

Death by a Thousand Cuts: The Micro Debit Scheme That Fooled Big Banks and Stole From Consumers



From 2015 to 2022, a group of tech-savvy criminals orchestrated what prosecutors are calling a "death by a thousand cuts" attack on the American banking system and consumers. Their weapon of choice? Micro debits — tiny, often unnoticed withdrawals that slipped past the defenses of banks.

This is the story of how a handful of fraudsters, managed to siphon millions from unsuspecting victims and leave America's biggest banks scrambling while they perpetrated a scheme that netted them millions – one tiny cut at a time.

Shell Companies Were Created and Straw Owners Were Recruited

The scheme began as the brainchild of a trio of tech savvy Canadians – Henry Loconti, John Flynn, and Shoaib Ahmad. Their idea? Siphon money out of victims bank accounts without their knowledge. To do that, they would simply pull it out of their accounts using ACH transactions from fake merchants. They would keep the amounts low so most consumers might not even notice. (By the way, Henry Conti Jr is the son of the famous Henry Conti who started the legendary club in Cleveland called [The Agora](#).)

To make the scheme work however, they needed to establish seemingly legitimate companies that could get merchant accounts in the US. So, they recruited "signers" that lived in the United States – individuals who would serve as “straw owners” of the companies to provide a veneer of legitimacy and helping to obscure the fact the business were foreign owned.

Many shell companies were created to perpetrate the scheme. Some of the companies mentioned included:

- Idata-Clouds, LLC
- Ecloud Secure
- IKALLS, LLC
- My Kloud Box
- NRG Support
- Silver Safe Box
- Streaming Coupons
- Gigatech
- Dollar Web Sales

For instance, the shell company IKALLS, LLC was set up with a signer from Waianae, Hawaii listed as having 51% ownership, while a Canadian associate held the remaining 49%.

The conspirators went to great lengths to create the appearance of proper documentation, drafting operating agreements, membership transfer documents, and even fabricating scenarios where one signer would "sell" their interest to another.

They used these elaborately constructed documents to open bank accounts and obtain payment processing services, often providing false information to banks and processors about the nature and ownership of the businesses.

The Trio Each Had A Unique Specialty in the Scheme

As most business operations do, they each had a specialty.

- **Henry Conti** – He played the role of the “**Broker**”. As a broker, he facilitated connections between different parts of the operation. He was involved in communications about micro debits, managing return rates, and setting up new payment processing relationships for shell entities.

- **John Flynn** – He played the role of “**The merchants technical assistant**”. Flynn worked closely with a merchant, helping to manage various aspects of the fraudulent operations. He was involved in purchasing lead lists, coordinating micro debits, communicating with other conspirators about transaction details, and managing the technical aspects of the scheme such as websites for shell companies.
- **Shoaib Ahmad** - He played the role of “**The Merchant**”. As a merchant, Ahmad was directly involved in the fraudulent debiting of consumer accounts. He managed shell companies, coordinated with brokers and signers, purchased lead lists, and was involved in decisions about transaction amounts and managing return rates. He also participated in funding accounts used for micro debits.

They Bought List of Consumers That They Could Use For Fraudulent ACH Withdrawals

To perpetrate the scheme, the trio relied on buying list of consumers PII and banking details so they could hit accounts with unauthorized debits. For this they turned to a guy named Timothy Munoz (aka "Tim Munoz").

According to the indictment, On February 24, 2016, Munoz responded to a request for leads, including "ID Theft leads", "PDL long form leads", and "ID theft/Medical for 50yrs old and up to 70". He provided a sample of 1,000 leads and offered to sell them for 10 cents each.

The list contained names, bank accounts, bank routing numbers, addresses, IP Addresses – everything that they would need to perpetrate the scheme against those consumers.

They Scrubbed The List To Improve The Quality Of The Data And Then Started Submitting Fraudulent ACH Debits

After buying the list, the offenders would scrub the list through various ways to make sure that the list were of good quality before submitting the fraudulent ACH transactions.

They did this in a few ways

- *Making small "penny" or "micro" credits to verify the accounts were active.*
- *Removing accounts likely to cause returns (e.g., closed accounts).*
- *Potentially filtering out government (.gov) email addresses and other high-risk targets.*

After making sure the list were accurate they initiated unauthorized ACH debits from the victims' accounts, typically for amounts that wouldn't immediately trigger suspicion (e.g., \$24.95 or \$29.95).

To avoid detection, they used various techniques like creating fake websites for the shell companies to appear legitimate, generating false "proof of authorization" documents if questioned by the payment processors, and using "micro debits" between their own accounts to artificially lower return rates and avoid scrutiny from banks and NACHA.

When consumers complained or attempted to return transactions, they would sometimes issue refunds to prevent victims from reporting to authorities.

A Microtransaction Scheme Helped Keep Their Chargeback Rates Low

To remain hidden for longer periods of time, the trio had to keep the chargeback rate low so that the processors would not close their accounts.

For that they turned to tiny legitimate transactions where they controlled both sides of the transaction. The micro-transactions (also called "micro debits", "affiliate transactions", or "friendly items") were used to artificially lower the overall return rates for their fraudulent transactions. This was done to avoid scrutiny from banks and stay within NACHA guidelines.

How their scheme worked is laid out here:

- They would initiate very small debits (around \$1.35 to \$1.50 each) between accounts they controlled.
- These transactions were guaranteed not to be returned since they controlled both ends of the transaction.
- By adding these successful transactions to their mix, they lowered the percentage of returned transactions.

Complaints Soared While The Fraud Posted To Consumers Accounts

On Yelp, complaints about some of the merchants that they used poured in. In all cases, victims noticed charges for \$38.65 which was a dead giveaway.

 Jan 21, 2020

Would give them a zero if I could! My account was charged \$38.65 like everyone else! I called them heated and said where did you get my bank info from? Completely silent in the background, clearly not a business! I asked to speak to someone as to how they have my bank info and he said he could have someone call me back. He said it would be returned in 1-3 days. Of course I called my bank, put in a fraud claim and they are stopping it. HOWEVER, they cannot simply flag this company to prevent them from taking my money, so the rep said I need to close out my account and get another one ASAP! Really??? I'm inconvenienced majorly as this is my account that I pay all my bills out of! Unbelievable how crooked this world is!

★☆☆☆☆ Jul 23, 2019

Same here....They illegally withdraw from your account after making a test withdrawal of .01 cent and then they withdrawal 38.65 from your account for a internet business that I never signed up for. They gave stolen information that they have illegally obtained. Why are they not in jail? When you call the fake customer service number, they say they will give it back in 1-3 days. I reported them to my bank as frauds. I'm going to contact my state attorney general next.

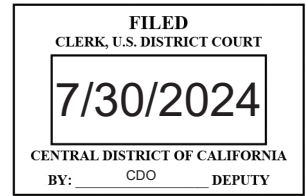
★☆☆☆☆ Aug 13, 2020

They starting charging me like everyone claims! During times like this \$38 bucks is \$100 bucks to some people! Bank put stop payment so no other charges can come thru! Keep the \$40 bucks hope you need it!

This company is a SCAM. They stole my information and started debiting \$38.65 from my account monthly. When I called, guy who said his name was "Carl" had no explanation of how or why this happened. He said my account had been "set up but never used" and that he could return the money "no questions asked". Of course he could! When I asked for details, he couldn't give me any answers. He also stated he "had never seen this before" He implied I could've clicked on something by accident. NO, I did not click and register on a company or service I have no INTEREST or USE for and have never SEEN; and NO, I did not put in my bank information by mistake. He sounded shady, and it was completely silent in the background. I told him my bank would be contacting him although he insisted he would refund my money right away.

I saw another review where the guy was told his money would be refunded right away and he was happy with the quick result. It's not about that- of course they will give you your money back no hassle, because they weren't AUTHORIZED to take it in the first place, and did so by stealing personal information. They do that so we can get off their backs when caught!

Read the Whole Complaint On Following Pages



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
January 2024 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

HENRY LOCONTI,
JOHN FLYNN,
 aka "John Hogg,"
 aka "John Murphy,"
SHOAI B AHMAD,
 aka "Shoba,"
 aka "Shobi,"
 aka "Shobie,"
 aka "Shoby,"
TIMOTHY MUNOZ,
 aka "Tim Munoz,"
ERIC CRESPIN,
 aka "Eric Marin," and
LEZLI ST. HILL,
 aka "Lez,"
 aka "Liz,"

Defendants.

CR No. 24-00219 (A) -MCS

F I R S T
S U P E R S E D I N G
I N D I C T M E N T

[18 U.S.C. § 1962(d): Racketeer Influenced and Corrupt Organizations Conspiracy; 18 U.S.C. § 1343: Wire Fraud; 18 U.S.C. §§ 1963 and 982: Criminal Forfeiture]

//

1 The Grand Jury charges:

2 COUNT ONE

3 [18 U.S.C. § 1962(d)]

4 [ALL DEFENDANTS]

5 A. INTRODUCTORY ALLEGATIONS

6 At times relevant to this First Superseding Indictment:

7 1. Defendants HENRY LOCONTI; JOHN FLYNN, also known as ("aka")
8 "John Hogg," aka "John Murphy"; SHOAIB AHMAD, aka "Shoba," aka
9 "Shobi," aka "Shobie," aka "Shoby"; TIMOTHY MUNOZ, aka "Tim Munoz";
10 ERIC CRESPIAN, aka "Eric Marin"; and LEZLI ST. HILL, aka "Lez," aka
11 "Liz", and others known and unknown to the Grand Jury, were members
12 and associates of a criminal organization referred to hereinafter as
13 "THE ENTERPRISE." In furtherance of a scheme to fraudulently obtain
14 money from American consumers' bank accounts, members and associates
15 of THE ENTERPRISE engaged in, among other things, mail, wire, and
16 bank fraud; identity theft; access device fraud; and money
17 laundering. THE ENTERPRISE operated in the Central District of
18 California and elsewhere.

19 2. THE ENTERPRISE, including its leaders, members, and
20 associates, constituted an "enterprise," as defined in Title 18,
21 United States Code, Section 1961(4), that is, a group of individuals
22 associated in fact, although not a legal entity. THE ENTERPRISE
23 constituted an ongoing organization whose members functioned as a
24 continuing unit for a common purpose of achieving the objectives of
25 THE ENTERPRISE. THE ENTERPRISE engaged in, and its activities
26 affected, interstate and foreign commerce.

27 3. Members and associates of THE ENTERPRISE played different
28 roles at different times:

1 a. Merchants: Merchants used business entities (each a
2 "Shell Entity") to offer to consumer-victims subscriptions for some
3 service or product, such as cloud storage, for a recurring charge.
4 In fact, the Shell Entities served as cover for a scheme to make
5 unauthorized debits against consumer-victims' bank accounts (the
6 "Consumer Bank Accounts"). Merchants purchased identifying and
7 financial information of consumer-victims, at times through brokers,
8 and caused unauthorized debits to be originated against Consumer Bank
9 Accounts, many of which were held or serviced by federally insured
10 financial institutions (the "Consumer Banks"). These unauthorized
11 debits removed funds from the Consumer Bank Accounts and caused them
12 to be deposited into bank accounts controlled by or for the Shell
13 Entities (each a "Shell Entity Bank Account") at "Originating Banks,"
14 sometimes each called an "ODFI," many of which were also federally
15 insured.

16 b. Payment processors: Through their Originating Banks,
17 payment processors operated some Shell Entity Bank Accounts for
18 merchants. The payment processors facilitated the merchants'
19 debiting of the Consumer Bank Accounts. These debits sometimes
20 resulted in rejected or "returned" transactions (each a "return"),
21 including returns based on complaints by consumer-victims that the
22 transactions were unauthorized. Payment processors helped process
23 returns and conducted other financial transactions for the merchants.

24 c. Signers: Signers served as nominal owners of Shell
25 Entities and/or Shell Entity Bank Accounts. Signers generally helped
26 merchants and brokers create, open, and control the Shell Entities
27 and Shell Entity Bank Accounts.

28

1 d. Lead list sources: "Lead lists" contained identifying
2 and financial information of prospective consumer-victims, including
3 bank routing numbers and bank account numbers. Lead list sources
4 generally sold lead lists (at times referred to as "traffic") to
5 merchants.

6 e. Brokers: Brokers helped merchants find payment
7 processors, signers, lead list sources, and other assistance.

8 B. MEMBERS AND ASSOCIATES OF THE ENTERPRISE

9 4. The defendants' roles in THE ENTERPRISE were:

10 a. Defendant LOCONTI, a resident of Chardon, Ohio, was a
11 broker.

12 b. Defendant FLYNN, a resident of Canada, assisted
13 Merchant-1 (which term is defined below) in Merchant-1's role as a
14 merchant.

15 c. Defendant AHMAD, a resident of Canada, was a merchant.

16 d. Defendant MUNOZ, a resident of Wilmington, California,
17 was a lead list source.

18 e. Defendant CRESPIN, a resident of Canada, assisted
19 Merchant-1 in Merchant-1's role as a merchant.

20 f. Defendant ST. HILL, a resident of Canada, assisted
21 Merchant-1 in Merchant-1's role as a merchant.

22 5. The following persons, each of whose identity is known to
23 the Grand Jury, were members and associates of THE ENTERPRISE:

24 a. "CC A-1," a resident of Hawaiian Gardens, California,
25 was president of a company headquartered in the Central District of
26 California ("Company A"). Both personally and through Company A,
27 CC A-1 was primarily a broker and at times a merchant. Company A
28 maintained one or more email servers located in the Central District

1 of California that routed email communications between Company A
2 personnel, including CC A-1 and others, and other members and
3 associates of THE ENTERPRISE located outside this district.

4 b. "CC A-2," a resident of Huntington Beach, California,
5 was a broker who primarily worked for CC A-1 at Company A and, at
6 times, used a Company A email account.

7 c. "CC A-3," a resident of Long Beach, California,
8 assisted CC A-1 in CC A-1's roles as a broker and as a merchant and,
9 at times, used a Company A email account.

10 d. "Merchant-1," a resident of Canada and Cyprus, was
11 primarily a merchant and at times a lead list source. Merchant-1
12 controlled one or more email accounts hosted by a third party located
13 in Arizona, some of which were used by defendants FLYNN, CRESPIAN, and
14 ST. HILL.

15 e. "Merchant-2," a resident of Canada, was a merchant who
16 primarily worked with Merchant-1.

17 f. "Processor-1," a resident of Las Vegas, Nevada, was
18 president of a payment processor.

19 g. "Broker-1," a resident of Waianae, Hawaii, was a
20 broker.

21 h. "Signer-1," a resident of Waianae, Hawaii, was a
22 signer who worked for Broker-1.

23 i. "Signer-2," a resident of Montreal, Canada, was a
24 signer who worked for defendant AHMAD.

25 j. "Signer-3," a resident of Huntington Beach,
26 California, was a signer who primarily worked for CC A-1.

27
28

1 k. "Signer-4," a resident of Las Vegas, Nevada and
2 Pittsburg, California, was a signer who primarily worked for
3 Merchant-1.

4 C. PURPOSES OF THE ENTERPRISE

5 6. The purposes of THE ENTERPRISE included:

6 a. Enriching the members and associates of THE ENTERPRISE
7 through fraud;

8 b. Obtaining, preserving, and protecting the proceeds of
9 THE ENTERPRISE through acts of money laundering; and

10 c. Protecting THE ENTERPRISE, its members and associates,
11 and its unlawful activities from detection by financial institutions,
12 government agencies, and others.

13 D. THE MANNER AND MEANS OF THE ENTERPRISE

14 7. Defendants LOCONTI, FLYNN, AHMAD, MUNOZ, CRESPIN, and ST.
15 HILL, and other members and associates of THE ENTERPRISE, agreed to
16 conduct and participate in the conduct of the affairs of THE
17 ENTERPRISE, through the following means, among others:

18 a. Members and associates of THE ENTERPRISE bought and
19 sold lead lists containing identifying and financial information of
20 prospective consumer-victims for the purpose of fraudulently
21 obtaining money from the consumer-victims by making unauthorized
22 debits against those consumer-victims' Consumer Bank Accounts.

23 Members and associates of THE ENTERPRISE vetted lead lists through a
24 "scrub," by making test credits ("penny" or "micro" credits) to the
25 Consumer Bank Accounts on the lists, and through other means. The
26 scrubbing process would remove from the lead lists, for example,
27 closed Consumer Bank Accounts that would cause returns on debit
28 attempts.

1 b. Members and associates of THE ENTERPRISE created, and
2 caused to be created, Shell Entities, and obtained the use of, and
3 controlled, Shell Entity Bank Accounts.

4 c. Members and associates of THE ENTERPRISE recruited
5 domestic signers to, among other purposes, help conceal connections
6 between domestic Shell Entities and Shell Entity Bank Accounts and
7 foreign members and associates of THE ENTERPRISE. Members and
8 associates of THE ENTERPRISE managed these signers through interstate
9 and foreign email, messaging, and telephone communications.

10 d. Using the lead lists and other sources of prospective
11 consumer-victim information, members and associates of THE ENTERPRISE
12 originated debits, and caused debits to be originated, for the
13 benefit of Shell Entities, against Consumer Bank Accounts. THE
14 ENTERPRISE caused millions of dollars in unauthorized debits against
15 Consumer Bank Accounts for the benefit of the members and associates
16 of THE ENTERPRISE.

17 e. To conceal and continue their unauthorized debits
18 against Consumer Bank Accounts and conceal their returns and return
19 rates, and continue to collect the proceeds of the fraud, members and
20 associates of THE ENTERPRISE took the following actions, among
21 others:

22 i. Members and associates of THE ENTERPRISE created
23 websites for some Shell Entities to give the impression those
24 entities were providing legitimate services and products, even though
25 the websites sometimes lacked functionality and few, if any, actual
26 customers subscribed to services through them.

27 ii. When a Consumer Bank, Originating Bank, or other
28 person or entity requested proof of authorization ("POA") for a debit

1 against a Consumer Bank Account, members and associates of THE
2 ENTERPRISE created false and fraudulent documentation to be presented
3 to the requester, claiming that the consumer-victim had authorized
4 the debit, as a payment to a Shell Entity for a subscription for a
5 service and product provided by the Shell Entity, by signing up for
6 the Shell Entity's service and product through the Shell Entity's
7 website.

8 iii. Members and associates of THE ENTERPRISE
9 monitored the Shell Entities' return rates and took steps to ensure
10 that the return rates did not affect the ability of THE ENTERPRISE to
11 continue the fraudulent debiting of Consumer Bank Accounts, including
12 the following:

13 (I) Members and associates of THE ENTERPRISE
14 knew and believed that the number of returns, and a Shell Entity's
15 percentage of returns in comparison to all debits ("return rate"),
16 often caused and would have caused scrutiny from the Originating
17 Banks. For example, members and associates of THE ENTERPRISE knew
18 and believed that, for Automated Clearing House ("ACH") debits,
19 National Automated Clearing House Association ("NACHA") rules imposed
20 certain thresholds for acceptable return rates and certain
21 obligations on Originating Banks to monitor return rates. Members
22 and associates of THE ENTERPRISE knew that high return rates could
23 cause the Originating Banks to stop originating debits for the Shell
24 Entities and therefore restrict the members' and associates' ability
25 to further debit Consumer Bank Accounts.

26 (II) Depending on the return rates of the
27 unauthorized consumer-victim debits, members and associates of THE
28 ENTERPRISE regularly caused their Originating Banks to originate, for

1 the Shell Entities, thousands of "micro" debits (also referred to as
2 "affiliate" or "friendly" items or transactions) against Shell Entity
3 Bank Accounts at other financial institutions, withdrawing a small
4 amount of money with each debit. Since members and associates of THE
5 ENTERPRISE controlled the Shell Entity Bank Accounts, they knew these
6 micro debits would not result in returns and would therefore
7 artificially suppress the Shell Entity return rates at Originating
8 Banks to levels that, as the members and associates understood and
9 believed, would avoid Originating Banks' scrutiny and potential
10 termination of banking services.

11 iv. When some consumer-victims discovered the
12 unauthorized debits, members and associates of THE ENTERPRISE, at
13 times through purported "customer service" personnel, used refunds
14 and other means to dissuade consumer-victims from reporting the
15 debiting Shell Entities to Consumer Banks, government agencies, and
16 others.

17 f. After proceeds of unauthorized debits from the
18 Consumer Bank Accounts were credited to Shell Entity Bank Accounts,
19 members and associates of THE ENTERPRISE caused some of the proceeds
20 to be funneled to other Shell Entity Bank Accounts in order to fund
21 the micro debits the members and associates of THE ENTERPRISE used to
22 conceal and disguise Shell Entity return rates and in order to
23 promote and prolong their scheme. Members and associates of THE
24 ENTERPRISE, at times, also caused some of the proceeds to be
25 transferred from domestic Shell Entity Bank Accounts to accounts
26 outside the United States in transactions designed in whole and in
27 part to conceal and disguise the nature, source, ownership, and
28 control of the proceeds.

1 E. THE OBJECT OF THE CONSPIRACY

2 8. Beginning on or about September 18, 2015, and continuing
3 through January 2022, in Los Angeles County, within the Central
4 District of California, and elsewhere, defendants LOCONTI, FLYNN,
5 AHMAD, MUNOZ, CRESPIN, and ST. HILL, and others known and unknown to
6 the Grand Jury, being persons employed by and associated with THE
7 ENTERPRISE, which was engaged in, and the activities of which
8 affected, interstate and foreign commerce, knowingly, willfully, and
9 unlawfully conspired with each other, and with others known and
10 unknown to the Grand Jury, to violate Title 18, United States Code,
11 Section 1962(c), that is, to conduct and participate, directly and
12 indirectly, in the conduct of the affairs of THE ENTERPRISE through a
13 pattern of racketeering activity, as that term is defined in Title
14 18, United States Code, Sections 1961(1) and 1961(5), consisting of
15 multiple acts indictable under:

16 a. Title 18, United States Code, Section 1341 (relating
17 to mail fraud);

18 b. Title 18, United States Code, Section 1343 (relating
19 to wire fraud);

20 c. Title 18, United States Code, Section 1344 (relating
21 to financial institution fraud);

22 d. Title 18, United States Code, Section 1028 (relating
23 to fraud and related activity in connection with identification
24 documents);

25 e. Title 18, United States Code, Section 1029 (relating
26 to fraud and related activity in connection with access devices);

27 f. Title 18, United States Code, Section 1956 (relating
28 to the laundering of monetary instruments); and

1 g. Title 18, United States Code, Section 1957 (relating
2 to engaging in monetary transactions in property derived from
3 specified unlawful activity).

4 9. It was a further part of the conspiracy that each defendant
5 agreed that a conspirator would commit at least two acts of
6 racketeering activity in the conduct of the affairs of THE
7 ENTERPRISE.

8 F. OVERT ACTS

9 10. In furtherance of the conspiracy, and to accomplish its
10 object, on or about the following dates, defendants LOCONTI, FLYNN,
11 AHMAD, MUNOZ, CRESPIN, and ST. HILL, together with others known and
12 unknown to the Grand Jury, committed and willfully caused others to
13 commit the following overt acts, among others, within the Central
14 District of California and elsewhere:¹

15 Overt Act No. 1: On December 4, 2015, Merchant-1 emailed
16 defendant FLYNN, asking that defendant FLYNN make sure that the lead
17 lists they purchased included Internet Protocol ("IP") addresses for
18 the consumer-victims.

19 Overt Act No. 2: On December 7, 2015, CC A-2 sent an email to
20 defendant FLYNN, copying CC A-1 and Merchant-1 and attaching two lead
21 lists containing 4,024 and 13,426 leads, respectively, stating, "I
22 would go through though and make sure the consumers age is okay with
23 you guys. I did notice some (only a few) that were pretty old."

24 Overt Act No. 3: On December 30, 2015, in response to an
25 email from defendant FLYNN to defendant LOCONTI and CC A-1 that
26

27
28 ¹ Unless indicated otherwise in brackets, phrases in quotation
marks reproduce the original spellings, spacings, case, emphases, and
ellipses.

1 stated, "batch 1 - 1000 micros[;] - no scrub[.] batch 2 - 253
2 orders[;] - YES scrub and process," defendant LOCONTI sent an email
3 to defendant FLYNN and CC A-1, stating in part, "Can you please send
4 more micro debit to offset the high returns for this month. Need to
5 send them ASAP so not to miss the cutoff."

6 Overt Act No. 4: On December 30, 2015, following defendant
7 LOCONTI's email referenced in Overt Act No. 3, defendant FLYNN sent
8 an email to defendant LOCONTI and CC A-1, stating, "Ok I just
9 uploaded another micro batch 1500 orders."

10 Overt Act No. 5: On February 24, 2016, in response to an
11 email from CC A-2 to defendant MUNOZ, copying CC A-1, that requested
12 leads, including "ID Theft leads", "PDL long form leads", and "ID
13 theft/Medical for 50yrs old and up to 70", defendant MUNOZ sent an
14 email to CC A-2, stating in part, "I've attached a 1k sample of a
15 buyers file for the ID theft sales. I can get them for you for 10
16 cents." Attached to defendant MUNOZ's email was a lead list
17 containing 1,000 leads.

18 Overt Act No. 6: On April 6, 2017, CC A-1 sent an email to
19 defendant FLYNN, copying defendant CRESPIAN, Merchant-1, CC A-2, and
20 others, regarding instructions to integrate with Company A's
21 processing gateway.

22 Overt Act No. 7: On April 12, 2017, in response to Merchant-1
23 forwarding to defendant FLYNN an email that Signer-4 had originally
24 received from a Better Business Bureau ("BBB") for Shell Entity
25 Ecloud Secure, defendant FLYNN sent an email to Merchant-1, asking,
26 "why is [Signer-4] using the same gmail address for multiple corps at
27 the BBB? this draws a direct line between the corps."
28

1 Overt Act No. 8: On September 22, 2017, defendant CRESPI
2 sent an email to defendant FLYNN, Merchant-1, and Merchant-2,
3 attaching an instruction manual created by defendant CRESPI
4 regarding the use of the software application he created for them to
5 generate and track transactions, including micro debits.

6 Overt Act No. 9: On April 16, 2018, Merchant-1 forwarded to
7 defendant ST. HILL an email from Merchant-2 explaining his scrubbing
8 process and suggesting how to respond to a Virginia State Attorney
9 General inquiry about a consumer complaint, stating, "We kill most
10 .GOV on the way in. I always scroll and look for any suspicious
11 emails. Banks, GOV police, lawyers etc etc. Personally I would not
12 provide a POA to an AG unless the AG specifically asks. I would go
13 with, we reviewed the case of Mr's X and deem it to be a valid
14 sale. We have since refunded ...etc etc We consider that matter
15 closed. Again, don't offer up a POA on a platter to an AG."

16 Overt Act No. 10: On June 28, 2018, in an email chain
17 regarding transactions for Shell Entities Silver Safe Box and Dollar
18 Web Sales, Processor-1 sent an email to defendant CRESPI, Merchant-
19 1, and others, stating in part, "I'm very concerned that without the
20 affiliate transactions the return rates will raise eyebrows at the
21 bank ... we need to ensure the affiliate items (\$ 1.35 per item ???)
22 are part of the equation here [. . .] We don't want the bank to see
23 the 1st week of batches have 20% return rates because the affiliate
24 CCD items are missing."

25 Overt Act No. 11: On September 20, 2018, Broker-1 sent an
26 email to CC A-1 and CC A-2, stating, "As I told [CC A-1], we put
27 [Signer-1] on the app for US purposes" and including as an attachment
28 Processor-1's company's "New Merchant Questionnaire" for Shell Entity

1 "IKALLS," which listed a single "owner/officer," Signer-1, with
2 address in Waianae, Hawaii, and 51 percent ownership, and which
3 answered in the negative to the question, "Is there any foreign (non-
4 U.S.) ownership in this Company?"

5 Overt Act No. 12: On September 25, 2018, Broker-1 forwarded to
6 CC A-1 and CC A-2 an email from defendant AHMAD with the subject
7 "Articles of ikalls" in which defendant AHMAD wrote, "Hi [Broker-1],
8 Please see attached documents. Thanks[,] " writing "see attached,
9 [Signer-1] is a signer on the operating agreement and is President."
10 Attached to Broker-1's email was a "Limited Liability Company
11 Operating Agreement of IKALLS, L.L.C." The operating agreement
12 purported to be executed by Signer-1, as Operating Manager, and
13 Signer-2, as President. Schedule A to the operating agreement listed
14 two members of the company, their addresses, and percentage interest:
15 Signer-1, with address in Waianae, Hawaii, and 51 percentage
16 interest, and Signer-2, with address in Saint-Laurent, Quebec,
17 Canada, and 49 percentage interest.

18 Overt Act No. 13: On September 27, 2018, CC A-2 sent an email
19 with the subject "iKalls LLC Merchant Submission" to Processor-1,
20 copying CC A-1 and CC A-3, in which CC A-2 wrote, "Please see the
21 attached merchant submission." Attached to CC A-2's email were
22 Processor-1's company's "New Merchant Questionnaire" for Shell Entity
23 "IKALLS" referenced in Overt Act No. 11 and the "Limited Liability
24 Company Operating Agreement of IKALLS, L.L.C." referenced in Overt
25 Act No. 12.

26 Overt Act No. 14: On November 26, 2018, in response to an
27 email from Broker-1 to defendant AHMAD that copied CC A-1 and CC A-2
28 and asked CC A-2 to "fill Shoby in and better explain" three steps

1 that Broker-1 and defendant AHMAD needed to take to keep their
2 "account functional," CC A-2 advised regarding the "micro credit" or
3 "penny credit" that "If the customer's account doesn't exist, doesn't
4 match, etc. (return codes for R-2,3 and 4's usually) this is where
5 they will be caught (roughly 90% or higher) of those returns will be
6 caught here." CC A-2 also stated, "We have seen merchants that
7 operate in the 30-40% return rate get down to half of that with doing
8 this process. It not only drops your overall return rate and looks
9 better to the bank, but it drops down your returns costs." CC A-2
10 further stated, "On top of all of this there will be micro debit
11 transactions that will probably be needed in order to stay within the
12 NACHA guidelines for unauthorized returns to be under 0.50%," and
13 explained how to use micro debits.

14 Overt Act No. 15: On December 10, 2018, in response to an
15 email from Merchant-1 to a payment processor, copying defendant
16 LOCONTI, regarding Shell Entity Ecloud Secure in which Merchant-1
17 signed the email in Signer-4's name but used an email address in
18 Merchant-1's name, defendant LOCONTI emailed Merchant-1, stating,
19 "[Merchant-1] you used the wrong email address with [payment
20 processor]."

21 Overt Act No. 16: On January 31, 2019, defendant ST. HILL
22 tested the web signup function for Shell Entity NRG Support using the
23 name "lezli rich."

24 Overt Act No. 17: On January 31, 2019, defendant FLYNN
25 forwarded to Merchant-1 an email notification generated by the test
26 referenced in Overt Act No. 16, asking, "[Merchant-1], someone just
27 signed up for NRG - strange. is this you testing?"

28

1 Overt Act No. 18: On January 31, 2019, in response to
2 Merchant-1 forwarding to defendant ST. HILL the email from defendant
3 FLYNN referenced in Overt Act No. 17 and asking, "Was this you ?",
4 defendant ST. HILL stated, "YES."

5 Overt Act No. 19: On February 18, 2019, defendant FLYNN sent
6 an email to a Company A employee, attaching a false and fraudulent
7 POA for Shell Entity My Kloud Box.

8 Overt Act No. 20: On April 3, 2019, in an email chain
9 regarding submitting transactions for Shell Entity Silver Safe Box to
10 a payment processor in which defendant CRESPIIN used an email address
11 with the domain for Shell Entity NRG Support, defendant LOCONTI sent
12 an email to defendant CRESPIIN and CC A-1, copying Merchant-1, stating
13 in part, "Why do you use an email address that gets you in trouble
14 with processors? [. . .] You signed up as Silver Safe Box, not NRG..
15 This is what started all the trouble over at [other payment
16 processor]. This is simple merchant 101 how to stay in business
17 tactics. Eric I suggest getting a Silver Safe Box email address (or
18 at least a Gmail address) when working with [this] processor I set
19 [Merchant-1] up with so he can not get into trouble like with [other
20 payment processor]." Defendant LOCONTI's email also linked to a BBB
21 webpage of complaints against Shell Entity NRG Support.

22 Overt Act No. 21: On April 3, 2019, in response to defendant
23 LOCONTI's email referenced in Overt Act No. 20, defendant CRESPIIN
24 sent an email to defendant LOCONTI and CC A-1, copying Merchant-1,
25 stating in part, "Yes that was a mistake. [. . .] Will use a generic
26 gmail account for the future."

27 Overt Act No. 22: On June 14, 2019, defendant AHMAD sent an
28 email to CC A-1 and Broker-1, attaching a "Membership Interest

1 Purchase Agreement," purporting to be signed by Signer-2 on June 14,
2 2019 in Montreal, Canada, which purported to demonstrate that Signer-
3 2 transferred all interest in Shell Entity iKalls to Signer-1.

4 Overt Act No. 23: On June 18, 2019, CC A-2 emailed Processor-
5 1, copying CC A-1 and CC A-3, and others, under subject "iKalls
6 Updated Documents." CC A-2 stated, "[Processor-1], Please find the
7 attached requested documents which reflect the LLC's new Operating
8 Agreement, Updated EIN and the Purchase Agreement between buyer and
9 seller." Attached to CC A-2's email was a "Membership Interest
10 Purchase Agreement," purporting to be signed by Signer-1 on June 14,
11 2019 in the State of Hawaii and by Signer-2 on June 14, 2019 in
12 Montreal, Canada, which purported to demonstrate that Signer-2
13 transferred all interest in Shell Entity iKalls to Signer-1.

14 Overt Act No. 24: On August 26, 2019, defendant CRESPIIN sent
15 an email to Merchant-1, listing 11 login user names and passwords to
16 their file transfer protocol (FTP) server in the Republic of Türkiye.

17 Overt Act No. 25: On September 16, 2019, in response to
18 Merchant-1 forwarding to defendant MUNOZ some transaction results for
19 a lead list from defendant MUNOZ and complaining, "The result of that
20 file is 7.25 % Good to bill ! [. . .] You used to sell me .50
21 per order for better results !!", defendant MUNOZ emailed to
22 Merchant-1, "You do not know how hard it is to find new sources.
23 [. . .] The idea is to increase your database and that's what this
24 accomplishes."

25 Overt Act No. 26: On February 10, 2020, CC A-1 emailed
26 defendant AHMAD, copying Broker-1 and CC A-2, stating "Shoby[,]
27 Please read email received from [Processor-1]. Do not submit new
28 traffic until we connect you with the scrub [CC A-2] has." CC A-1

1 continued, "This account is going to blow up if we cant get the
2 re5urns under control for new business." Copied in CC A-1's email
3 was the following message from Processor-1: "You probably also need
4 to get involved with where they are buying their data. The penny
5 credit file from last week had 95% returns. The bank will surely ask
6 me to explain those results."

7 Overt Act No. 27: On February 10, 2020, in an email exchange
8 following the email from CC A-1 referenced in Overt Act No. 26, CC A-
9 2 responded to Broker-1, copying CC A-1 and defendant AHMAD: "I'll
10 have to get you the file format first thing in the morning. You don't
11 need all of the information to be filled out though, just routing and
12 account and it will give you back a positive or negative result file.
13 It might also be wise to have the lead broker just log in before
14 selling any leads, upload the file and see how many are actually
15 clear before buying them. I mentioned this before to Shobie as well
16 and it's why it scrubs just based on minimal info rather than someone
17 having to provide everything."

18 Overt Act No. 28: On April 9, 2020, in response to an email
19 from defendant FLYNN, copying Merchant-1, requesting defendant ST.
20 HILL to list for Merchant-1 all of her email addresses and what she
21 uses them for, defendant ST. HILL discussed 14 email addresses with
22 domains associated with Shell Entities Ecloud Secure, Gigatech, My
23 Kloud Box, NRG Support, and Silver Safe Box.

24 Overt Act No. 29: On July 16, 2020, CC A-1 sent an email to
25 Merchant-1 and defendant AHMAD with the subject "Better Quality
26 Traffic." CC A-1 wrote, "[Merchant-1], I spoke with Shoby this
27 morning regarding setting up a conference call with you to discuss
28 the possibilities of assisting Shoby in acquiring better quality

1 traffic from you directly. Could we possibly do that call at 8:30AM
2 my time, 11:30 Montreal? Please advise if that works. If so, I'll
3 initiate the call, connect you two then provide cell numbers in an
4 email."

5 Overt Act No. 30: On July 22, 2020, defendant FLYNN sent an
6 email to CC A-2, in which, at Merchant-1's request, defendant FLYNN
7 asked CC A-2 to identify Shell Entity Gigatech's correct Internet
8 domain.

9 Overt Act No. 31: On November 18, 2020, CC A-1 emailed
10 defendant AHMAD, under subject "1K CA Leads," stating, in part,
11 "Shobi, Please find the attached 1k CA leads," and attaching a file
12 named "Shobi 1k Leads.xlsx," which was a lead list that contained
13 1,000 leads, all with addresses in California.

14 Overt Act No. 32: On December 10, 2020, Signer-3 sent CC A-3
15 multiple text messages that provided the names and telephone numbers
16 for consumer-victims H.C. and M.M.

17 Overt Act No. 33: On December 10, 2020, Merchant-1 emailed a
18 user at the domain for Shell Entity NRG Support, directing them to
19 call three consumer-victims of a different Shell Entity and copying
20 defendant ST. HILL and CC A-3. Merchant-1's email forwarded another
21 email from CC A-3 that included the names and telephone numbers of
22 the three consumer-victims, D.Q., H.C., and M.M., and stated, "The
23 following customers have called regarding their account. Please note
24 [Signer-3] does his best to get the consumers name, some are willing
25 and some are not so compliant. I get the information directly from
26 him."

1 Overt Act No. 34: On January 31, 2021, defendant LOCONTI
2 forwarded to CC A-1 an email from Merchant-1 regarding a new payment
3 processing relationship for Shell Entity Silver Safe Box.

4 Overt Act No. 35: On March 10, 2021, defendant AHMAD caused a
5 wire transfer in the amount of \$500 to be sent to fund a domestic
6 bank account ("Account A") that was managed by Company A personnel
7 and used to fund micro debits for Shell Entities controlled by both
8 Merchant-1 and defendant AHMAD.

9 Overt Act No. 36: On March 16, 2021, Merchant-1 caused a wire
10 transfer in the amount of \$5,000 to be sent to Account A.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COUNTS TWO THROUGH SIX

[18 U.S.C. § 1343]

[ALL DEFENDANTS]

11. The Grand Jury realleges paragraphs 1 through 7 and 10 of this First Superseding Indictment here.

A. THE SCHEME TO DEFRAUD

12. Beginning on or about September 18, 2015, and continuing through January 2022, in Los Angeles County, within the Central District of California, and elsewhere, defendants LOCONTI, FLYNN, AHMAD, MUNOZ, CRESPIAN, and ST. HILL, and others known and unknown to the Grand Jury, knowingly and with intent to defraud, devised, participated in, and executed a scheme to defraud financial institutions, as defined in Title 18, United States Code, Section 20, including Originating Banks and Consumer Banks, as to material matters, and to obtain money and property from the Originating Banks and Consumer Banks by means of material false and fraudulent pretenses, representations, and promises, and the concealment of material facts.

13. The fraudulent scheme operated, in substance, in the manner set forth in paragraph 7 of this First Superseding Indictment.

B. THE USE OF THE WIRES

14. On or about the dates set forth below, in Los Angeles County, within the Central District of California, and elsewhere, the following defendants, for the purpose of executing the above-described scheme to defraud affecting a financial institution, transmitted, and caused the transmission of, the following items by means of wire and radio communication in interstate and foreign commerce:

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COUNT	DATE	DEFENDANT (S)	ITEM WIRED
TWO	12/30/2015	LOCONTI and FLYNN	Interstate email from defendant FLYNN to CC A-1 described in Count One, Overt Act No. 4
THREE	2/24/2016	MUNOZ	Interstate email from defendant MUNOZ to CC A-2 described in Count One, Overt Act No. 5
FOUR	4/3/2019	LOCONTI and CRESPIAN	Interstate email from defendant CRESPIAN to CC A-1 described in Count One, Overt Act No. 21
FIVE	6/18/2019	AHMAD	Interstate email from CC A-2 to Processor-1 described in Count One, Overt Act No. 23
SIX	12/10/2020	ST. HILL	Interstate email from Merchant-1 to CC A-3 described in Count One, Overt Act No. 33

FORFEITURE ALLEGATION ONE

[18 U.S.C. § 1963]

1
2
3 1. Pursuant to Federal Rule of Criminal Procedure 32.2, notice
4 is hereby given that the United States of America will seek
5 forfeiture as part of any sentence, pursuant to Title 18, United
6 States Code, Section 1963, in the event of any defendant's conviction
7 of the offense set forth in Count One of this First Superseding
8 Indictment.

9 2. Any defendant so convicted shall forfeit to the United
10 States of America the following:

11 a. Any interest the convicted defendant has acquired or
12 maintained as a result of such offense;

13 b. Any interest in, security of, claim against, or
14 property or contractual right of any kind affording a source of
15 influence over, any enterprise which the convicted defendant has
16 established, operated, controlled, conducted, or participated in the
17 conduct of, as a result of such offense;

18 c. Any property constituting, or derived from, any
19 proceeds which the convicted defendant obtained, directly or
20 indirectly, from racketeering activity as a result of any such
21 offense; and

22 d. To the extent such property is not available for
23 forfeiture, a sum of money equal to the total value of the property
24 described in subparagraphs (a), (b), and (c).

25 3. Pursuant to Title 18, United States Code, Section 1963(m),
26 any defendant so convicted shall forfeit substitute property, up to
27 the total value of the property described in the preceding paragraph
28 if, as the result of any act or omission of said defendant, the

1 property described in the preceding paragraph, or any portion thereof
2 (a) cannot be located upon the exercise of due diligence; (b) has
3 been transferred, sold to or deposited with a third party; (c) has
4 been placed beyond the jurisdiction of the court; (d) has been
5 substantially diminished in value; or (e) has been commingled with
6 other property that cannot be divided without difficulty.

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FORFEITURE ALLEGATION TWO

[18 U.S.C. § 982]

1
2
3 1. Pursuant to Rule 32.2(a) of the Federal Rules of Criminal
4 Procedure, notice is hereby given that the United States of America
5 will seek forfeiture as part of any sentence, pursuant to Title 18,
6 United States Code, Section 982(a)(2), in the event of any
7 defendant's conviction of the offenses set forth in any of Counts Two
8 through Six of this First Superseding Indictment.

9 2. Any defendant so convicted shall forfeit to the United
10 States of America the following:

11 a. All right, title and interest in any and all property,
12 real or personal, constituting, or derived from, any proceeds
13 obtained, directly or indirectly, as a result of the offense; and

14 b. To the extent such property is not available for
15 forfeiture, a sum of money equal to the total value of the property
16 described in subparagraph (a).

17 3. Pursuant to Title 21, United States Code, Section 853(p),
18 as incorporated by Title 18, United States Code, Section 982(b), any
19 defendant so convicted shall forfeit substitute property, up to the
20 total value of the property described in the preceding paragraph if,
21 as the result of any act or omission of said defendant, the property
22 described in the preceding paragraph, or any portion thereof: (a)
23 cannot be located upon the exercise of due diligence; (b) has been
24 transferred, sold to or deposited with a third party; (c) has been
25 placed beyond the jurisdiction of the court; (d) has been
26
27
28

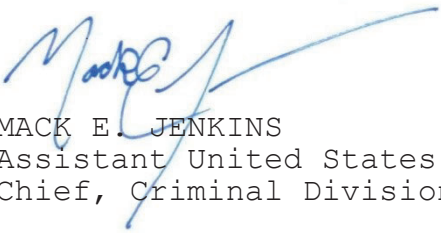
1 substantially diminished in value; or (e) has been commingled with
2 other property that cannot be divided without difficulty.

3
4 A TRUE BILL

5
6 /s/

7 _____
Foreperson

8 E. MARTIN ESTRADA
9 United States Attorney

10 
11 MACK E. JENKINS
12 Assistant United States Attorney
13 Chief, Criminal Division

14 KRISTEN A. WILLIAMS
15 Assistant United States Attorney
16 Chief, Major Frauds Section

17 MONICA E. TAIT
18 Assistant United States Attorney
19 Major Frauds Section

20 AMANDA N. LISKAMM
21 Director, Consumer Protection Branch
22 United States Department of Justice

23 WEI XIANG
24 MEREDITH B. HEALY
25 AMY P. KAPLAN
26 Trial Attorneys
27 Consumer Protection Branch
28 United States Department of Justice