working. While he was still connected on Wi-Fi, he received emails that his email account passwords were reset. He was still logged into those accounts while the suspect was simultaneously in control. He saw emails saying other accounts connected to the email were being reset. Those accounts included [redacted] and [redacted] The suspect also attempted to gain access to his Coinbase, HitBTC, Binance and Bittrex cryptocurrency accounts and his blockchain cryptocurrency wallet. The suspects called him twice asking for blackmail payments of $200,000 in Bitcoin to get all his accounts back. One of the suspects sounded young and Asian and the second suspect sounded Eastern European and seemed like he was trying to disguise his voice.

Suspect telephone number (732) 456-2221 and identification of (S) Nicholas TRUGLIA

Records provided by AT&T also indicated that the when the suspect's phone was in control of the identified victim accounts, the phone was located in the New York, New York area. In addition, the records indicated that the phone number 732-456-2221 was connected to the suspect IMEI (359239069326461) on 10/5/18, but that this connection was not reported as a fraudulent SIM Swap by the customer. I believe this is indicative of the suspect using a SIM card in his/her possession to test whether the cell phone is functioning properly and connects to the cell carrier's network. I therefore believe the phone number 732-456-2221 belonged to the suspect.

On 10/26/18, the Honorable Maureen Folan, Judge of the Superior Court, signed a search warrant for AT&T records pertaining to the account associated with the telephone number 732-456-2221. AT&T provided REACT investigators with records that identified the subscriber as "Jeffrey St. Denis" and included the additional information described below.

On 10/29/18, the cryptocurrency exchange Coinbase provided records to investigators which identified an account associated with the phone number 732-456-2221, the number believed to be associated with the suspect. These records indicated this phone number was used to register a Coinbase account in the name of Nicholas TRUGLIA using the social security number [redacted] and the email

address nick.truglia@me.com. Another name associated with the account was Jeffrey St. Denis, the same name as shown in AT&T subscriber records for the suspect phone number. The records also included copies of documents the subscriber used to identify himself, which included a Connecticut Driver License in the name of Nicholas TRUGLIA with a date of birth of 9/25/96 and a U.S. passport in the name of Nicholas St. Denis TRUGLIA (note the middle name that matches the name used in AT&T subscriber information from the suspect account) with a date of birth of 9/25/97.

TRUGLIA's Coinbase account also showed deposits and withdrawals of cryptocurrency occurring between 1/6/16 and 3/24/18, and then no activity after 3/24/18 until 10/27/18. On 10/27/18, mere hours after the theft of the bitcoins described above, as well as approximately 14.3 Ether ("ETH") from (V) Robert R.'s account with the cryptocurrency exchange Binance, a small amount of Ether (approximately .025 ETH) was deposited into TRUGLIA's Coinbase account. Santa Clara County District Attorney Investigator D. Berry received records pertaining to Robert R.'s account from Binance on 10/27/18 that reflected the 14.3 ETH theft from Robert R.'s account, although that stolen ETH was transferred only once to an exterior address, and has not moved from that address as of the writing of this report.

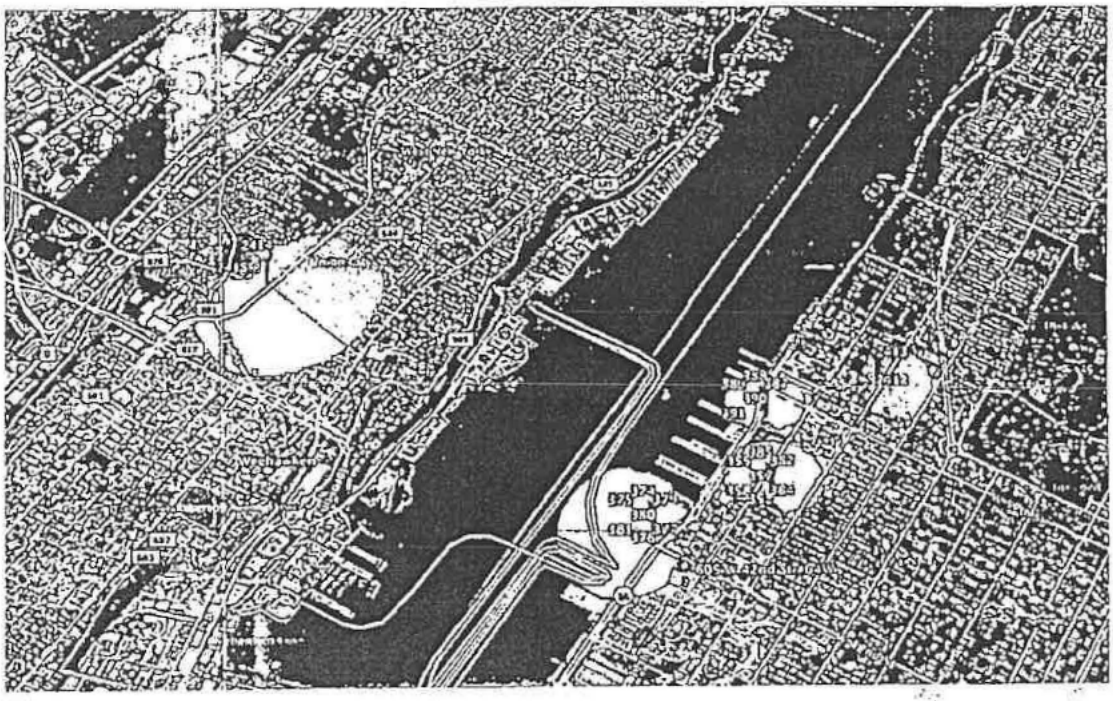
On 11/6/18, REACT investigators received records from the State of New York showing Nicholas TRUGLIA had a New York State Identification Card which listed an address of 605 West 42ND Street 64W, New York, New York 10036.

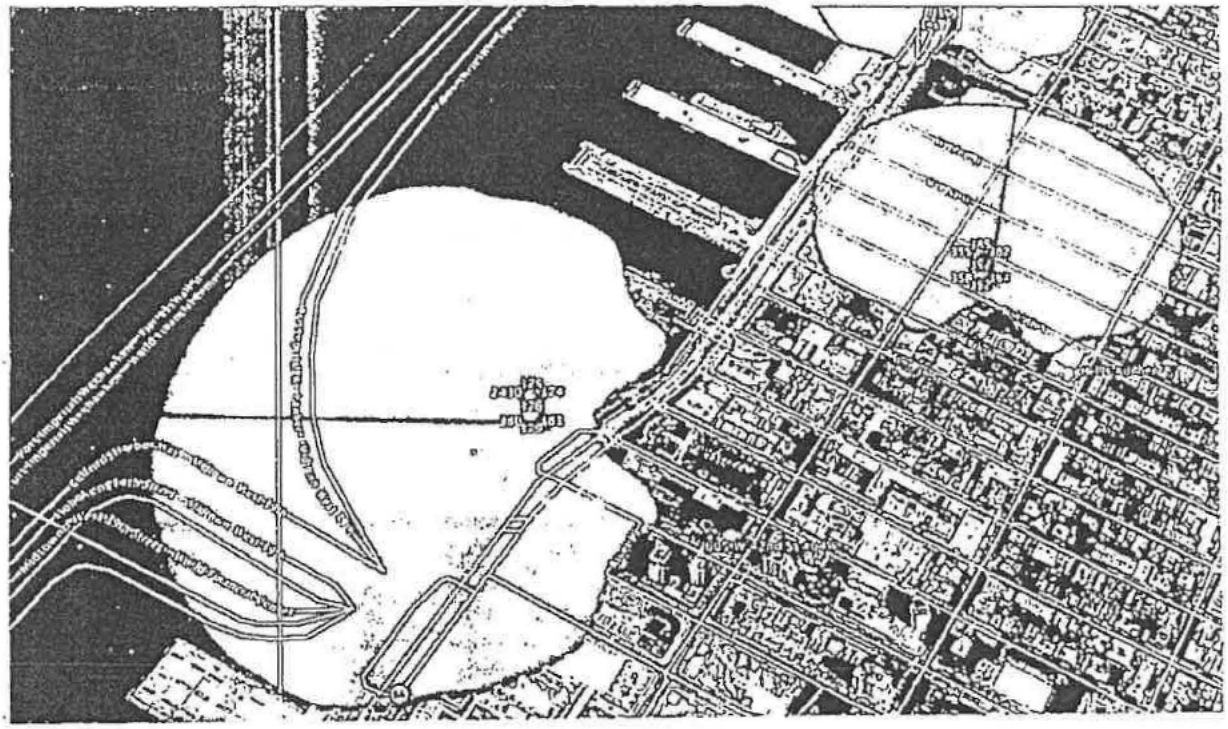
Sgt. Tarazi examined the records obtained from AT&T and arrived at the following conclusions, in summary (see Sgt. Tarazi's supplemental report for details):

- The records pertaining to TRUGLIA's cell phone account (732-456-2221) indicate the owner of the AT&T phone number 732-456-2221 was assigned a SIM card that was physically inserted into an iPhone X with IMEI ending in -5311. Someone removed the SIM card form this iPhone X and placed it inside an iPhone 6 with IMEI ending in -6461, which is the device used to effect the SIM swaps. After approximately 18 minutes, someone removed the SIM

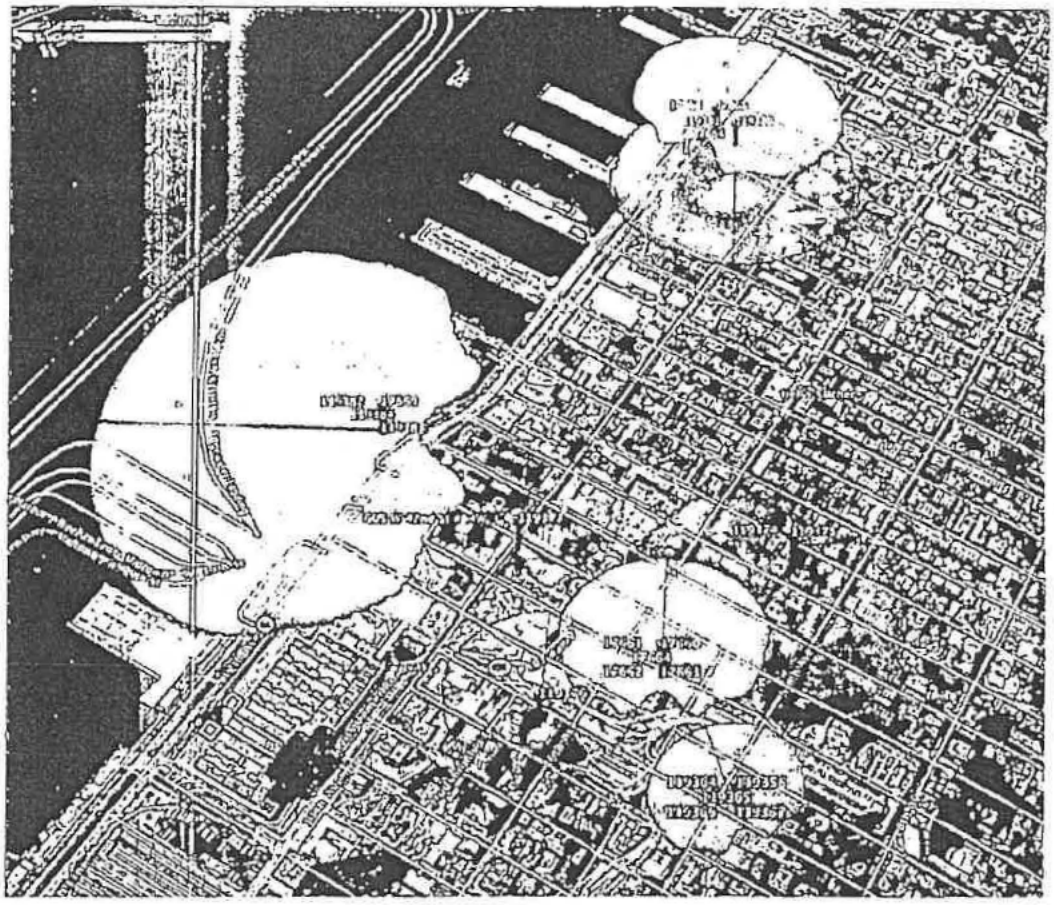
card from the iPhone 6 (-6461) and put it back into the iPhone X (-5311). This SIM card has remained inside the iPhone X (5311) since it was put back in.

- The AT&T cell phone towers to which the iPhone 6 (6461) was connected during the approximate 2 hours and 10 minutes it was in control of victim Matthew R.'s account was consistent with the device having been located at 605 W 42nd Street, #64W, New York, NY, as depicted below:



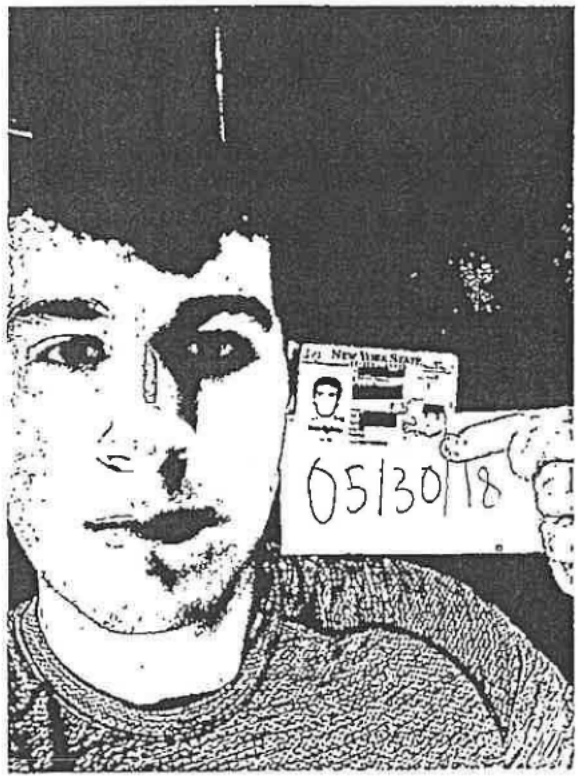


- During that same time period, that same AT&T cell phone tower, as well as several other nearby towers, were used by the iPhone X associated with TRUGLIA's account (5211), as depicted below.



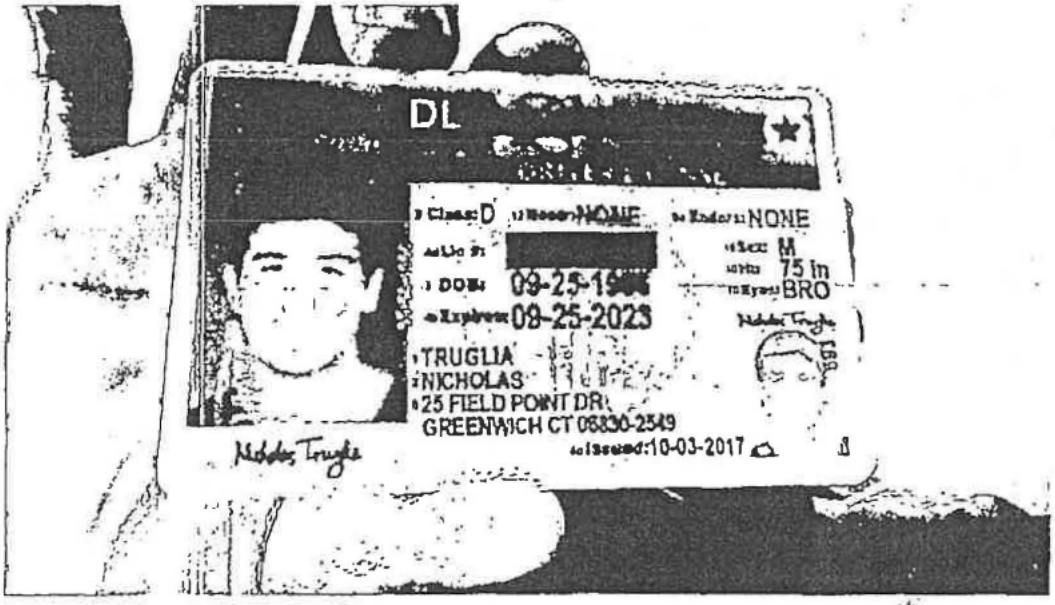
Prior Attempted Account Takeover involving TRUGLIA

On 10/31/18, Coinbase provided additional information indicating that Truglia has previously been involved in account takeover activity. Coinbase informed REACT investigators that in mid-May 2018, Coinbase received an anonymous tip that someone was going to hack into the Coinbase account of Quinten Capobianco, who had previously died. After Coinbase secured the target account, an external attempt was made to access the account. Coinbase prompted the suspect to provide a photograph of himself holding his ID card as verification, and in response the suspect provided the photograph below.



Based on a comparison to known images, I recognize the person in the photograph above as Nicholas Truglia, who is holding what appears to be a false New York State driver license in Capobianco's name but bearing Truglia's image. Furthermore, Coinbase records indicated that the same device that attempted to access Capobianco's account was then used to log into Truglia's account.

The following three photos were provided as proof of identity for the other Coinbase accounts opened in Truglia's name:


DL
Class: D
NONE
M
75 in
BRO
09-25-2023
TRUGLIA
NICHOLAS
25 FIELD POINT DR
GREENWICH CT 06830-2549
Issued: 10-03-2017

The following picture is from Truglia's New York Identification, which was obtained through a law enforcement database.

DMV Photo Request

DMV Photo

Subject Information	
Name:	TRUGLIA,NICHOLAS,S
ClientID:	161405797
Case Number:	108711
DMV Transaction Number:	756281
DMV Transaction Date/Time:	2018-11-05 15:38:31:767

Back

I believe all of the pictures above depict Truglia.

Based on this information, I believe Suspect Truglia attempted to access the deceased person's Coinbase account. This behavior is consistent with the SIM Swapping activity described in this report in the use of impersonation techniques to steal cryptocurrency.

Laundering of stolen funds

Santa Clara County District Attorney Criminal Investigator D. Berry, a REACT Task Force investigator, has examined the flows of cryptocurrency out of Robert R.'s Coinbase, Gemini, and Binance accounts. Investigator Berry observed that the bitcoins transferred out of his Coinbase and Gemini accounts were initially aggregated into a single Bitcoin address, and then moved in a series of transactions that appear intended to obfuscate the source and destination of funds. After some of those layers of movement, proceeds of the theft were deposited into accounts at Binance, a cryptocurrency exchange based in Malta, in a series of transactions apparently structured to avoid account registration requirements (just under 2 bitcoins per transaction, which is the limit above which an account involving "customer due diligence" must be established). Binance provided information related to those transactions, which showed that a series of accounts exhibiting similar behavior had received,

and then promptly withdrawn, the identified stolen bitcoins, which were then aggregated into some overlapping Bitcoin addresses. *See Investigator Berry's supplemental report for additional details.*

Based on my training and experience, I know that moving stolen cryptocurrency through multiple addresses, breaking up stolen amounts into multiple segments of smaller amounts, structuring flows to avoid reporting requirements, and taking steps to avoid meaningful customer due diligence are all consistent with money laundering efforts.

CONCLUSION

Based on the statements of the victims, IMEI number 359239069326461 being connected to S-TRUGLIA's personal cell phone line, Sgt. Tarazi's analysis of phone records, and Investigator Berry's analysis regarding cryptocurrency tracing, I believe S-TRUGLIA committed the following crimes detailed below:

V-Ross:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Gmail account

487(a) PC – Theft of approximately $500,000 from his Coinbase account

487(a) PC – Theft of approximately $500,000 from his Gemini account

V-Anderson:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Twitter account and sending messages

V-Danielson:

502(c)(1) PC and 530.5(C) PC – Unlawfully Accessing Gmail account