: 18 U.S.C. § 1029(b)(2)
Conspiracy to Commit Access Device Fraud

Count 4: 18 U.S.C. § 1956(h)
Conspiracy to Commit Money Laundering

Forfeiture Notice

UNDER SEAL

INDICTMENT

September 2024 Term – at Alexandria, Virginia

1. Sergey Sergeevich IVANOV created and/or operated payment services called UAPS, PinPays, and PM2BTC. These businesses provided money transfer services directly to criminals. These services also provided payment processing system software that was designed for and advertised to cyber criminals. The UAPS, PM2BTC, and PinPays services were designed and intended to facilitate criminal transactions and conduct and to launder the proceeds.

2. IVANOV conspired with Timur Kamilevich SHAKHMAMETOV, who created and operated Joker's Stash, a website devoted to selling stolen payment card data. While Joker's Stash was in operation, it offered for sale data from approximately 40 million payment cards

annually, totaling hundreds of millions of payment cards overall, and was one of the largest known carding markets in history. Estimates of its profits range from \$280 million to more than \$1 billion. IVANOV laundered the proceeds from Joker's Stash.

General Allegations

At times relevant to this Indictment:

3. The following definitions apply:

a. "Carding" refers to the unlawful acquisition and use of data associated with debit and credit cards for purposes of conducting fraudulent transactions and withdrawals.

"Carders" refers to individuals engaged in carding. The types of data of interest to carders include card-issuer type, account number, card verification value (CVV) or card verification code (CVC), card expiration date, and personal identification numbers (PINs) (collectively, "payment card data").

b. Cryptocurrency is a network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency include Bitcoin.

c. "Bitcoin" is a decentralized cryptocurrency that can be used and transferred electronically from person to person, independent of financial institutions. Bitcoin is stored on the Bitcoin blockchain in Bitcoin addresses. Bitcoin holders transmit Bitcoin between Bitcoin addresses. No identifying information about the payor or payee is transmitted in a Bitcoin transaction, as generally only the Bitcoin addresses of the parties are needed for the transaction.

d. The term “cybercrime forum” refers to websites where people involved in cybercrime come together to discuss and commit criminal activities, including payment card fraud, computer hacking, and other related criminal activity.

e. The term “moniker” refers to a chosen username or nickname used in an online environment to conceal the user’s true identity.

4. Forums A, B, and C were cybercrime forums. The administrators of Forum A typically required members who wished to advertise on Forum A to gain official “vendor” or “seller” status, and to secure approval from the Forum A leadership to post specific advertisements. The prospective vendor also had to pay fees to both secure status and post advertisements. The price for advertising on Forum A depended on the timing, design, and desired forum placement or section.

5. Financial Institution 1 was a U.S. financial institution headquartered in McLean, Virginia and was insured by the Federal Deposit Insurance Corporation.

6. IVANOV was a citizen of, and resided primarily in, the Russian Federation. IVANOV used the online monikers Taleon and UAPS, among others, on various online criminal forums.

7. IVANOV employed other individuals to assist with the operation of UAPS, including support and technical staff.

8. The moniker UAPS advertised the UAPS service on online criminal forums, including Forums A and C. These advertisements would tout UAPS’ features such as only maintaining transaction records for a short time and not being regulated by the laws of any country.

9. For example, on May 28, 2013, the UAPS moniker posted an advertisement on Forum C announcing the new UAPS service that would allow users to “receive payments in

multiple ways” and advertising that “deposit and withdrawal are accessible directly from the system, to/from most electronic payment systems, banks, etc.” The advertisement noted that its “benefits” included that the UAPS service was “not registered anywhere” and “not regulated by any law,” that UAPS “will never ask for your personal data,” and that information was “permanently deleted” after two months. The advertisement also highlighted that it had a feature that would allow an online seller to use the UAPS technology to facilitate purchases from the seller’s website.

10. SHAKHMAMETOV was a citizen of, and resided in, the Russian Federation. SHAKHMAMETOV used the online monikers JokerStash, Vega, v1pee, vip, and ViperSV, among others, on various online criminal forums.

11. All amounts of currency, dates, and times are approximate.

COUNT ONE
(Conspiracy to Commit Bank Fraud)

THE GRAND JURY CHARGES THAT:

12. Paragraphs 1 through 9 and paragraph 11 are hereby incorporated by reference.

13. From at least in or around October 2013 and continuing to the present, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendant,

SERGEY SERGEEVICH IVANOV, a/k/a Taleon, a/k/a UAPS,

who is expected to be first brought to the Eastern District of Virginia, did knowingly and intentionally combine, conspire, confederate, and agree with others known and unknown to the Grand Jury to commit and aid and abet an offense under Chapter 63 of Title 18, United States Code, namely, bank fraud, in violation of Title 18, United States Code, Sections 1344 and 2, that is, to knowingly execute and attempt to execute a scheme and artifice to defraud a financial

institution, and to obtain any of the moneys or funds owned by, and under the custody and control of, a financial institution, including Financial Institution 1, by means of materially false and fraudulent pretenses, representations, and promises, and to aid and abet the same.

Manner and Means of the Conspiracy

It was part of the conspiracy that:

14. IVANOV and others operated a carding website called Rescator, on which they sold stolen payment card data from U.S. financial institutions and personally identifiable information (PII) of U.S. citizens. These financial institutions and individuals had not authorized the public dissemination or sale of the data. IVANOV and his coconspirators also sold payment card data which had been stolen in significant data breaches of major U.S. companies.

15. For example, Rescator advertised the sale of data from up to 40 million payment cards and the PII of approximately 70 million people that had been stolen from a major U.S. retail firm in 2013. The breach cost the U.S. retail victim at least \$202 million in expenses and caused damage to the consumers, who became targets of identity theft by other cybercriminals.

16. A coconspirator using the moniker Rescator promoted the Rescator website and its products by advertising the Rescator website and its payment card data on numerous online cybercrime forums. For example, beginning in or around December 2013 on Forum A, the Rescator moniker promoted the Rescator website that he used to sell payment card data from the aforementioned breach of a major U.S. retail corporation. This data remained for sale on the Rescator site through at least February 2015. On February 18, 2015, the Rescator moniker posted on Forum C seeking to purchase stolen credit card information from other Forum C members.

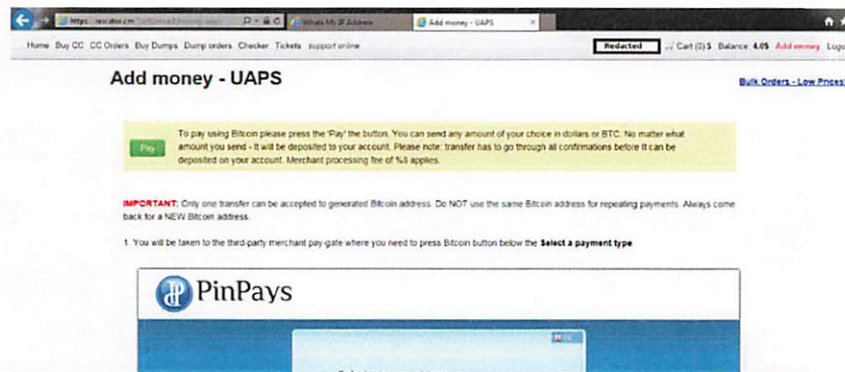
17. One of the primary methods of payment accepted on the Rescator carding website was Bitcoin, which was processed by the UAPS payment processing service. The Rescator carding

website provided specific instructions with visuals on how to navigate UAPS, describing it as “the UAPS payment gateway.”

18. IVANOV provided payment processing support for the Rescator carding website through the UAPS and PinPays services for purchases made using Bitcoin. In order to purchase stolen credit card data, the Rescator carding website required its customers to fund their accounts via a payment processor or exchange service designated by the Rescator carding website. Once customer accounts were funded, customers could then purchase stolen payment cards. The Rescator carding website would then debit the corresponding cost of each card purchase from the customer balance.

19. On or about February 17, 2015, an individual known to the Grand Jury (“Person A”) navigated to the Rescator website, viewed lists of the payment card data offered for sale there, and used the Rescator carding website to purchase data from payment cards issued by various United States financial institutions. The Rescator carding site directed Person A to UAPS to fund the purchase. Person A purchased payment card data for payment cards issued by various United States financial institutions from the Rescator carding website.

20. On April 13, 2015, Person A again purchased payment card data from the Rescator carding website. Person A was directed to a website using both the UAPS and PinPays names to fund the purchase.



Person A then purchased payment card data for payment cards issued by various United States financial institutions from the Rescator carding website.

21. Financial Institution 1 had issued 45 of the payment cards purchased by Person A in February and April of 2015. Financial Institution 1 incurred losses from fraudulent charges made with the payment card data offered for sale on the Rescator carding website.

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

COUNT TWO
(Conspiracy to Commit Bank Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

22. The allegations in paragraphs 1 through 11 are incorporated by reference herein.

23. From in or around October 2014 and continuing until on or about February 3, 2021, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendant,

TIMUR KAMILEVICH SHAKHMAMETOV, a/k/a JokerStash, a/k/a Vega, a/k/a v1pee,
a/k/a vip, a/k/a ViperSV,

who is expected to be first brought to the Eastern District of Virginia, did knowingly and intentionally combine, conspire, confederate, and agree with others known and unknown to the Grand Jury to commit bank fraud, in violation of Title 18, United States Code, Sections 1344 and 2, that is, to knowingly execute and attempt to execute a scheme and artifice to defraud a financial institution, and to obtain any of the moneys and funds owned by, and under the custody and control of, a financial institution, including Financial Institution 1, by means of materially false and fraudulent pretenses, representations, and promises, and to aid and abet the same.

Manner and Means of the Conspiracy

It was part of the conspiracy that:

24. SHAKHMAMETOV and others operated the carding website called Joker's Stash, on which they offered for sale payment card data belonging to individuals and associated with financial institutions that had not authorized the sale or public dissemination of the data, as well as the PII of U.S. citizens. Much of the payment card data and PII offered for sale on Joker's Stash had been stolen in significant data breaches of major United States companies.

25. SHAKHMAMETOV and others promoted Joker's Stash and its products by advertising the Joker's Stash website and its payment card data on numerous online cybercrime

forums, particularly Forum A. For example, on June 25, 2015, the moniker JokerStash posted an advertisement on Forum A in which he advertised the sale of “millions of fresh fire dumps & cvv,” that is, newly stolen payment card data, and provided customers with directions on how to visit the Joker’s Stash Website. JokerStash advertised at least tens of millions of payment cards for sale on Forum A during the site’s operations.

26. SHAKHMAMETOV and others would also emphasize that Joker’s Stash’s products were recently stolen and sold exclusively on the Joker’s Stash website. Recently stolen payment card data that was offered exclusively on the Joker’s Stash carding website was less likely to have been deactivated by the payment card issuers, making the Joker’s Stash product more valuable and increasing the conspirators’ profits.

27. For example, on or about October 11, 2014, the moniker JokerStash posted on Forum B that he would shortly be selling “absolute virgin fresh new zero-day db [database] with 100%+1 valid rate” that would be available “only at Joker’s Stash.” On or about January 27, 2020, JokerStash posted on Forum A advertising a new set of 30 million payment cards available for sale that were “Exclusively ONLY at JOKER’s STASH!” Likewise, in answering a potential customer’s questions about where Joker’s Stash payment card data came from, JokerStash responded “everything is ours :-).”

28. Similarly, the Joker’s Stash carding website promised its customers refunds on certain purchases within specified time periods if the purchased payment card data was determined to be no longer valid and thus could not be used to complete transactions. The refund guarantee further protected customers and incentivized them to purchase payment card data from the site.

29. SHAKHMAMETOV also conspired with the administrator of Try2Check, a service that confirmed the validity of purchased payment card data, in order to further incentivize

customers to purchase from Joker's Stash. Joker's Stash advertised Try2Check on its website and featured the service prominently in its ads. Joker's Stash also integrated Try2Check's functionality directly into its website, giving customers the option to validate their newly purchased cards by clicking a button. Using Try2Check sometimes cost customers a small fee, but in other instances, Joker's Stash would offer the service to customers for free. For some purchases, if the payment cards were found to be invalid, Joker's Stash would automatically grant purchasers a refund. The promotion and integration of Try2Check was intended to demonstrate the validity—and thus the value—of the payment card data offered for sale on Joker's Stash, further incentivizing sales.

30. In general, Joker's Stash charged anywhere from \$25 to \$75 for data from a single payment card. Data that was newer—and thus more likely to be valid and usable to conduct fraudulent transactions—was frequently sold at a higher price. Joker's Stash users were also offered discounts for large purchases, as depicted below:

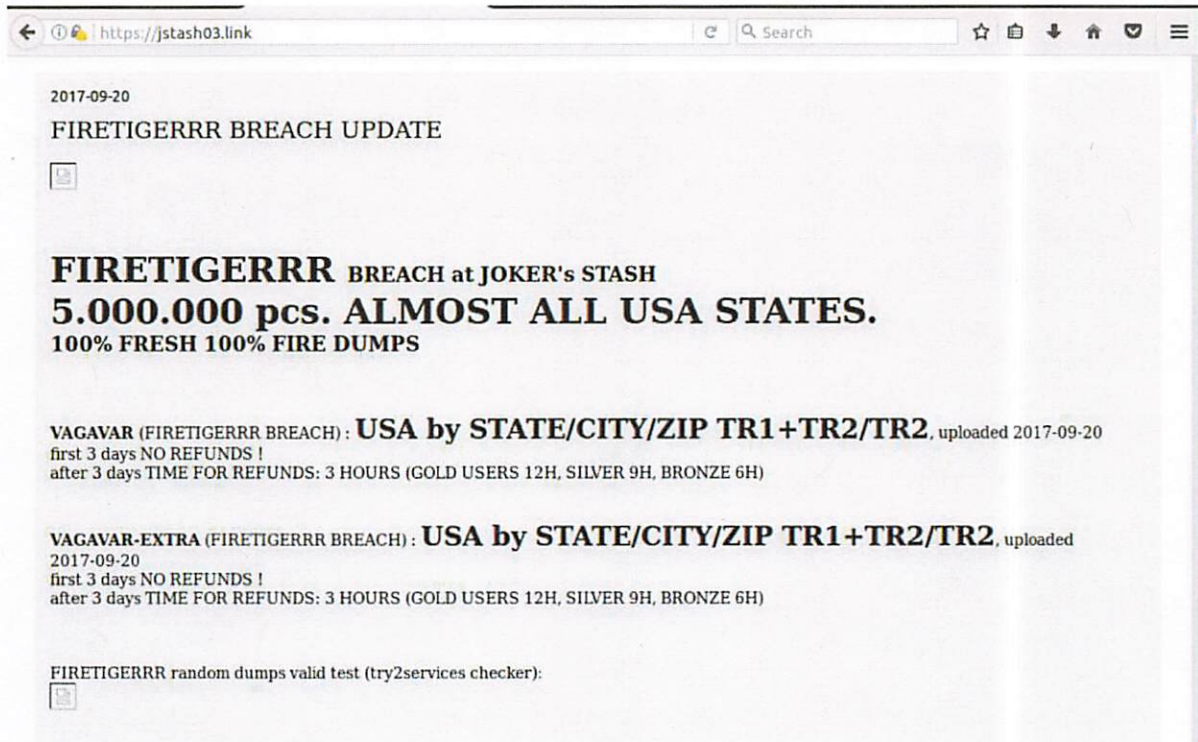
Bulk orders

Automatic discount system. Buy big and save							
Order Total	\$1–\$299	\$300–\$499	\$500–\$999	\$1,000–\$2,499	\$2,500–\$4,999	\$5,000–\$9,999	\$10,000+
Discount	0%	5%	10%	15%	20%	25%	30%

31. On or about October 22, 2014, an individual known to the Grand Jury (“Person B”) navigated to the Joker's Stash website, viewed lists of payment card data offered for sale, and purchased payment card data associated with approximately 32 different payment cards issued by Financial Institution 1. At least some of the purchased payment card data was valid and sold without authorization.

32. On or about September 22, 2017, an individual known to the Grand Jury (“Person C”) navigated to the Joker's Stash website while in the Eastern District of Virginia and viewed

lists of payment card data offered for sale, as depicted below. In particular, Person C viewed advertised data stolen from a breach of a U.S. corporation.



33. For this particular breach, the Joker's Stash website allowed customers the ability to filter for specific stolen payment cards of interest, to include cards issued to individual victims in Virginia, as depicted below. This filtering function allowed purchasers to select payment card data close to where they were operating to reduce the likelihood that the compromise would be detected and the cards deactivated before they could be used for fraudulent purposes.

The screenshot shows the Joker's Stash website interface. At the top, there is a navigation bar with the site logo, 'Write & Swipe', and user account information including 'username redacted', 'Profile', 'Balance: \$0.00 USD', and 'Log out'. A shopping cart icon indicates '0 items in your cart'. Below the navigation bar, the page title is 'Buy Dumps' with a sub-link 'Preorder BINs (Autobuy)'. The main content area is a 'Filter' section with the following details:

- Base: Latest - KOTA (fresh skimmed base) : USA (ND,CT,BC,CA,OH,TX,FL,NM,MA,SC,OR + other states) TR1+TR2, HIGH VALID 80-85%, uploaded 2017-09-22 (time for refunds: 3 hours)
- Selected filter: TIGRIX (FIRETIGERRR BREACH) : USA by STATE/CITY/ZIP TR1+TR2/TR2, uploaded 2017-09-18 (time for refunds: 3 hours)
- Country: United States (selected), other
- State: VA (selected)
- City: (Any)
- Service code: 1xx, 2xx, other (Any)
- ZIP codes (one per line): Excluding
- Bank: (Any)
- Card brand: Visa, Mastercard, AMEX (Any)
- Card level: (Any)
- Credit/debit: credit, debit (Any)
- BINs (one or more per line): Excluding
- Price (USD): \$ - \$
- Tracks: TR1+TR2 or TR2
- Expiration date (YYMM; one or more per line): Disabled due to security reasons (protection against law enforcement staff lookups)
- Last 4 digits (one or more per line): You need better partner's rating to use this filter

At the bottom of the filter section, there are 'Apply filters' and 'Reset' buttons.

34. On or about September 22, 2017, Person C, while in the Eastern District of Virginia, paid approximately \$1,150 and purchased payment card data from the Joker's Stash carding website. At least some of the purchased payment card data was valid and sold without authorization.

35. Financial Institution 1 incurred losses from fraudulent charges made with the payment card data offered for sale on the Joker's Stash carding website.

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

COUNT THREE
(Conspiracy to Commit Access Device Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

36. The allegations in paragraphs 1 through 11 and 24 through 35 are incorporated by reference herein.

37. From in or around October 2014 and continuing until at least on or about February 3, 2021, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendant,

TIMUR KAMILEVICH SHAKHMAMETOV, a/k/a JokerStash, a/k/a Vega, a/k/a v1pee,
a/k/a vip, a/k/a ViperSV,

who is expected to be first brought to the Eastern District of Virginia, did knowingly and intentionally combine, conspire, confederate, and agree with each other and others known and unknown to the Grand Jury to commit and aid and abet the following offenses under Title 18, United States Code, Section 1029(a):

a. trafficking in unauthorized access devices, that is, knowingly and with intent to defraud, trafficking in one or more unauthorized access devices during a one-year period, to wit: payment card data issued by United States entities, including Financial Institution 1, and by such conduct, in that period of one year, obtaining anything of value aggregating \$1,000 or more, affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 1029(a)(2) and 2; and

b. unlawfully advertising access devices, that is, without the authorization of the issuer of the access devices, knowingly and with intent to defraud soliciting a person for the purpose of offering access devices, to wit: payment card data issued by United States entities, including Financial Institution 1, affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 1029(a)(6) and 2.

Overt Acts in Furtherance of the Offenses Which Were the Objects of the Conspiracy

38. The acts specified in paragraphs 25 through 34 were also committed in furtherance of the offenses which were the object of the conspiracy alleged in the instant count and are incorporated here.

(All in violation of Title 18, United States Code, Section 1029(b)(2).)

COUNT FOUR
(Conspiracy to Commit Money Laundering)

THE GRAND JURY FURTHER CHARGES THAT:

39. The allegations in paragraphs 1 through 11 are incorporated by reference herein.

40. From in or around October 2014 and continuing until at least on or about February 3, 2021, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendants,

SERGEY SERGEEVICH IVANOV, a/k/a Taleon, a/k/a UAPS, and
TIMUR KAMILEVICH SHAKHMAMETOV, a/k/a JokerStash, a/k/a Vega, a/k/a v1pee,
a/k/a vip, a/k/a ViperSV,

who are expected to be first brought to the Eastern District of Virginia, did knowingly and intentionally combine, conspire, confederate, and agree with each other and others known and unknown to the Grand Jury to commit the following offenses:

a. Conducting and attempting to conduct a financial transaction, knowing that the property involved in the transaction represented the proceeds of specified unlawful activity, to wit, access device fraud and conspiracy to commit access device fraud, as alleged in Count 3, and knowing that the transaction was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of that specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and

b. Knowingly engaging or attempting to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 that was derived from specified unlawful activity, to wit, access device fraud and conspiracy to commit access device fraud, as alleged in Count 3, in violation of Title 18, United States Code, Section 1957(a).

Manner and Means of the Conspiracy

41. As part of the conspiracy, IVANOV, SHAKHMAMETOV, and others sought to accomplish the objects of the conspiracy through the Manners and Means set forth in Paragraphs 24 through 35. It was further part of the conspiracy that:

42. Customers seeking to replenish their Joker's Stash account balances sent Bitcoin to cryptocurrency wallets controlled by SHAKHMAMETOV and other coconspirators operating Joker's Stash. From there, SHAKHMAMETOV and other coconspirators operating Joker's Stash would transfer those funds to cryptocurrency wallets controlled by IVANOV and other coconspirators operating the UAPS and PM2BTC infrastructure, including in amounts greater than \$10,000. IVANOV and other coconspirators would then transfer the funds to other wallets they controlled, including to a cryptocurrency exchange known not to cooperate with law enforcement.

43. On or about November 11, 2014, an individual known to the Grand Jury ("Person B") visited the Joker's Stash carding website and sent Bitcoin to a Bitcoin address controlled by Joker's Stash to fund Person B's purchase account. Those funds were then comingled with other customers' funds before being transferred to a wallet controlled by IVANOV and other coconspirators operating the UAPS and PM2BTC infrastructure. From there, on or about November 11, 2014, the funds were transferred to a wallet controlled by IVANOV at a cryptocurrency exchange known not to cooperate with law enforcement.

44. On or about August 13, 2015, an individual known to the Grand Jury ("Person B") visited the Joker's Stash carding website and sent Bitcoin to a Bitcoin address controlled by Joker's Stash to fund Person B's purchase account. Those funds were then comingled with other customers' funds before being transferred to a wallet controlled by IVANOV and other coconspirators operating the UAPS and PM2BTC infrastructure. From there, on or about August

13, 2015, the funds were transferred to a wallet controlled by IVANOV at a cryptocurrency exchange known not to cooperate with law enforcement.

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

NOTICE OF FORFEITURE

THE GRAND JURY FURTHER FINDS PROBABLE CAUSE THAT:

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.

Pursuant to Federal Rule of Criminal Procedure 32.2(a), the defendants are hereby notified that if convicted of an offense alleged in Counts One and Two, the defendants shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(A), any property constituting, or derived from, any proceeds they obtained, directly or indirectly, as a result of such offense.

Pursuant to Federal Rule of Criminal Procedure 32.2(a), the defendants are hereby notified that, if convicted of the offense alleged in Count 3 of this Indictment, the defendants shall forfeit to the United States, pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1029(c)(1)(C): (A) any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of the violation; and (B) any personal property used or intended to be used to commit the violation.


Pursuant to Federal Rule of Criminal Procedure 32.2(a), the defendants are hereby notified that, if convicted of the offense alleged in Count 4 of the Indictment, the defendants shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in the violation, or any property traceable to such property.

Pursuant to Title 21, U.S. Code, Section 853(p), the defendants shall forfeit substitute property, if, by any act or omission of the defendants, 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.

(All in accordance with Title 18, United States Code, Sections 981(a)(1), 982(a)(2)(A), 982(a)(2)(B), and 1029(c)(1)(C); Title 21 United States Code, Section 853; and Fed. R. Crim. P. 32.2.)

A TRUE BILL:
Pursuant to the E-Government Act,
The original of this page has been filed
under seal in the Clerk's Office
Foreperson of the Grand Jury

Jessica D. Aber
United States Attorney



Zoe Bedell
Assistant United States Attorney