502(c)(1) PC and 664/487(a) PC – Unlawfully Accessing Fidelity Mutual Fund and attempting to wire $300,000 from the account

V-Katsnelson:

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

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

502(c)(1) PC – Unlawfully Accessing Evernote account

502(c)(1) PC – Unlawfully Accessing Coinbase account

V-Basu:

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

664/502(c)(1) PC– Unlawfully Attempting to Access Dropbox account

I am requesting the Santa Clara County District Attorney's Office issue a warrant for the arrest of S-TRUGLIA for the above listed charges.

END REPORT.

PLEO:

TFA C. Tuttle #1945 – Original report
TFA S. Tarazi #2029 – Cell Tower/Geolocation Supplemental Report
TFA D. Berry #47 – Cryptocurrency Tracing Supplemental Report

# Regional Enforcement Allied Computer Team
# INVESTIGATION REPORT:
# NARRATIVE

Supplemental Report

Investigation:

On 10-27-2018, REACT detectives received a spreadsheet file from AT&T Fraud Investigator Robert Arno entitled "359239069326461 updated 102718." The first number represents an IMEI number that had been used to conduct SIM swaps. These phone numbers had been identified by AT&T as being used on the above listed IMEI, belonging to an iPhone 6. This IMEI will be referred to by the last 4 digits (6461) throughout the report.

| Mobile Number | SIM Card Number | First Use Date |
|---|---|---|
| [redacted] | [redacted] | Fri Oct 26 19:50:27 EDT 2018 |
| [redacted] | [redacted] | Fri Oct 26 17:41:20 EDT 2018 |
| [redacted] | [redacted] | Wed Oct 24 20:37:24 EDT 2018 |
| [redacted] | [redacted] | Tue Oct 23 19:44:54 EDT 2018 |
| [redacted] | [redacted] | Mon Oct 22 23:48:25 EDT 2018 |
| [redacted] | [redacted] | Sun Oct 21 12:50:23 EDT 2018 |
| [redacted] | [redacted] | Thu Oct 18 15:37:36 EDT 2018 |
| [redacted] | [redacted] | Tue Oct 16 14:35:07 EDT 2018 |
| [redacted] | [redacted] | Mon Oct 15 19:30:26 EDT 2018 |
| [redacted] | [redacted] | Mon Oct 15 18:31:02 EDT 2018 |
| [redacted] | [redacted] | Mon Oct 15 15:22:49 EDT 2018 |
| (732) 456-2221 | 310410074713285 | Fri Oct 05 19:24:43 EDT 2018 |

Each number above, except for 732-456-2221, was identified by Robert Arno as being an account victimized by an unauthorized SIM Swap by the IMEI ending is 6461. Several of the numbers above have been identified as victims of cryptocurrency theft. See Detective Tuttle's Supplemental Report for further details.

The number 732-456-2221 has been identified as belonging to Suspect Truglia. The phone number had been used to register for a PayPal and Coinbase account in Suspect Truglia's name. See Detective Berry's Supplemental report for further details.

I authored and served a Search Warrant for AT&T records regarding IMEI number ending in 6461 (iPhone 6). I received partial record returns which included the call detail records for the phone number [redacted] and the subscriber information for the rest of the numbers listed above.

Detective Tuttle authored and served a Search Warrant for AT&T records regarding the phone number 732-456-2221 (Suspect Truglia's AT&T phone number).

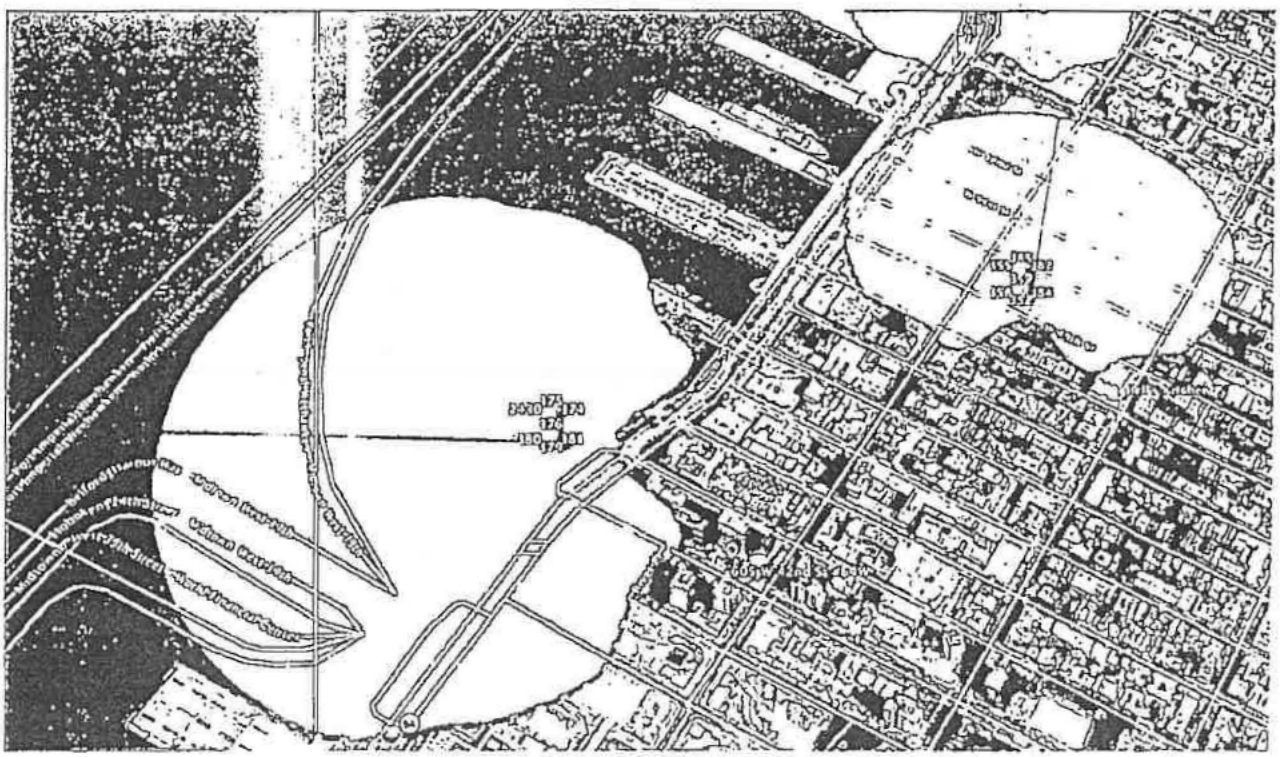
I examined the call detail records for Suspect Truglia's phone line and I noticed that on 10-5-18 at 23:24:43 (UTC) the IMEI number on the account switched from 354851092905311 (iPhone X) to the iPhone 6 ending in 6461. The records indicate the IMEI switched back to the iPhone 10 (5311) at 23:43:54 (UTC), approximately 18 minutes later. The iPhone X (5311) has been assigned to the Suspect Truglia's account since it switched back.

These records mean the owner of the AT&T phone number 732-456-2221 linked to Suspect Truglia was assigned a SIM card that was physically inserted into the iPhone X (5311). Someone removed the SIM card form this iPhone X and placed it inside the iPhone 6 (6461). 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.

I examined the call detail records for the phone number [redacted] and I noticed that 10-23-18 at 22:09:35 (UTC) the IMEI switched from [redacted] (iPhone 10) to the iPhone 6 (6461). This IMEI remained active on the account until it switched back to the original IMEI number on 10-25-18 at 01:35:16, approximately 2 hours 25 minutes later. This time span is reasonable to explain the victim losing reception on his/her phone, realizing what happened, contacting AT&T and disconnecting the illegally connected phone from their account.

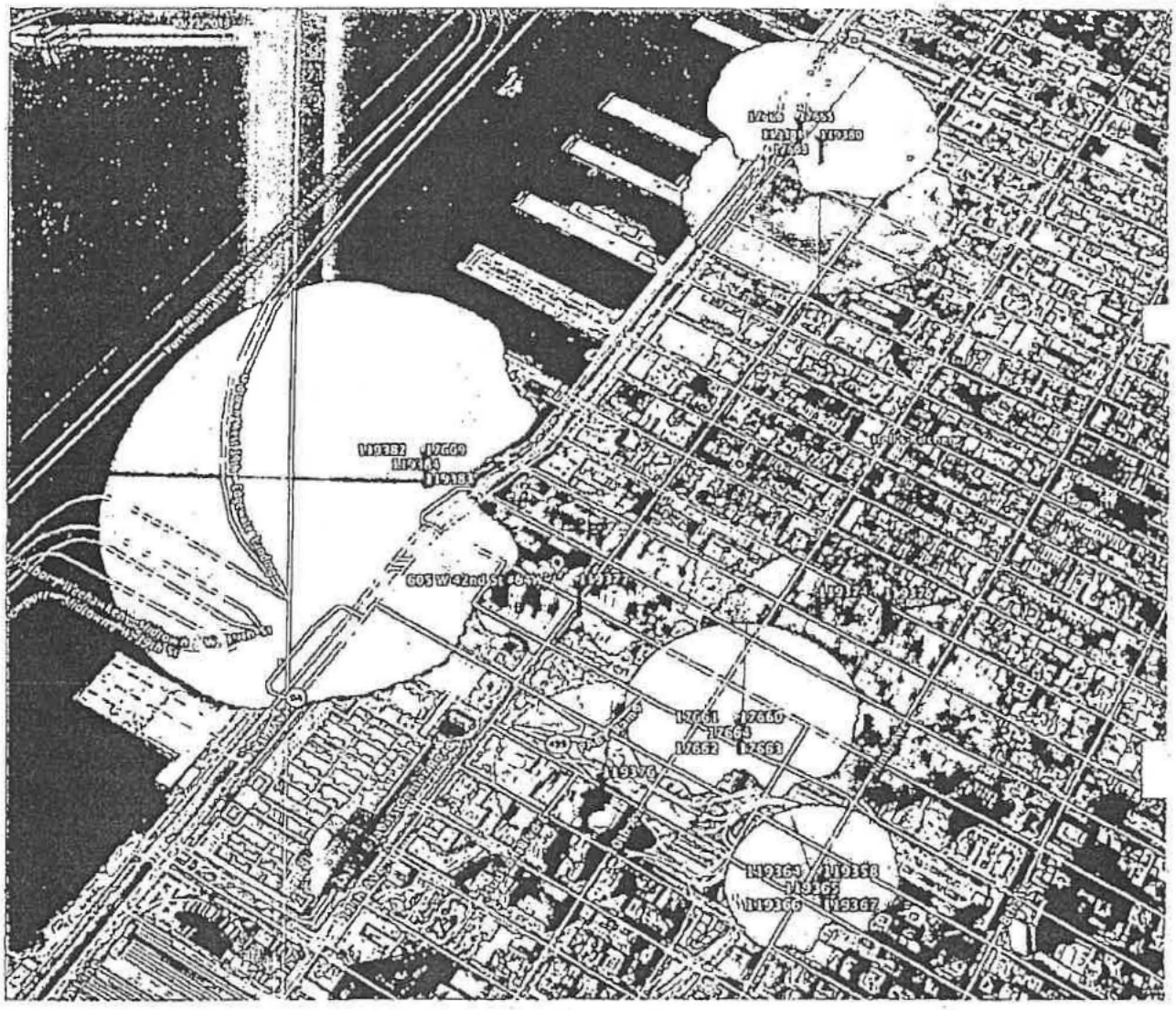
I examined the geolocation data provided by AT&T for two phone numbers discussed above.

The following pictures depict the AT&T cell phone towers the iPhone 6 (6461) was connected to during the approximate 2 hours and 10 minutes it was in control of the victim's account ([redacted]). The address 605 W 42nd Street, #64W, New York, NY is placed for reference as it is listed as Suspect Truglia's residential address on his New York issued Identification Card.



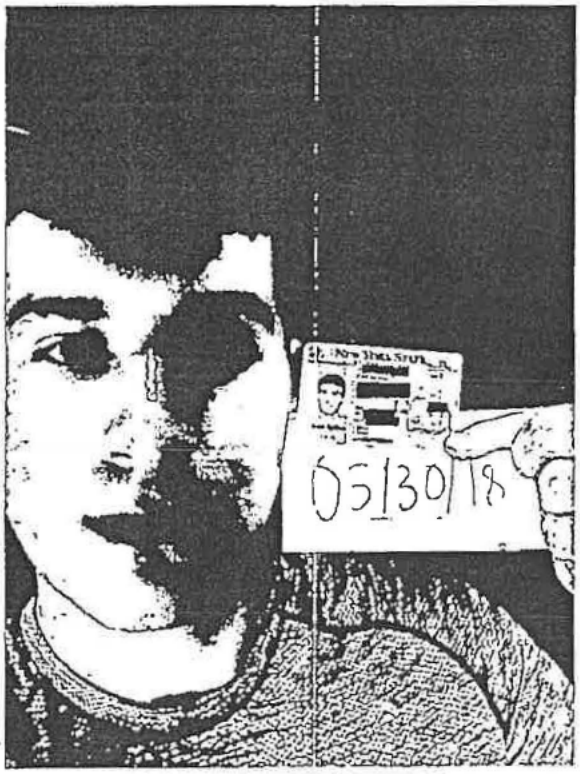
The tower to the west of 605 W 42nd Street is identified by LTE ECGI-ENBID: 28486920-111277.

I further examined the geolocation data for Suspect Truglia's AT&T records for the same time period depicted above (approximately 2 hour 10 minute time window).




The same AT&T tower LTE ECGI-ENBID: 28486920-111277 was used by Suspect Truglia's AT&T account as well as several nearby towers. This is consistent with both devices being in the same geographical area at the same time.

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.




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


D
NONE
M
75 in
BRO
08-25-2023
TRUGLIA
NICHOLAS
25 FIELD POINT DR
GREENWICH CT 06830-2549
10-03-2017


The following picture is from Suspect 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 depicted above are of Suspect 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 described in this report as the ultimate goal of the SIM Swapping is to steal cryptocurrency.

Based on the information above, I believe Suspect Truglia to have been in possession of the iPhone 6 (6461) and iPhone X (5311) described above and is responsible for conducting the SIM Swaps listed on page 1 of this report. See Detective Tuttle's Original report for further information.

END REPORT

PLEO:

Sgt. S. Tarazi- 2029