2021R01133/JLS

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. Andre M. Espinosa
	:	
v.	:	Mag. No. 22-11181
	:	
RICHARD FORREST SHERMAN	:	**CRIMINAL COMPLAINT**

I, Gregory Pico, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the United States Secret Service, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Gregory Pico, Special Agent
United States Secret Service

Special Agent Pico attested to this Affidavit by telephone pursuant to F.R.C.P. 4.1(B)(2)(A) on this 25th day of July, 2022.

S/ Andre M. Espinosa

Hon. Andre M. Espinosa
United States Magistrate Judge

ATTACHMENT A

Count One
(Wire Fraud Conspiracy)

From at least as early as in or around February 2013 through in or around October 2020, in the District of New Jersey, and elsewhere, defendant,

RICHARD FORREST SHERMAN,

knowingly and intentionally conspired and agreed with others to devise a scheme and artifice to defraud, and to obtain money and property from victims by means of false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce certain writings, signs, signals, pictures, and sounds, including a wire communication sent on or about June 26, 2019, from a location outside of New Jersey to a location in New Jersey, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Gregory Pico, am a Special Agent of the United States Secret Service. The information contained in the complaint is based upon my personal knowledge, as well as information obtained from other sources, including: (a) statements made or reported by various witnesses with knowledge of relevant facts; (b) my review of publicly available information; and (c) my review of evidence. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where the contents of documents and the actions and statements of others are reported herein, they are reported in substance and in part, except where otherwise indicated. Where I assert that an event took place on a particular date or time, I am asserting that it took place on or about the date or time alleged.

1. At all times relevant to this Complaint:

a. Richard Forrest Sherman ("Sherman") was a resident of either Salem, Oregon or Boerne, Texas.

b. Sherman, with others, operated and held an interest in several different corporate entities, including Eluviis LLC, Deletype LLC, Incendit LLC, and Dashing Corporation.

c. The "Victim Carrier" was a multinational telecommunications company that offered, among other services, cell phone services to millions of customers.

d. The Victim Carrier installed locking software on the devices it sold to customers. The locking feature barred the devices from being used with any carrier besides the Victim Carrier. This locking feature was important to the Victim Carrier because it typically sold cellular phones to purchaser's pursuant to an installment plan, and if a purchaser failed to make required payments on their contract, the Victim Carrier could use the software to lock the purchaser's phone and render it unusable. From a purchaser's perspective, unlocked cellular telephones were more valuable than a locked cellular telephone, in part, because an "unlocked" cellular telephone could be used with any compatible carrier. Thus, unlocking cellular telephones could enable one to, among other things, use it with any compatible carrier, avoid long-term contracts, and use prepaid services.

e. The "Technology Company" was a multinational technology company that provided, among other things, computer software and consumer electronics.

f. The "Joint Venture Company" was a joint venture between Technology Company and another legitimate company.

g. "Employee-1" was an employee of Victim Carrier. Employee-1 also worked with Sherman in connection with Sherman's entity Dashing Corporation as the Director of Business Development.

h. The "Cayman Company" was a company that purported to be located in the Cayman Islands and resold mobile data subscriber identity modules ("SIMs") around the world. The Cayman Company was controlled by two Canadian citizens ("Canadian-1" and "Canadian-2").

i. "Indicted Co-Conspirator-1" was an individual residing in Texas who managed and owned Unlockdon Distributor LLC and Mundo Wireless, entities that were used to facilitate phone unlocking services. On or about May 12, 2022, an indictment was returned in the U.S. District Court for the Eastern District of Texas charging Indicted Co-Conspirator-1 with participating in a phone unlocking scheme.

j. All wire transfers processed through the Fedwire Funds Service ("Fedwire") were processed in a way that caused an electronic communication to travel through a Federal Reserve facility in New Jersey.

Sherman's Fraud Scheme

2. Sherman, while he was employed by the Victim Carrier, exploited an exemption that the Victim Carrier provided to the Technology Company to unlock the SIM cards of mobile devices. Sherman exploited this exemption in order to trick the Victim Carrier into unlocking the SIM cards of thousands of mobile devices. Sherman and his coconspirators used the exemption to unlock phones and resell them. Sherman's entities received money in exchange for unlocking IMEIs, which he accomplished by exploiting the Victim Carrier's exemption.

3. Sherman worked for the Victim Carrier between in or around 2009 and in or around 2014. At the time he left the Victim Carrier, Sherman held the title of Global Account Manager – Strategic Accounts. During the course of his employment with the Victim Carrier, Sherman managed a client account of the Technology Company.

4. The Victim Carrier generally would process mobile device unlocking ("MDU") services for customers, when eligible, to allow them to use other phone carriers' SIM cards in their devices. To be eligible for the unlocking services: (1) the IMEI could not be blocked; (2) the device had to have been sold by The Victim Carrier and not another carrier; (3) the device IMEI had to show network usage on the line of service requesting the unlock; (4) at least 40 days or longer had passed since the device was first used on the

mobile number requesting the unlock; (5) the customer's account had to be in good standing (active and not past due) at the time the unlock was requested; and (6) the financial obligations of the device payment plan had to be met fully, reflecting a $0 balance.

5. This case-by-case assessment was important for the Victim Carrier because, if a SIM card was unlocked without a phone carrier's approval, that phone could later be reactivated by another user, even if the outstanding balance with the phone carrier remained unpaid.

6. When the Victim Carrier sold electronic devices to its customers, customers could elect to enter into an Equipment Installment Plan ("EIP") agreement by which the customer agreed to pay an amount each month towards the outstanding balance on their device until it was paid in full. If the customer failed to make those payments, the device would remain "locked" to the Victim Carrier and could not be used on another carrier's mobile network. Permitting the Victim Carrier the ability to lock devices that retained an outstanding balance on the EIP agreements provided the Victim Carrier with the leverage to collect on these unpaid balances owed to the company.

7. The Victim Carrier maintained a special exception to its MDU unlocking policy for the Technology Company. As a result, the Technology Company's accounts were not required to undergo the typical review process to determine MDU eligibility. Instead, a special process was established for the Technology Company and its affiliate entities that permitted the Technology Company to submit MDU requests that were not reviewed individually on a case-by-case basis to ensure that they met The Victim Carrier's eligibility requirements for MDUs.

8. Sherman exploited the Technology Company's special exception to the Victim Carrier's MDU unlocking policy by creating a series of accounts for a customer that appeared to be an affiliate of the Technology Company but was not. Sherman and others then submitted bulk MDU requests through these fake affiliate accounts that Sherman set up before leaving the Victim Carrier. Sherman, through his entities, received payment from others in exchange for causing the fake affiliate account to successfully send IMEIs in bulk to the Victim Carrier. The Victim Carrier, believing that the fake affiliate company was entitled to the MDU unlocking exception, unlocked these IMEIs in bulk. The Victim Carrier unlocking these IMEIs permitted others to resell phones for profit that otherwise would have remained locked and/or sell their ability to unlock phones for a fee. Sherman and his coconspirators exploited the fraud scheme until it was discovered in or around August 2020.

9. Sherman identified a legitimate account for the Joint Venture Company, which was treated as an affiliate account of the Technology Company. According to records and information received from The Victim

Carrier, in or around February 2013, Sherman requested that a billing account number ("BAN") be created that mirrored Joint Venture Company's BAN. Thereafter, Sherman requested that the account names be changed from the Joint Venture Company's name to a hybrid of "[Joint Venture Company] – Quantive Solutions" and then to simply "Quantive Solutions." Sherman also requested that the billing address and contact names for the Quantive Solutions BANs be changed several times. Over time, additional BANs were created for Quantive Solutions with this changed information, but the Tax-ID for the Joint Venture Company was kept in place on the Quantive Solutions accounts.

10. The BANs for Quantive Solutions, as a result of their being mirrored from a legitimate Technology Company affiliate account, enjoyed the same special exception to Telecommunication Company-2's MDU policy. In other words, requests for MDUs that were processed through Quantive Solutions' BANs were processed without being reviewed.

11. As a part of the scheme, Sherman requested that certain email addresses be added to the Quantive Solutions accounts as points of contact for the BAN. In or around June 2014, Sherman requested that several BANs opened for Quantive Solutions were notated to allow "Mark Cooper" and "anyone emailing from the DSG alias," and "anyone calling and identifying themselves as DSG Support Tech" to make changes on all of the Quantive Solutions accounts. This included emails to and from someone identifying themselves as "Mark Cooper" at m.cooper@quantivesolutions.com and various individuals using the account "dsglabsupport@quantivesolutions.com." The title line of Sherman's request identified Quantive Solutions as an affiliate of the Technology Company and the display name of m.cooper@quantivesolutions.com was "Mark Cooper ([Technology Company])," suggesting that Cooper was affiliated with the Technology Company.

12. Sherman left the Victim Carrier in or around June 2014 after setting up the Quantive Solutions BANs to ensure that they received the MDU exception and appeared to be a Technology Company affiliate when, in fact, they were not.

13. Individuals using the Quantive Solutions email accounts submitted MDU requests in bulk to the Victim Carrier. Records obtained for accounts "m.cooper@quantivesolutions.com" and "dsglabsupport@quantivesolutions.com" indicate that these email accounts were opened and used for the purpose of duping the Victim Carrier into processing bulk MDUs.

14. Near the end of 2014, other employees at the Victim Carrier became suspicious of the Quantive Solutions BANs. On or about December 1,

2014, Employee-1 forwarded an email to m.cooper@quantivesolutions.com stating that the following message had been sent to him:

> We've had several unlock requests for the iPhone 6 for [Joint Venture Company] QUANTIVE SOLUTIONS BAN [Redacted] that are suspicious. Shortly after requesting the unlock codes for this account we are receiving Handset Research requests stating customers on other accounts never received the devices (orders were never received). It appears that they may be using this account to obtain unlock codes for devices on other accounts. Can you please review and let me know your thoughts? I normally would reach out to Richard as he set up the process for [Redacted] and it's Affiliate's (this account being one of them) but it appears he may no longer be with [Victim Carrier]. Below are examples of some of these IMEI's that were requested. We were able to deny these as IMEI Blocked; however wanted to attempt to stop anything fraudulent that may be happening. Thank you for your assistance [Employee-1]!

15. On December 8, 2014, Employee-1 emailed "Mark Cooper" at Quantive Solutions with another email he had received from a Victim Carrier employee asking whether Quantive Solutions was an affiliate of the Technology Company. Employee-1 responded to this employee that Quantive Solutions was an affiliate of the Technology Company, which was not true.

16. Quantive Solutions continued to submit bulk MDU requests through the Victim Carrier BANs reflecting it was a Technology Company affiliate, while Sherman's co-conspirators sent money to accounts in the names of entities affiliated with Sherman. For example:

a. On or about September 15, 2015, the Cayman Company wired through the Fedwire System approximately $99,980.00 to a bank account held in the name of Incendit LLC, another one of Sherman's entities.

b. On or about November 17, 2015, the Cayman Company wired through the Fedwire System approximately $99,980.00 to a bank account held in the name of Incendit LLC.

c. On or about February 3, 2016, the Cayman Company wired through the Fedwire System approximately $99,980.00 to a bank account held in the name of Incendit LLC.

d. On or about May 23, 2017, the Cayman Company wired through the Fedwire System approximately $199,980.00 to a bank account held in the name of Incendit LLC.

e. Records reflect that Paypal accounts associated with Cayman Company and Canadian-1 sent over $2.5 million to a Paypal account controlled by Sherman in the name of Incendit LLC between 2017 and 2019.

17. Records obtained during the investigation revealed that through the course of the scheme, Indicted Co-Conspirator-1 would send a list of IMEIs that needed to be unlocked to the Cayman Company. The individual using m.cooper@quantivesolutions.com would email that list of IMEIs to dsglabsupport@quantivesolutions.com. Email account dsglabsupport@quantivesolutions.com then submitted the list of IMEIs to the Victim Carrier in bulk under the Quantive Solutions BANs, which the Victim Carrier would process and unlock, falsely believing that the unlock requests were coming from a Technology Company affiliate account. Thereafter, a financial account in the name of an entity affiliated with Sherman received money. For example:

a. On or about June 16, 2019, Indicted Co-conspirator-1 emailed Canadian-1 using one of Canadian-1's business email addresses a list of IMEIs, with the title "[The Victim Carrier] Unlockdon imei list All Model $]25 (06/17/2019)."

b. On or about June 17, 2019, at approximately 12:54, m.cooper@quantivesolutions.com emailed the same list of IMEIs previously sent to Canadian-1's business referenced in the preceding paragraph to dsglabsupport@quantivesolutions.com with the instructions: "Ready to submit."

c. On or about June 17, 2019, at approximately 2:07 pm, dsglabsupport@quantivesolutions.com emailed to the Victim Carrier an excel spreadsheet of the IMEIs referenced in the preceding paragraph and in the subject of the email wrote: "[Technology Company] Affiliate Quantive IMEI Unlock Process[.]"

d. On or about June 19, 2019, a representative of the Victim Carrier sent an email back to dsglabsupport@quantivesolutions.com with an attachment of the unlocked IMEIs that were requested in the preceding paragraphs above. The email reflects internal discussions among members of the Victim Carrier that reflect they believed the MDU request was being made by a Technology Company affiliate.

e. On or about June 22, 2019, Canadian-1's business email sent an email to Indicted Co-Conspirator-1 with a list of the

unlocked IMEIs reflected in the email referenced by the preceding paragraph and required payment for each unlocked IMEI.

f. On or about June 26, 2019, Canadian-1's business email sent an invoice to Indicted Co-Conspirator-1. The invoice was issued by Incendit LLC—one of Sherman's companies—in the approximate amount of $52,361.01 for "Mobile Software Services."

g. On or about the same day, a bank account controlled by Indicted Co-Conspirator-1 wired through the Fedwire system approximately $52,361.01 to a business bank account in the name of Incendit LLC.

18. While Sherman and his coconspirators funneled the IMEI requests through several different email accounts, including accounts that appeared to be managed by "Quantive Solutions" in an attempt to make it appear that the unlocking requests were properly within the Victim Carrier's MDU exception applicable to a Technology Company affiliate, records collected in the course of the investigation reflect that "Quantive Solutions" was a fake entity, and that Sherman and Sherman's entities were involved in the fraud throughout the course of the scheme. For example:

a. Email account m.cooper@quantivesolutions.com was created on or about June 10, 2014 at 18:37:33, while dsglabsupport@quantivesolutions.com was created on or about June 10, 2014 at 18:42:48 from the same IP address. The last logins to both accounts correspond to the time period in 2020 when the Victim Carrier and the Technology Company discovered the fraud and confronted the representatives of "Quantive Solutions" via these accounts.

b. On or about July 2, 2014, m.cooper@quantivesolutions.com sent an email to Sherman at his Victim Carrier email address. After not receiving any response (likely because, around this time Sherman had left the Victim Carrier's employment), on or about July 9, 2014, "Mark Cooper" sent an email to dsglabsupport@quantivesolutions.com that said: "He[y] do you know if this list was ever checked and submitted? I don't have a reply from you on it and it appears they are still locked."

c. On or about September 22, 2014, dsglabsupport@quantivesolutions.com engaged in an email exchange with another email account (the "Gift Card Email Account") about purchasing a large number of gift cards. The

Gift Card Email Account received a message from Paypal that Eluviis LLC—one of Sherman's entities—had sent money to the user of the Gift Card Email Account from Paypal. The verified customer listed for the Eluviis LLC Paypal account was Canadian-1.

d. On November 29, 2015, dsglabsupport@quantivesolutions.com sent an email to "Richard@eluviis.com" with the subject: "Eluviis LLC Annual Meeting Minutes." The minutes state: "Possible transfer of software developing work to new entity (possible name is Deletype)" and "New ownership to be 50% [Redacted] and 50% Richard Sherman."

e. On or about June 28, 2016, dsglabsupport@quantivesolutions.com responded to an email from the Victim Carrier. Header data from that email reflected that the email was sent by: Eluviiss-MacBook-Air.local.mail.

f. On September 26, 2016, dsglabsupport@quantivesolutions.com emailed a Deletype email address asking: "How many more do we have of those. Need to send a couple of batches out" with the Subject: "White Sims".

g. On or about January 23, 2017, dsglabsupport@quantivesolutions.com sent an email to a Deletype email address that forwarded unlock information for "[Technology Company] Affiliate Quantive IMEI Unlock Process" at The Victim Carrier. The email contained a spreadsheet with unlocked IMEIs for Apple devices.

h. On April 4, 2017, dsglabsupport@quantivesolutions.com sent an email requesting: "Can you ask them to pay this one? Thanks will be having a new one soon." Attached was an invoice from "Deletype/Incendit LLC" in Salem, Oregon for 39 5GB Tablet Mobile Broadband plans—mobile line fee.

i. Law enforcement obtained records from the electronic drive associated with Sherman's personal email address. Included in those records was a letter dated May 4, 2017 signed with Sherman's printed name explaining that Eluviis LLC and Deletype LLC were materially the same company, both of which were associated with Sherman.

j. On or about September 14, 2018, a representative from Blackberry emailed support@quantive.ch and m.cooper@quantivesolutions.com with the greeting: "Hi Mark *and Richard*" (emphasis supplied).

k. On or about September 26, 2019, dsglabsupport@quantivesolutions.com sent an email to an email account utilized by Indicted Co-Conspirator-1 that said: "Please see attached invoice." The invoice attached was from Incendit LLC with a listed email address of richard@eluviis.com to Unlockdon Distributor for $50,129.10 for "mobile device related services."

l. On July 9, 2020, Indicted Co-Conspirator-1 received an invoice from Incendit LLC with a listed email address of richard@eluviis.com in the approximate amount of $33,890.

Sherman's Response to the Victim Carrier's Investigation

19. In or around August 2020, the Victim Carrier was contacted by a tipper who alleged, in sum and substance, that a fake company with phony representatives was being used to unlock thousands of phones from the Victim Carrier each month, which permitted the individuals involved to make up to approximately $800,000 per month unlocking the IMEIs through the fraud. According to the tip, the individual who set up the account was a former employee of the Victim Carrier who left the company because he was facing separate charges for defrauding another wireless carrier.

20. The investigation has revealed that immediately prior to working with the Victim Carrier, Sherman worked for another wireless carrier. According to that wireless carrier, Sherman had also defrauded that employer by using fake accounts and hiding fraudulent activity in actual customer accounts.

21. The Victim Carrier contacted Quantive Solutions and the Technology Company as a result of the allegations and their internal review of Quantive Solutions' unlocking requests.

22. On or about October 18, 2020, dsglabsupport@quantivesolutions.com sent an email to a representative of the Technology Company acknowledging that Quantive Solutions was not a Technology Company affiliate but claiming that they were taking advantage of a discount available to developers.

23. According to records from the email provider, account dsglabsupport@quantivesolutions.com was last logged into in or around October 2020.

24. MDU requests were submitted through the Quantive Solutions BANs from at least by 2014 through 2020. While the investigation remains ongoing, a preliminary analysis reflects that between in or around December 2017 through in or around August 2020, Quantive Solutions submitted

approximately 315,429 MDU requests to the Victim Carrier. A loss analysis of the unpaid loan obligations owed to the Victim Carrier during this time period is approximately $4,426,594.69. In other words, during the last three years of the scheme, the Victim Carrier was unable to recover over $4 million worth of outstanding balances on phones with IMEIs that were unlocked as a result of Sherman's fraudulent scheme.