EXHIBIT B

SUPERIOR COURT OF CALIFORNIA
COUNTY OF SANTA CLARA
HALL OF JUSTICE

COMPLAINT FOR ARREST WARRANT(S)
NICHOLAS TRUGLIA EFG418

THE PEOPLE OF THE STATE OF CALIFORNIA,
Plaintiff,

vs.

NICHOLAS TRUGLIA (09/25/1997),
605 WEST 42ND STREET NEW YORK NY 10036

Defendant(s).

FELONY COMPLAINT

DA NO: 181134734
CEN
NT WARR

FILED
NOV 13 2018
Clerk of the Court
Superior Court of CA County of Santa Clara
BY _____ DEPUTY

The undersigned is informed and believes that:

COUNT 1

On or about October 18, 2018, in the County of Santa Clara, State of California, the crime of USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION, in violation of PENAL CODE SECTION 530.5(a), a Felony, was committed by NICHOLAS TRUGLIA who did willfully obtain personal identifying information, the cell phone number of Saswata Basu, and used the information for an unlawful purpose, including to obtain, and attempt to obtain, credit, goods, services, real property, and medical information, in the name of Saswata Basu without his or her consent.

COUNT 2

On or about October 18, 2018, in the County of Santa Clara, State of California, the crime of COMPUTER CRIME - ALTERING AND DAMAGING COMPUTER DATA WITH INTENT TO DEFRAUD OR OBTAIN MONEY, OR OTHER VALUE, in violation of PENAL CODE SECTION 502(c)(1)(A), a Felony, was committed by NICHOLAS TRUGLIA who did knowingly access and without permission alter, damage, delete, destroy, and otherwise use data, a computer, computer system, and computer network in order to devise or execute any scheme or artifice to defraud, deceive, or extort.

COUNT 3

On or about October 26, 2018, in the County of San Francisco, State of California, the crime of USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION, in violation of PENAL CODE SECTION 530.5(a), a Felony, was committed by NICHOLAS TRUGLIA who did willfully obtain personal identifying information, the cell phone number of Robert Ross, and used the information for an unlawful purpose, including to obtain, and attempt to obtain, credit, goods, services, real property, and medical information, in the name of Robert Ross without his or her consent.

COUNT 4

On or about October 26, 2018, in the County of San Francisco, State of California, the crime of COMPUTER CRIME - ALTERING AND DAMAGING COMPUTER DATA WITH INTENT TO DEFRAUD OR OBTAIN MONEY, OR OTHER VALUE, in violation of PENAL CODE SECTION 502(c)(1)(A), a Felony, was committed by NICHOLAS TRUGLIA who did knowingly access and without permission alter, damage, delete, destroy, and otherwise use data, a computer, computer system, and computer network in order to devise or execute any scheme or artifice to defraud, deceive, or extort.

COUNT 5

On or about October 26, 2018, in the County of San Francisco, State of California, the crime of GRAND THEFT OF PERSONAL PROPERTY OF A VALUE OVER NINE HUNDRED AND FIFTY DOLLARS, in violation of PENAL CODE SECTION 487(a), a Felony, was committed by NICHOLAS TRUGLIA who did unlawfully take personal property, cash, of a value exceeding nine hundred and fifty dollars ($950.00), the property of Robert Ross.

COUNT 6

On or about October 26, 2018, in the County of San Francisco, State of California, the crime of GRAND THEFT OF PERSONAL PROPERTY OF A VALUE OVER NINE HUNDRED AND FIFTY DOLLARS, in violation of PENAL CODE SECTION 487(a), a Felony, was committed by NICHOLAS TRUGLIA who did unlawfully take personal property, of a value exceeding nine hundred and fifty dollars ($950.00), the property of.

COUNT 7

On or about October 16, 2018, in the County of Los Angeles, State of California, the crime of USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION, in violation of PENAL CODE SECTION 530.5(a), a Felony, was committed by NICHOLAS TRUGLIA who did willfully obtain personal identifying information, the cell phone number of Angel Anderson, and used the information for an unlawful purpose, including to obtain, and attempt to obtain, credit, goods, services, real property, and medical information, in the name of Angel Anderson without his or her consent.

COUNT 8

On or about October 16, 2018, in the County of Los Angeles, State of California, the crime of COMPUTER CRIME - ALTERING AND DAMAGING COMPUTER DATA WITH INTENT TO DEFRAUD OR OBTAIN MONEY, OR OTHER VALUE, in violation of PENAL CODE SECTION 502(c)(1)(A), a Felony, was committed by NICHOLAS TRUGLIA who did knowingly access and without permission alter, damage, delete, destroy, and otherwise use data, a computer, computer system, and computer network in order to devise or execute any scheme or artifice to defraud, deceive, or extort.

COUNT 9

On or about October 26, 2018, in the County of San Francisco, State of California, the crime of USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION, in violation of PENAL CODE SECTION 530.5(a), a Felony, was committed by NICHOLAS TRUGLIA who did willfully obtain personal identifying information, the cell phone number of Myles Danielson, and used the information for an unlawful purpose, including to obtain, and attempt to obtain, credit, goods, services, real property, and medical information, in the name of Myles Danielson without his or her consent.

COUNT 10

On or about October 26, 2018, in the County of San Francisco, State of California, the crime of COMPUTER CRIME - ALTERING AND DAMAGING COMPUTER DATA WITH INTENT TO DEFRAUD OR OBTAIN MONEY, OR OTHER VALUE, in violation of PENAL CODE SECTION 502(c)(1)(A), a Felony, was committed by NICHOLAS TRUGLIA who did knowingly access and without permission alter, damage, delete, destroy, and otherwise use data, a computer, computer system, and computer network in order to devise or execute any scheme or artifice to defraud, deceive, or extort.

COUNT 11

On or about October 26, 2018, in the County of Francisco, State of California, the crime of USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION, in violation of PENAL CODE SECTION 530.5(a), a Felony, was committed by NICHOLAS TRUGLIA who did willfully obtain personal identifying information, the cell phone number of Myles Danielson, and used the information for an unlawful purpose, including to obtain, and attempt to obtain, credit, goods, services, real property, and medical information, in the name of Myles Danielson without his or her consent.

COUNT 12

On or about October 26, 2018, in the County of Santa Clara, State of California, the crime of COMPUTER CRIME - ALTERING AND DAMAGING COMPUTER DATA WITH INTENT TO DEFRAUD OR OBTAIN MONEY, OR OTHER VALUE, in violation of PENAL CODE SECTION 502(c)(1)(A), a Felony, was committed by NICHOLAS TRUGLIA who did knowingly access and without permission alter, damage, delete, destroy, and otherwise use data, a computer, computer system, and computer network in order to devise or execute any scheme or artifice to defraud, deceive, or extort.

COUNT 13

On or about October 26, 2018, in the County of San Francisco, State of California, the crime of ATTEMPTED GRAND THEFT OF PERSONAL PROPERTY OF A VALUE OVER NINE HUNDRED AND FIFTY DOLLARS, in violation of PENAL CODE SECTION 664-PENAL CODE SECTION 487(a), a Felony, was committed by NICHOLAS TRUGLIA who did ATTEMPT TO unlawfully take personal property, cash, of a value exceeding nine hundred and fifty dollars ($950.00), the property of Myles Danielson.

COUNT 14

On or about October 21, 2018, in the County of San Francisco, State of California, the crime of USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION, in violation of PENAL CODE SECTION 530.5(a), a Felony, was committed by NICHOLAS TRUGLIA who did willfully obtain personal identifying information, the cell phone number of Gabrielle Katsnelson, and used the information for an unlawful purpose, including to obtain, and attempt to obtain, credit, goods, services, real property, and medical information, in the name of Gabrielle Katsnelson without his or her consent.

COUNT 15

On or about October 21, 2018, in the County of San Francisco, State of California, the crime of COMPUTER CRIME - ALTERING AND DAMAGING COMPUTER DATA WITH INTENT TO DEFRAUD OR OBTAIN MONEY, OR OTHER VALUE, in violation of PENAL CODE SECTION 502(c)(1)(A), a Felony, was committed by NICHOLAS TRUGLIA who did knowingly access and without permission alter, damage, delete, destroy, and otherwise use data, a computer, computer system, and computer network in order to devise or execute any scheme or artifice to defraud, deceive, or extort.

COUNT 16

On or about October 21, 2018, in the County of San Francisco, State of California, the crime of USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION, in violation of PENAL CODE SECTION 530.5(a), a Felony, was committed by NICHOLAS TRUGLIA who did willfully obtain personal identifying information, the cell phone number of Gabrielle Katsnelson, and used the information for an unlawful purpose, including to obtain, and attempt to obtain, credit, goods, services, real property, and medical information, in the name of Gabrielle Katsnelson without his or her consent.

COUNT 17

On or about October 21, 2018, in the County of San Francisco, State of California, the crime of COMPUTER CRIME - ALTERING AND DAMAGING COMPUTER DATA WITH INTENT TO DEFRAUD OR OBTAIN MONEY, OR OTHER VALUE, in violation of PENAL CODE SECTION 502(c)(1)(A), a Felony, was committed by NICHOLAS TRUGLIA who did knowingly access and without permission alter, damage, delete, destroy, and otherwise use data, a computer, computer system, and computer network in order to devise or execute any scheme or artifice to defraud, deceive, or extort.

COUNT 18

On or about October 21, 2018, in the County of San Francisco, State of California, the crime of USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION, in violation of PENAL CODE SECTION 530.5(a), a Felony, was committed by NICHOLAS TRUGLIA who did willfully obtain personal identifying information, the cell phone number of Gabrielle Katsnelson, and used the information for an unlawful purpose, including to obtain, and attempt to obtain, credit, goods, services, real property, and medical information, in the name of Gabrielle Katsnelson without his or her consent.

COUNT 19

On or about October 21, 2018, in the County of San Francisco, State of California, the crime of COMPUTER CRIME - ALTERING AND DAMAGING COMPUTER DATA WITH INTENT TO DEFRAUD OR OBTAIN MONEY, OR OTHER VALUE, in violation of PENAL CODE SECTION 502(c)(1)(A), a Felony, was committed by NICHOLAS TRUGLIA who did knowingly access and without permission alter, damage, delete, destroy, and otherwise use data, a computer, computer system, and computer network in order to devise or execute any scheme or artifice to defraud, deceive, or extort.

COUNT 20

On or about October 21, 2018, in the County of San Francisco State of California, the crime of USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION, in violation of PENAL CODE SECTION 530.5(a), a Felony, was committed by NICHOLAS TRUGLIA who did willfully obtain personal identifying information, the cell phone number of Gabrielle Katsnelson, and used the information for an unlawful purpose, including to obtain, and attempt to obtain, credit, goods, services, real property, and medical information, in the name of Gabrielle Katsnelson without his or her consent.

COUNT 21

On or about October 21, 2018, in the County of San Francisco, State of California, the crime of COMPUTER CRIME - ALTERING AND DAMAGING COMPUTER DATA WITH INTENT TO DEFRAUD OR OBTAIN MONEY, OR OTHER VALUE, in violation of PENAL CODE SECTION 502(c)(1)(A), a Felony, was committed by NICHOLAS TRUGLIA who did knowingly access and without permission alter, damage, delete, destroy, and otherwise use data, a computer, computer system, and computer network in order to devise or execute any scheme or artifice to defraud, deceive, or extort.

AGGRAVATED WHITE COLLAR CRIME ENHANCEMENT

It is further alleged that the felony crimes charged in Counts 5, 6, 13 are related, that a material element of the crimes is fraud and embezzlement, that the crimes involve a pattern of related felony conduct, and that the pattern of related felony conduct by NICHOLAS TRUGLIA involves the taking of more than five hundred thousand dollars ($500,000), within the meaning of Penal Code sections 186.11(a)(1) and (a)(2).

Any defendant, including a juvenile, who is convicted of and pleads guilty and no contest to any felony offense, including any attempt to commit the offense, charged in this complaint or information is required to provide buccal swab samples, right thumbprints and a full palm print impression of each hand, and any blood specimens or other biological samples required pursuant to the DNA and Forensic Identification Database and Data Bank Act of 1998 and Penal Code section 296, et seq.

Further, attached and incorporated by reference are official reports and documents of a law enforcement agency which the complainant believes establish probable cause for the arrest of defendant NICHOLAS TRUGLIA, for the above-listed crimes. Wherefore, A WARRANT OF ARREST IS REQUESTED.

Complainant therefore requests that the defendant(s) be dealt with according to law.
I certify under penalty of perjury that the above is true and correct.
Executed on November 9, 2018, in SANTA CLARA County, California.

#1945

Tuttle T1945
(Tuttle T1945)
REACT 20180066
WEST/ D411/ FELONY/ MS

Cash or Bond $ 1,000,000.00
Date: 11/9/2018

JUDGE OF THE SUPERIOR COURT

Warrant Received for Service by:

_____

on _____

EFG418

ARREST WARRANT
SUPERIOR COURT OF CALIFORNIA, COUNTY OF SANTA CLARA

THE PEOPLE OF THE STATE OF CALIFORNIA,
PLAINTIFF

vs.

Nicholas Truglia
605 W 42nd ST
New York NY 10036,
DEFENDANT

DOCKET NO.: C1806134
WARRANT NO.: 1800100005
COMPLAINT AGENCY: SCC Office of the Sheriff
AGENCY CASE NO.:

DESCRIPTION

DRIVER'S LIC. NO.:
BIRTHDATE: 09/25/1997
HEIGHT:
WEIGHT:
EYES:
HAIR:
SEX:

THE PEOPLE OF THE STATE OF CALIFORNIA TO ANY PEACE OFFICER OF SAID STATE:
COMPLAINT UNDER OATH HAVING BEEN MADE BEFORE ME BY:
, , SCC Office of the Sheriff

THAT THE OFFENSE OF: **PC530.5(A)-F-USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION; PC502(C)(1)(A)-F-ACCESS COMPUTER/ALTER/ETC DATA:DEVISE SCHEME/ETC DEFRAUD/ETC; PC530.5(A)-F-USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION; PC502(C)(1)(A)-F-ACCESS COMPUTER/ALTER/ETC DATA:DEVISE SCHEME/ETC DEFRAUD/ETC; PC487A-F-GRAND THEFT: MONEY/LABOR/PROPERTY; PC487A-F-GRAND THEFT: MONEY/LABOR/PROPERTY; PC530.5(A)-F-USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION; PC502(C)(1)(A)-F-ACCESS COMPUTER/ALTER/ETC DATA:DEVISE SCHEME/ETC DEFRAUD/ETC; PC530.5(A)-F-USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION; PC502(C)(1)(A)-F-ACCESS COMPUTER/ALTER/ETC DATA:DEVISE SCHEME/ETC DEFRAUD/ETC; PC530.5(A)-F-USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION; PC502(C)(1)(A)-F-ACCESS COMPUTER/ALTER/ETC DATA:DEVISE SCHEME/ETC DEFRAUD/ETC; PC664/487(A)-F-ATTEMPT: GRAND THEFT OF PERSONAL PROPERTY/ETC EXCEEDING $950; PC530.5(A)-F-USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION; PC502(C)(1)(A)-F-ACCESS COMPUTER/ALTER/ETC DATA:DEVISE SCHEME/ETC DEFRAUD/ETC; PC530.5(A)-F-USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION; PC502(C)(1)(A)-F-ACCESS COMPUTER/ALTER/ETC DATA:DEVISE SCHEME/ETC DEFRAUD/ETC; PC530.5(A)-F-USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION; PC502(C)(1)(A)-F-ACCESS COMPUTER/ALTER/ETC DATA:DEVISE SCHEME/ETC DEFRAUD/ETC; PC530.5(A)-F-USING PERSONAL IDENTIFYING INFORMATION WITHOUT AUTHORIZATION; PC502(C)(1)(A)-F-ACCESS COMPUTER/ALTER/ETC DATA:DEVISE SCHEME/ETC DEFRAUD/ETC**

A FELONY HAS BEEN COMMITTED, AND ACCUSING:

Nicholas Truglia

THEREOF, YOU ARE THEREFORE COMMANDED TO ARREST THE ABOVE NAMED DEFENDANT AND BRING SAID DEFENDANT FORTHWITH BEFORE THE ENTITLED COURT.

DEFENDANT MAY BE ADMITTED TO BAIL IN THE SUM OF $ 1,000,000 [00]

Witness my hand and seal,
Ordered on this the 13th Day of November, 2018

JUDGE OF THE SUPERIOR COURT OF CALIFORNIA

Regional Enforcement Allied Computer Team **INVESTIGATION REPORT:** **COVER AND PARTY PAGES**	Case Number: 2018-0066		
	Occurred	Date	Time
	ON OR FROM	Oct 15, 2018	12:00:00 AM
Report Type: 502(c)(1) PC Unlawful Computer Access, 487(a) PC Grand Theft, 530.5(a) PC ID Th	TO	Oct 26, 2018	12:00:00 AM
Location of Crime: 605 West 42nd Street 64W, New York, New York 10036	REPORTED	Oct 19, 2018	12:00:00 AM

SUSPECT INFORMATION AND ASSOCIATED CHARGES

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
1	Truglia, Nicholas	09/25/1997	21	M	White	6'3"	200

Home Address	City	State	Zip Code
605 West 42nd Street 64W	New York	NY	10036

Phone Number/Type	E-mail Address	DL #	PFN	CII #	Social Security #
732-456-2221		[redacted]			[redacted]

Applicable Charge	Description of Charge	
502(c)(1) PC	Unlawful Computer Access	
487(a) PC	Grand Theft	
530.5(a) PC	Identity Theft	
664/487(a) PC	Attempted Grand Theft	

COURT COPY

INVOLVED PARTY INFORMATION

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
1	Basu, Saswata	[redacted]	48	M	A		

Address	City	State	Zip Code
[redacted]	[redacted]	[redacted]	[redacted]

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]			Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
2	Ross, Robert	[redacted]	55	M	White		

Address	City	State	Zip Code
[redacted]	[redacted]	[redacted]	[redacted]

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]		[redacted]	Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
3	Anderson, Angel	[redacted]	46	F	W		

Address	City	State	Zip Code
[redacted]	[redacted]	[redacted]	[redacted]

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]			[redacted]	Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
4	Danielson, Myles Walker	[redacted]	33	M	W		

Address	City	State	Zip Code
[redacted]	[redacted]	[redacted]	[redacted]

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]		[redacted]	Victim

#	Name: Last, First Middle	Date of Birth	Age	Sex	Race	Height	Weight
5	Katsnelson, Gabrielle	[redacted]	34	F	W		

Address	City	State	Zip Code
[redacted]	[redacted]	[redacted]	[redacted]

Phone Number/Type	E-mail Address	Other Phone	DL #	Relationship to Case
[redacted]	[redacted]		[redacted]	Victim

Regional Enforcement Allied Computer Team
INVESTIGATION REPORT:
NARRATIVE

SYNOPSIS:

Victim Saswata Basu, a resident of [redacted], had his AT&T cell phone taken over by the suspect who then gained unlawful access to V. Basu's Yahoo email account and attempted to access his Dropbox account. I was also contacted by Victim Ross who lost access to his cell phone, Gmail account and had approximately $1,000,000 stolen from two cryptocurrency exchanges where the suspects transferred USD into Bitcoin and transferred funds into cryptocurrency wallets the suspects controlled. The suspect also attempted to wire transfer approximately $300,000 from Victim Danielson's Fidelity account but was stopped by the victim. The victims listed in this investigation live [redacted]

BACKGROUND DEFENITIONS:

"Cryptocurrency": Any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.

"SIM card": For some types of mobile communication devices, a Subscriber Identity Module (or "SIM") card is a small card that is inserted into a mobile device (such as a cell phone handset) to enable the mobile device to communicate with its service provider, as it contains network data needed to make a successful connection to the cellular network provider. SIM cards store files that can be used to uniquely identify them, including the ICCID (Integrated Circuit Card Identifier, a 19- or 20-digit serial number for the SIM card that uniquely identifies the card itself) and the IMSI (International Mobile Subscriber Identity, a 14-or 15- digit number that uniquely identifies a subscriber's account with the cellular network provider).

"SIM swap": An account takeover method by which cellular phone service accounts are compromised. In this scheme, the suspect arranges (through bribery of someone with access,

artifice/"social engineering," or other methods) for a cellular service provider to change the SIM card assigned to particular account to a new SIM card under the suspect's control. Once the suspect controls the new SIM card, he/she can impersonate the victim in correspondence with other service providers (such as email providers) by using the victim's cell phone number to request changes to account settings, eventually resetting the password and taking control of the account.

"IMEI": IMEI is short for International Mobile Equipment Identity is a 15 or 17 digit number that is used to uniquely identify certain types of mobile phone devices. Many providers of electronic communication services log the IMEI number used to access their systems.

2-Factor Authentication ("2FA"): A security mechanism that requires two types of credentials for authentication and is designed to provide an additional layer of validation.

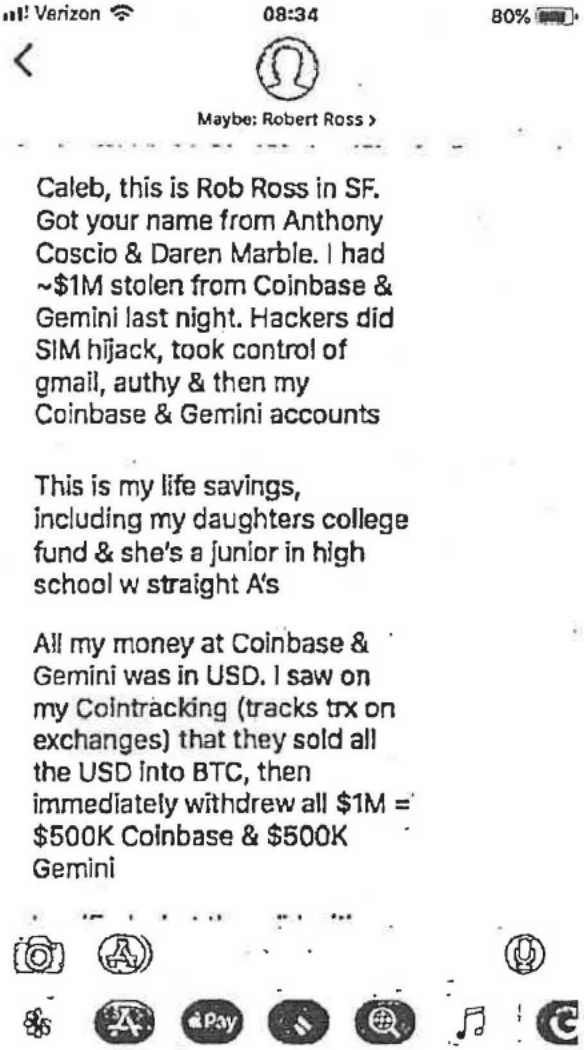
INVESTIGATION:

(V) Saswata B.

Saswata B. is a resident of [redacted] He is a previously reported victim of a SIM swap that occurred in May of 2018 that has been investigated by the REACT Task Force. On 10/18/18, he notified Santa Clara Sheriff's Office Sergeant S. Tarazi that he had just been the victim of another SIM swap, where the target was his phone number ending in [redacted]. During the incident, the suspects unlawfully accessed his Yahoo email but did not steal any currency or cryptocurrency. AT&T provided records which indicated the mobile communication device utilizing the SIM card used to take over the victim's account during this SIM swap was assigned the IMEI 359239069326461.

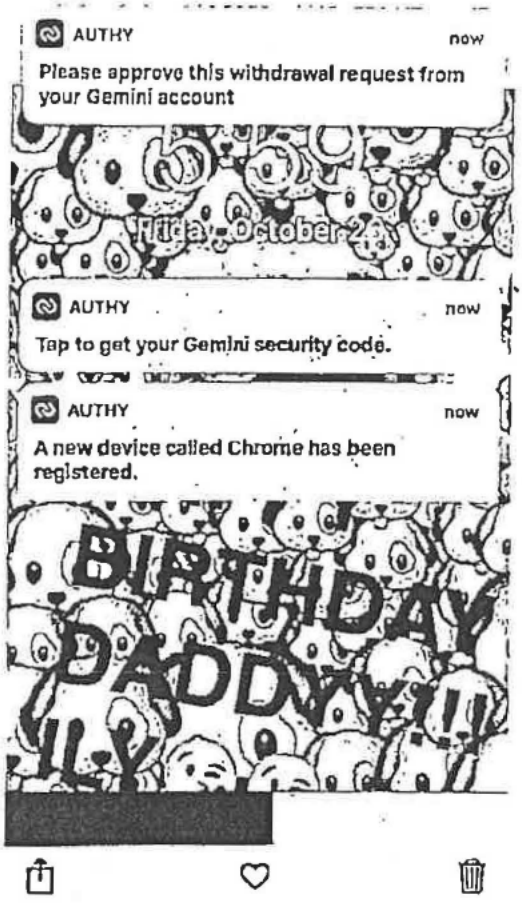
(V) Robert R.

On 10/27/1818, at approximately 0800 hours, I began receiving text messages (depicted below) on my department issued cell phone from a phone number [redacted], which I did not recognize.



I called the number and the voice of a panicked male adult identified himself as (V) Robert R. He gave me the following paraphrased statement over the phone and through email communications:

Robert R. is a resident of [redacted] On 10/26/18, at approximately1800 hours, his cell phone, which uses a phone number ending in -[redacted] started getting notifications from the "Authy" application seen below which the suspect was controlling.



Gemini is a cryptocurrency exchange in which Robert R. had approximately $500,000 USD, and he had approximately $500,000 more was in a similar account with cryptocurrency exchange Coinbase. At approximately the same time he saw the messages above, Robert R. lost cell service, was logged out of and lost access to his Gmail account ([redacted], and the suspects took over his "Authy" 2-factor authentication application. He realized a theft was in progress as he could not access any accounts (Gmail, Authy, AT&T or cryptocurrency accounts). He immediately went to an Apple Store where representatives helped him call AT&T Customer Support, who told the victim his SIM card had been changed. Apple inserted a new SIM into his cell phone and AT&T activated the new SIM card, which restored his access to his own phone service.

When this occurred, all of Robert R.'s funds stored on Coinbase (approximately $500,000) and Gemini (approximately $500,000) had been held in USD. The suspect used all the funds in USD at both exchanges to purchase bitcoins, then immediately withdrew all of the bitcoins. Robert R. found this out by looking at transactions on his CoinTracking account, which is connected to his Coinbase and Gemini exchange accounts. This information was subsequently verified by obtaining records directly from Coinbase and Gemini via search warrant.

Robert R. told me he did not sleep at all that night and was up trying to get access to his accounts, figuring out how to retrieve his stolen money and finding someone to help him with the theft. Although he had access to his phone, he was still locked out of his Gmail account, Authy security application, and all of his cryptocurrency accounts. The money stolen was his life savings and money earmarked for his daughter's college fund. He told me many times that he was not sure how he was going to live the rest of his life and send his daughter to college without this money.

Search Warrant to AT&T for records pertaining to IMEI 359239069326461

On 10/29/18, the Honorable Linda Clark, Judge of the Superior Court, signed a search warrant for AT&T records pertaining to accounts linked to the IMEI number 359239069326461. In response, AT&T provided REACT investigators with records that showed the mobile device bearing that IMEI number had been used to effect the account takeovers of both of the victims described above, Saswata B. and Robert R., as well as those of other victims. In total, the records indicated that 11 unique phone numbers had been SIM swapped using this device between 10/15/18 and 10/26/18.

I spoke with the following additional victims who were among the victims listed and whose accounts were taken over using the device bearing IMEI 359239069326461:

(V) Myles D.

I met with this victim in person on 11/6/18 at approximately 0800 hours, and he related the following. Myles D. lives in [redacted]. On 10/26/18, at approximately 1530 hours, Myles D.'s

AT&T cell phone ([redacted]) stopped working while he was at an appointment. Approximately an hour later he confirmed with his wife that her phone was also not working. At approximately 1700 hours, he went to an AT&T Store to try and resolve the issue. The AT&T Store employee pulled the SIM card from his phone and compared the SIM card to the SIM card listed in the account and realized the numbers were different. The employee changed the SIM card back to the original SIM card number and Myles D. regained access to his cell phone service. Once he had phone service back, he checked his Gmail account ([redacted]) and learned it was disabled by Google. He contacted Google and had his email access restored, and found out that the suspects had accessed his Gmail account for approximately 4 minutes before Google realized the access was unauthorized and Google disabled the account.

At approximately 1800 hours, he returned to his workplace to look into the hack further because he felt using work computers was safer. He looked in his Gmail account and saw an email from an unknown subject with a Gmail address stating this person knew who had hacked him and seemed to be offering assistance. He forwarded that email to Google to see if Google could tell him anything about that account. A short time later he received a telephone call from a blocked number. The voice on the other line stated they were in a "Dark Web" chat room and a group of subjects were talking about going after the victim's cryptocurrency accounts. Myles D. does not have any cryptocurrency but [redacted]. He was scared and believed he was talking to the hackers, and hung up the phone.

On 10/28/18, Myles D. received an email from Fidelity informing him that three of his mutual fund accounts had been liquidated and were pending wire transfers. He contacted Fidelity and was able to cancel the wire transfers. The suspect(s) had attempted to transfer approximately $300,000 from the victim's Fidelity account.

(V) Angel A.

I spoke with this victim via telephone on 11/1/18, and she related the following. Angel A. is a resident of [redacted]. On 10/16/18, her AT&T cell phone number [redacted] stopped

working. A short time later she realized she had lost access to her Twitter social media account ([redacted]). The suspect who was in control of [redacted] began sending bomb threats to airlines from her Twitter account along with racist "Tweets" regarding Former President Barack Obama. The victim contacted Twitter and regained access to her account. She is unaware of any other accounts that were compromised.

(V) James M.

I spoke with this victim via telephone on 11/1/18, and he related the following. James M. is a resident of [redacted]. On 10/15/18, his AT&T cell phone number ([redacted]) stopped working. He received an email from Instagram that the password was changed for his Instagram username ([redacted]) and the email account associated to his [redacted] Instagram account was changed to fuhedam@zdenka.net. The suspect attempted to access his Facebook account, but Facebook stopped the attempt. He believes somebody with the Instagram account @gay hacked him because the victim was taunted on his new Instagram Account by that user via Instagram Direct Message for having lost access to [redacted]. The victim was never able to regain access to [redacted] which he had used for business purposes.

(V) Gabrielle K.

I spoke with this victim via telephone on 10/30/18, and she related the following. Gabrielle K. is a resident of [redacted]. On 10/21/18, her AT&T cell phone number ([redacted]) stopped working. She noticed this when she woke up and her had phone no service. She received an email from AOL that her password was changed and a Gmail notification that her Gmail, Evernote and Dropbox passwords had changed. She also received a notice that her Coinbase cryptocurrency account login information had changed. She was able to disable her Coinbase account before any further actions were taken by the suspect. She then went to an AT&T Store to get a new SIM card.

(V) Matthew R.

I spoke with this victim via telephone on 11/2/18, and he related the following. Matthew R. is a resident of [redacted]. On 10/23/18, his AT&T cell phone number ([redacted]) stopped