



UNITED STATES DISTRICT COURT

for the

Central District of California



United States of America,

Plaintiff,

v.

SAMAN DELAFRAZ, and
BENJAMIN DANESHGAR

Defendants.

Case No. 2:25-mj-05544-DUTY

**CRIMINAL COMPLAINT BY TELEPHONE
OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the dates of 2015 to the present, in the county of Los Angeles in the Central District of California, the defendants violated:

Code Section

18 U.S.C. § 1956(h)

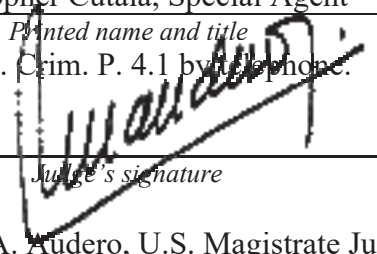
Offense Description

Conspiracy to Commit Money Laundering

This criminal complaint is based on these facts:

Please see attached affidavit.☒ Continued on the attached sheet./s/ Christopher Cutaia*Complainant's signature*Christopher Cutaia, Special Agent*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 09/08/2025City and state: Los Angeles, California
*Judge's signature*Hon. Maria A. Audero, U.S. Magistrate Judge*Printed name and title*

Contents

I.	INTRODUCTION.....	1
II.	PURPOSE OF AFFIDAVIT.....	1
III.	SUMMARY OF PROBABLE CAUSE.....	2
IV.	STATEMENT OF PROBABLE CAUSE.....	4
A.	DELAFRAZ, DANESHGAR, Wireless World, and Associated Financial Accounts.....	4
B.	Wireless World Procured Consumer Electronics and Gift Cards That Were Derived from Criminal Activity.....	9
1.	Coconspirator and Supplier Blade Bai.....	9
a.	DELAFRAZ and Bai WhatsApp Chats Show Numerous Transactions in Merchandise and Gift Cards.....	11
b.	Payments from Wireless World to Bai....	14
c.	Surveillance Confirmed Wireless World's Receipt of Merchandise from Bai.....	21
2.	Coconspirator and Supplier Juan Carlos Thola	22
a.	Thola Admitted Sale of Crime Proceeds to Wireless World.....	23
b.	DELAFRAZ and Thola WhatsApp Chats Confirm Repeated Sales of Stolen Merchandise.....	25
c.	Payments from Wireless World to Thola.	28
3.	Coconspirator A.....	29
a.	Communications with DELAFRAZ.....	29
b.	Communications with DANESHGAR.....	32
c.	Search of Coconspirator A's Residence and Car.....	33
4.	Coconspirator B.....	34
a.	Thefts in Georgia.....	35
b.	Gift Cards Redeemed in Los Angeles....	36

c.	Search of Coconspirator B's Yahoo Account.....	39
d.	Surveillance of Coconspirator B.....	40
e.	December 9, 2021 Search of Coconspirator B.....	41
5.	Coconspirators C & D.....	43
a.	Gift Card Schemes in the Los Angeles Area.....	43
b.	Confidential Human Source Sale of Merchandise to Coconspirator D.....	45
c.	Payments from Wireless World.....	46
d.	Communications with Wireless World....	46
e.	Communications with Coconspirator A...	49
f.	Search of Coconspirators C & D's Warehouse.....	50
6.	DELAFAZ and DANESHGAR Directly Purchased Electronics Using Gift Cards Funded with Fraud.....	51
a.	Nashville, Tennessee Credit Card Fraud	51
b.	Home Depot Orders Using Stolen Credit Cards.....	54
c.	Best Buy Online Orders Using Stolen Credit Cards.....	57
d.	Wireless World Purchases Identified by Home Depot.....	59
e.	Wireless World Purchases Identified by Best Buy.....	61
f.	Wireless World Purchases from Best Buy Identified Through UPS Records.....	64
C.	Wireless World Exports, Sales & Related Payments	66
a.	July 30, 2019 Inspection.....	67
b.	August 20, 2019 Inspection.....	69

c.	September 10, 2019 Inspection.....	71
d.	May 28, 2020 Inspection.....	74
e.	July 22, 2022 Inspection.....	75
f.	August 6, 2024 Export.....	75
g.	August 19, 2025 Inspection.....	76
i.	August 22, 2025 Inspection.....	77
D.	Fraudulent Economic Impact Disaster Loan.....	78
E.	Surveillance of Wireless World.....	80
1.	Physical Surveillance (2019).....	81
2.	FBI Surveillance Camera (2020).....	81
3.	HSI Surveillance Camera (2021).....	83
4.	HSI Surveillance Camera (2022).....	84
5.	Physical Surveillance (2025).....	84
F.	Ongoing Wireless World Operations.....	86
1.	Changed Shipping Patterns.....	86
2.	June 2025 Inspection in Miami.....	86
V.	CONCLUSION.....	91

AFFIDAVIT

I, Christopher Cutaia, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI") and have been employed by HSI for approximately 7 years. As part of my responsibilities, I have participated in numerous investigations into criminal offenses involving money laundering, unlicensed money remitting, financial frauds including wire and bank fraud and violations of Office of Foreign Asset Control ("OFAC") sanctions and am familiar with the means and methods used to commit such offenses. As a result of my training and experience, I am familiar with the techniques and methods of operations used by individuals involved in criminal activity to conceal their activities from detection by law enforcement officers.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against, and arrest warrants for SAMAN DELAFRAZ and BENJAMIN DANESHGAR for a violation of 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering).

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and

does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates, times, and dollar amounts are approximate.

III. SUMMARY OF PROBABLE CAUSE

4. The Federal Bureau of Investigation ("FBI") and HSI are investigating Wireless World, a business owned and operated by DELAFRAZ and DANESHGAR, for money laundering in connection with the domestic sale and international exportation of, among other things, millions of dollars' worth of consumer electronics and gift cards derived from a range of criminal activities, including, but not limited to wire fraud (18 U.S.C. § 1343), bank fraud (18 U.S.C. § 1344), interstate transportation of stolen property (18 U.S.C. §§ 2314, 2315), and identity theft (18 U.S.C. 1028).¹ Investigators have identified numerous suppliers, some of whom have previously been charged for their conduct, who were involved in the purchase of large volumes of consumer electronics using criminal proceeds which they then resold to Wireless World.

5. Wireless World currently operates from a warehouse in Van Nuys.² Since at least 2024, Wireless World has also operated from a warehouse in Delaware. Wireless World uses these

¹ Each of these underlying crimes is a "specified unlawful activity" for the purposes of money laundering as that term is defined in 18 U.S.C. § 1956(c) (7).

² Unless specified otherwise, the cities and locations identified in this affidavit are in California.

locations to aggregate electronics before shipping them out of the United States. Since 2019, Wireless World has exported more than \$611,000,000 in electronics from the United States, substantially all of which I believe to be the proceeds of crime for the reasons set forth in this affidavit. Wireless World continues to export large quantities of electronics, with shipments departing the United States as recently as September 2025.

6. The investigation into Wireless World has revealed that DELAFRAZ and DANESHGAR procure electronics and gift cards from many illicit sources, including, but not limited to those described in detail below:

a. Blade Bai and Coconspirators C and D sold electronics and gift cards to Wireless World. Those items were largely derived from telephone fraud schemes where victims were duped into purchasing and providing gift card numbers over the phone. Those gift cards, in turn, were used to purchase electronics and laundered into new gift cards to conceal the source of the funds.

b. Juan Carlos Thola³ sold electronics and gift cards to Wireless World. Those items were provided by Thola from December 2018 until August 2024. Thola acted as a coordinator and fence for South American crime tourism groups and other individuals who procured electronics and gift cards using stolen bank cards, among other means.

³ As discussed below, both Bai and Thola have been charged in this district in connection with some of the underlying criminal activity.

c. DELAFRAZ and DANESHGAR also acquired electronics directly themselves through fraud. They purchased electronics from Home Depot, Best Buy, and other retailers using gift cards that had been loaded with the proceeds of fraud - primarily with stolen credit cards. Those electronics were often shipped directly to the Wireless World warehouse or to mailboxes controlled by DELAFRAZ and DANESHGAR.

d. Coconspirators A and B sold electronics and gift cards to Wireless World. They acquired fraud-funded gift cards from and used those gift cards to purchase electronics.

IV. STATEMENT OF PROBABLE CAUSE

A. DELAFRAZ, DANESHGAR, Wireless World, and Associated Financial Accounts

7. From California Department of Motor Vehicles ("DMV") records, I know that DELAFRAZ is 32 years old, and a resident of Woodland Hills, and DANESHGAR is 34 years old and a resident of Los Angeles.

8. DELAFRAZ and DANESHGAR have operated using the business name Wireless World since 2015. Bank records, U.S. Customs records, and surveillance show that over the last 10 years, they have operated the business using various locations. Wireless World is currently located at 16141 Leadwell St., Van Nuys (the "Wireless World warehouse"), and has operated at that location since approximately February 2020.

9. More recently, Wireless World has also operated at 161-A Cirillo Circle, in New Castle, Delaware under a subsidiary named MaxOutDeals (the "MaxOutDeals warehouse".)

10. From California Secretary of State records, and other records received during this investigation, I know that DELAFRAZ and DANESHGAR have also operated using the names MaxOutDeals, MaxoutDeald, Mobile Deals, Inc., Global Wireless, West Coast Distributors, Virtual Wireless, Wireless Deals, Wireless Warehouse Direct, Gadget Stop, 2D Distribution.

11. Financial records, including doing business as ("d.b.a.") documentation and communications between DELAFRAZ, DANESHGAR, and their criminal coconspirators and affiliates, consistently use the name Wireless World to refer to the operation controlled by DANESHGAR and DELAFRAZ. The business is therefore referred to as Wireless World.

12. From my review of bank and financial records, and participation in this investigation, I know that DELAFRAZ and DANESHGAR established and operated bank accounts to aid in the operation of their scheme, including three accounts held at Cathay Bank in Los Angeles ("Wireless World Cathay Accounts"):

a. An account ending in 5080⁴ in the name of "Wireless World" ("Wireless World Cathay Account #1").

b. An account ending in 2155 in the name of "Wireless World" ("Wireless World Cathay Account #2"). Between June 14, 2024 and June 6, 2025, this account received nine wire transfers totaling \$1.125 million from Mexican bank InterCam Banco S.A., which was sanctioned on June 25, 2025, by the Office of Foreign Asset Control ("OFAC") for being of primary money

⁴ Financial accounts, including bank and credit card accounts are identified throughout this affidavit using only the last four digits of the account number.

laundering concern in connection with illicit opioid trafficking as a result of its long-standing pattern of associations, transactions, and provision of financial services that facilitate illicit opioid trafficking by Mexico-based cartels.

c. An account ending in 1761 in the name of "Wireless World" under the California registered d.b.a. "2D Distribution" ("Wireless World Cathay Account #3"). This account was opened on June 25, 2025, the same day that OFAC sanctions were announced against Intercam Banco S.A.

13. The Wireless World Cathay Accounts have served as Wireless World's primary bank accounts between 2019 and 2025. Based on my participation in this investigation and review of bank records, I know that DELAFRAZ and DANESHGAR have had other bank and financial accounts since 2015, but that many of those accounts have been closed by financial institutions based on concerns about fraud and money laundering. DELAFRAZ and DANESHGAR's operations appear to have generated significant income, not all of which is readily apparent in U.S. financial accounts that have been identified in this investigation. For the reasons described below, I believe that DELAFRAZ and DANESHGAR hold significant assets in some combination of cash, offshore accounts, and virtual assets.

a. As discussed in Section IV.D below, in 2020, Wireless World fraudulently applied for and received a Small Business Association loan. In the application for that loan, DELAFRAZ and DANESHGAR claimed net profit of \$883,929 in 2019 on

gross revenues of more than \$16 million. Those funds are not readily apparent in any identified financial accounts.

b. Export records show \$611 million in exports, and DANESHGAR's personal website www.bendanesghar.com claims that his companies have made more than \$1 billion in sales. Based on those figures, the expected profits from Wireless World operations are in the millions or tens of millions. Investigation to date has not identified U.S. financial accounts containing funds commensurate with the sales by Wireless World.

c. The investigation to date shows that some proceeds of this criminal scheme have been invested into real property. DANESHGAR owns a residence in Studio City, and 21% of the purchase price of that home was paid directly from the Wireless World Cathay Accounts. DELAFRAZ owns a residence in Los Angeles, and approximately 22% of the purchase price of that home was paid from the Wireless World Cathay Accounts via a now-closed Citibank account held in DELAFRAZ's name.

d. DELAFRAZ's Citibank account was closed in October 2024 by Citibank. While open the account maintained an average balance of approximately \$175,000. When it was closed, the funds were not moved to any known U.S. financial account.

e. Legal process on U.S. financial institutions and virtual asset service providers has not identified any accounts holding significant assets. DANESHGAR has a CapitalOne bank account that, between 2022 and 2025 has had an average balance of less than \$3,000. Both DANESHGAR and DELAFRAZ have accounts

with Coinbase and Robinhood Securities with relatively small balances.

f. Based on communications and photographs found in chats involving DANESHGAR, DELAFRAZ, and coconspirators, and police reports, I know that DELAFRAZ regularly maintains large amounts of cash, over \$100,000 either on his person or in the Wireless World warehouse.

g. Based on communications between DELAFRAZ and Blade Bai, discussed in part below in Section IV.B.1 below, I know that Wireless World maintained bank accounts outside the United States that it used to facilitate domestic transactions for electronics.

h. Based on travel records, recovered chats, export records, and financial records, I know that DELAFRAZ and DANESHGAR have established significant financial and personal relationships with entities and individuals in the United Arab Emirates. For example, a June 2022 article published online in the Dubai-based Khaleej Times details DANESHGAR's elaborate marriage proposal in Dubai and includes a statement from DANESHGAR that "Dubai will always be our home."

14. Based on my training and experience and my review of the financial records in this investigation, I believe that DELAFRAZ and DANESHGAR have taken steps to conceal the proceeds of their criminal conduct outside of the U.S. financial system, and likely hold those proceeds as cash, virtual assets, and in hidden foreign bank accounts and/or property holdings.

B. Wireless World Procured Consumer Electronics and Gift Cards That Were Derived from Criminal Activity

15. Based on my participation in this investigation, I know that DELAFRAZ and DANESHGAR conspired with various sources of supply for gift cards and goods derived from fraud, which they procured and sold onward. Two significant sources identified during this investigation were coconspirators Blade Bai and Juan Carlos Thola, each of whom has already been charged criminally for related conduct. Bai and Thola both provided electronics and gift cards to Wireless World. The electronics and gift cards were sold to Wireless World at below retail prices, even though Bai, Thola, and their confederates purchased many of the products at retail stores in California, where the state sales tax is at least 7.25%. Wireless World received goods and gift cards from numerous other suppliers, including Coconspirators A, B, C, and D, whose roles are discussed in more detail below. Finally, DELAFRAZ and DANESHGAR directly purchased goods themselves for resale through Wireless World using stolen credit cards and gift cards derived from fraud. DELAFRAZ and DANESHGAR laundered the proceeds of the crimes committed by themselves and their coconspirator suppliers through their export and sale of electronics.

1. Coconspirator and Supplier Blade Bai

16. In a November 2020 complaint, and subsequent indictment in Case No. 20-CR-621-AB in the Central District of California, a group of individuals, including Blade Bai were charged with money laundering conspiracy (the "Bai Indictment").

Bai was part of a gift card money laundering operation that used gift cards that were the proceeds of fraud to purchase high-value merchandise, such as electronic devices, at Target stores. Bai sold electronic devices and gift cards to Wireless World. Bai was convicted at trial and is currently serving a 15-year sentence.

17. The defendants in the Bai Indictment were charged in connection with a scheme in which scammers fraudulently induced victims, over the telephone, to purchase gift cards to resolve some nonexistent issue. One common scheme was the government imposter scam, in which scammers impersonated Social Security Administration or other government personnel, telling victims that their social security numbers had been compromised and that they had been used in crimes throughout the United States. Another common scheme was the technical-support scam, in which scammers told victims that their computers had been hacked. In all cases, the scammers duped the victims into buying Target gift cards to resolve the purported legal issue. The victims were then instructed to read off the gift card numbers and access codes over the phone to the scammers.

18. In actuality, the scammers generally, through other scheme participants, used the gift card information to purchase high-value merchandise, such as electronic devices, at Target stores. The merchandise was then largely resold or returned to a Target store for store credit to load onto new gift cards. This cycle of transactions helped to launder the fraud proceeds

and conceal the source of the funds loaded on the resulting gift cards.

19. Wireless World paid Bai for his merchandise primarily through wire transfers from the Wireless World Cathay Accounts. Between 2019 and November 2020 accounts associated with Bai received approximately \$11.419 million in wire transfers. Wire transfers were made to Bai's personal bank accounts and business accounts of entities registered to, or controlled by, Bai, including Enterfix and Catfish International Trading, Inc. Bai also used business accounts registered to, or controlled by, his associates to receive funds. Checks from the Wireless World Cathay Accounts were issued to two of those third-party entities. The checks were always written for quantities under the bank reporting threshold of \$10,000.

a. DELAFRAZ and Bai WhatsApp Chats Show Numerous Transactions in Merchandise and Gift Cards

20. Pursuant to a federal search warrant, I searched Bai's iPhone, and seized, among other things, conversation threads between Bai and DELAFRAZ using the messaging application WhatsApp. In those discussions, DELAFRAZ communicated using a telephone number ending in 3005, which I know from AT&T records is registered in DELAFRAZ's name. In those threads, Bai and DELAFRAZ discussed, at length, the sale of electronics and gift cards. Those discussions generally involved negotiations about the price that Wireless World would pay for items that Bai offered for sale. Some examples of those discussions follow.

Participant	Message
DELAFAZ	When r we gonna be up and running again?
Bai	Still running
DELAFAZ	I mean real running like before
DELAFAZ	200 iPad, 400 console. 200 AirPod
DELAFAZ	This kind lol
Bai	Not gonna be like that much bro
DELAFAZ	Those days over? Or will start again
Bai	Will be slower
Bai	More will be cards
Bai	But cost will higher
DELAFAZ	Cards is fine too.
Bai	Yea
DELAFAZ	What will cost be
Bai	78-80
Bai	Depends
Bai	Mine will be 78
Bai	The ones I bought will be 80

21. Based on my training and experience and knowledge of this investigation, I understand that in this October 22, 2019 conversation, Bai was informing DELAFRAZ that he would no longer be able to provide hundreds of Apple products at a time but would be shifting to selling DELAFRAZ more gift cards. I understand Bai's mention of "78-80" to refer to his sale price to DELAFRAZ as a percentage of the face value of the gift card, i.e. 78-80% of the face value of the gift cards.

22. On December 12, 2019, Bai and DELAFRAZ exchanged a series of messages about gift cards. Bai sent DELAFRAZ a photograph of gift cards sitting on a table that I recognize as being in Bai's home based on my observation of the table when I executed a warrant there. Bai wrote "[d]amn I hate counting." DELAFRAZ told Bai he would come pick up the cards, and Bai sent his home address. Bai then sent a series of images of individual cards wrapped in receipts with the face value total of the cards written on them, and with the following

explanations "Tt 36902," "Wm 58665," "iTunes 5300," "Google 15660," "Steam 450," and "Nintendo 50." He then sent a series of messages that I understand from my experience with this investigation to be the percentages of face value at which Bai was selling each card, "Tt wm 85" (Target, Walmart 85%), "iTunes google 83" (iTunes, Google 83%), "Steam 8" (Steam⁵ 80%), and "Nintendo 75" (Nintendo 75%).



23. From my participation in this this investigation, I believe that these stacks of gift cards wrapped in receipts with dollar totals and values likely depict the laundered proceeds of gift card return scams by Bai and money mules working for him. This methodology of moving victim funds to different gift card numbers is a tactic I routinely observed during this investigation, wherein the movement of funds creates obstacles for law enforcement, retailers and banks in tracing and recovering victims' money, and allows more time for criminal actors to spend and further launder the fraud proceeds.

⁵ Steam is an online video game distribution platform.

24. On February 26, 2020, Bai informed DELAFRAZ he may scale down his business and said "And I hear some thing(sic) about investigation"; "Don't wanna get in trouble"; "So only doing with trusted people now." DELAFRAZ replied "got it. yeah man you should always stay safe first."

25. On June 19, 2020, Bai and DELAFRAZ discussed meeting at Bai's warehouse location in Baldwin Park that evening, however, Bai decided against it because "My warehouse has a lot cops are(sic) night"; "Don't wanna have trouble". DELAFRAZ said he would come the following day.

b. Payments from Wireless World to Bai

26. Bai supplied Wireless World with both electronics and gift cards from at least April 2019 through mid-November 2020, when he was arrested by HSI in Los Angeles on federal charges.

27. During 2019, Bai primarily operated under the business name Enterfix. From my review of Cathay Bank and Bank of America ("BOA") records, I identified 59 wire transfers totaling \$5,576,647 sent from Wireless World Cathay Account #1 to Bai's Enterfix BOA bank account (x4042).

28. In late 2019, Bai began operating another bank account at BOA under the business name Catfish International Trading Inc. ("Catfish"). Wireless World made additional payments totaling \$861,653 to Bai's Catfish BOA bank account (x8007).

29. Based on my review of a Fontana Police Department ("FPD") report, I learned that a state search warrant was executed by FPD Detectives at Bai's Enterfix location in Temple

City on September 25, 2019, after a phone scam victim reported being defrauded.

30. During the FPD investigation, investigators determined that Bai used the Enterfix and Catfish BOA accounts to transact in illicit proceeds. After Bai's encounter with FPD in September 2019, I observed a change in Wireless World and Bai's financial transactions.⁶ Specifically, Wireless World began paying Bai through third-party foreign and domestic bank accounts. During my search of Bai's iPhone, I identified many WhatsApp messages between Bai and DELAFRAZ detailing these transactions.

31. One foreign entity receiving payments from Wireless World on Bai's behalf was "Home Electronic Commerce Limited," which held an account at Standard Chartered Bank (China) Limited. During 2020, Wireless World sent wire transfers totaling \$3,093,968 from Wireless World Cathay Account #1 to the Home Electronic Commerce account in China. Below are examples of wire transfers that I know from my review of WhatsApp messages represent funds paid by Wireless World to Bai for merchandise and gift cards.

a. On June 30, 2020, DELAFRAZ responded to a list of Apple products and prices sent by Bai in the following exchange. The exchange included an image which showed bank account details for the Home Electronic Commerce Limited bank account.

⁶ From bank records, I learned that in late 2019, Bai opened bank accounts with Cathay Bank in Los Angeles, at least one of which was in the name of Catfish.

Participant	Message
DELAFAZ	how much do you want me to wire (sic)
Bai	Just 10k
Bai	100k
Bai	[image showing bank account details]
Bai	This one 100k
DELAFAZ	can i put random number (sic)
DELAFAZ	or has to be 100k even (sic)
Bai	Around 100k maybe
DELAFAZ	like 101541
DELAFAZ	this is ok?
DELAFAZ	or closer to 100k
Bai	Yea
DELAFAZ	Don't have to be even
DELAFAZ	ok ill(sic) send in 30 min with all my other wires.

b. On June 30, 2020, consistent with this exchange, Wireless World sent \$101,541 from Wireless World Cathay Account #1 to the Home Electronic Commerce bank account in China.

c. September 17, 2020, Bai again directed DELAFRAZ to use the Home Electronic Commerce bank account to pay Bai \$68,000 for another transaction.

d. On the same day, in the message exchange shown below, DELAFRAZ wired an additional \$150,000 to the Chinese account to conduct a U.S. Dollar to Chinese Renminbi currency exchange transaction with Bai. The exchange included an image of wire transfer receipt showing the transfer of \$218,382 on September 17, 2020 from Wireless World Cathay Account #1 to the Home Electronic Commerce bank account in China.

Participant	Message
DELAFAZ	your po is 68k. im adding 150k to it right
DELAFAZ	so like 220 is ok to send?
Bai	Ok
DELAFAZ	[wire transfer receipt]
Bai	Ok

e. Based on my review of the U.S. government's Financial Crimes Enforcement Network database, Bai, DELAFRAZ, DANESHGAR, and their various business entities were not licensed to operate as money service businesses.

f. From my review of WhatsApp chats, I also learned that Bai used at least two other domestic business bank accounts at BOA in Los Angeles to received funds from Wireless World on his behalf.

i. On September 23, 2020, Bai sent DELAFRAZ a list of mostly Apple and Nintendo electronics, to which DELAFRAZ responded that he would purchase most of the batch and asked to send Bai a wire payment. Bai sent the details for one of the third-party accounts at BOA, along with a message saying "150025." DELAFRAZ responded with an image showing a completed wire of \$150,025 from Wireless World Cathay Account #1 to the third-party BOA account. During 2020, Wireless World sent a total of \$548,585 to this third-party BOA account on Bai's behalf.

ii. On November 3, 2020, Bai sent DELAFRAZ a list of electronics and asked that DELAFRAZ send a driver to pick the items up at his residence. Bai sent the details for the other the third-party account at BOA, along with a message saying "59026." DELAFRAZ responded with an image showing a completed wire of \$59,026 from Wireless World Cathay Account #1 to the third-party BOA account. During 2020, Wireless World sent a total of \$411,978 to this third-party BOA account on Bai's behalf.

32. In June 2020, I searched Bai's Google and Microsoft email accounts pursuant to search warrants. In the accounts, I found numerous Target store gift card numbers derived from phone scam victims. I also found over 70 Wireless World purchase orders from April 2019 to May 2020 documenting the sale of millions of dollars of consumer electronics and gift cards at below-market prices. Two examples are shown below: one purchase order for electronics, and another for gift cards. From my research into prices at that time, I know that the prices that Wireless World paid Bai for the electronics were below those charged by major retailers for the same products. Similarly, the prices paid for the gift cards listed below were significantly below face value, which I know to be a hallmark of the sale of fraud-derived gift cards. The first invoice shown also includes an entry for "TG 25k x .86" with a charge of \$25,000. I understand this entry to correspond to the sale of \$25,000 worth of Target gift cards at 86% of face value.

//

//

//



Wireless World
16141 Leadwell
Van Nuys, CA 91406

Purchase Order

VENDOR
Catfish International Trading Inc

SHIP TO
Wireless World
16141 Leadwell
Van Nuys, CA 91406 US

P.O. DATE 1089
05/08/2020

DESCRIPTION	QTY	PRICE	AMOUNT
Apple - AirPods with Wireless Charging Case - White	1	133.00	133.00
Apple - AirPods Pro - White	6	200.00	1,200.00
Apple - AirPods with Charging Case - White	8	107.00	856.00
Nintendo - Switch 32GB Lite - Yellow	16	180.00	2,880.00
Nintendo - Switch 32GB Lite - Gray	6	180.00	1,080.00
Nintendo - Switch 32GB Lite - Turquoise	2	180.00	360.00
TG 25k x .86	1	21,500.00	21,500.00
TOTAL			\$28,009.00



Wireless World, Inc
9649 Ownesmouth Ave.
Chatsworth, CA 91311

Purchase Order

Date	P.O. No.
12/3/2019	3797

Vendor

Enterlix
9550 Las Tunas Dr.
Tempe City, CA, 91780

Ship To

Wireless World, Inc
9649 Ownesmouth Ave.
Chatsworth, CA 91311

Item	Description	Qty	Rate	Amount
google play \$100 ...	Google Play \$100 Gift Card	128	83.00	10,624.00
Google Play \$50 ...	Google Play \$50 Card	2	41.50	83.00
iTunes \$100 Gift ...	iTunes \$100 Gift Card	29	83.00	2,407.00
xbox \$100 Gift Card	Xbox \$100 Gift Card	105	75.00	7,875.00
xbox \$50 card	XBOX \$50 Gift Card	2	37.50	75.00
Nintendo eShop \$...	Nintendo eShop \$50 Gift Card	35	37.50	1,312.50
STEAM \$50 Gift ...	STEAM \$50 Gift Card	16	40.00	640.00
Total				\$23,016.50

33. During this investigation, I also learned that at times Wireless World sold products through online platforms operated by Walmart. For commercial reseller accounts like those that were operated by Wireless World, the seller is often required to substantiate and document the source of supply for the goods sold. One reason that Wireless World likely issued invoices in connection with otherwise criminal transactions was to create a false paper trail to present a veneer of legitimacy for the online sales of goods through reputable third-party sales platforms.

34. I know from my training and experience that in normal circumstances, businesses do not sell goods for less than they paid for the goods. I also know from this investigation, that Bai acquired gift cards at a substantial discount from the face value of the corresponding gift card. When those fraud-derived gift cards were used to purchase merchandise, that merchandise was effectively purchased at a similar discount to the gift cards.

35. I also learned that one reason gift cards would be substantially discounted is the risk they would be cancelled or rendered unusable because they were stolen or obtained by fraud. This discount to face value of the gift card represents the buyer's risk of losing the full value of the card due to its fraudulent nature. Conversely, the seller is willing to sell the gift card for an amount below face value (for example, selling a \$250 gift card for \$200) because the gift card was

obtained by fraud and the seller either did not pay for it or their cost to obtain the gift card was minimal.

*c. Surveillance Confirmed Wireless World's
Receipt of Merchandise from Bai*

36. From July 7, 2020, to November 14, 2020, FBI personnel operated a remote surveillance camera at the Catfish warehouse location in Baldwin Park. The following is a summary of observations and analysis from camera footage.⁷

37. A cargo van registered to Wireless World (the "Wireless World van") was seen at Bai's warehouse 19 times. On many occasions, the Wireless World van drove into the cargo bay and out of view. However, on several occasions, the Wireless World van was visible, including the following:

a. On July 15, 2020, at 2:16 p.m. Bai's employee provided the driver of the Wireless World van a box.

b. On August 5, 2020, at 2:30 p.m. Bai's employee and the Wireless World van driver loaded seemingly full Target retail store shopping bags into the Wireless World van.

c. On November 9, 2020, at 1:35 p.m. Bai's employee loaded several boxes which appeared to contain Apple products into the Wireless World van.

d. On November 12, 2020, at 1:57 p.m. Bai's employee provided a box containing what appeared to be Apple products to the Wireless World van driver.

38. I also cross-referenced observations from the Catfish surveillance camera with observations from an FBI surveillance

⁷ The camera was situated at the cargo bay/rear area of the location, and the front of the business was not visible.

camera at the Wireless World warehouse during a similar period and identified the following instances:

a. On August 18, 2020, at 12:17 p.m. the Wireless World van entered the Bai warehouse's cargo bay and was observed at 2:04 p.m. entering the Wireless World warehouse cargo bay.

b. On September 14, 2020, at 12:23 p.m. after the Wireless World van was observed entering the cargo bay at Bai's warehouse, it was observed back at the Wireless World warehouse at 3:10 p.m., where workers offloaded approximately ten Target retail store shopping bags, as shown below.



2. Coconspirator and Supplier Juan Carlos Thola

39. In August 2024, in Case No. 24-CR-471-MWF in the Central District of California, a group of individuals, including Juan Carlos Thola were indicted for crimes including wire fraud, interstate transport of stolen merchandise, sale of stolen merchandise and money laundering (the "Thola Indictment"). The charges in that case related directly to the

sale of merchandise and gift cards by the defendants to Wireless World (identified as "Fence 2" in the Thola Indictment).

40. Based on my discussions with other law enforcement officers and my review of investigative reports, I know that the FBI Los Angeles Major Theft Task Force investigated a network of theft crews whose members committed thefts and burglaries all over the United States. Theft crew members stole victims' credit cards and debit cards and then used the stolen credit and debit cards to purchase gift cards, electronics, and other portable items that the members then shipped or mailed to members of the network based in Los Angeles. Those confederates then fenced the items purchased with the stolen credit and debit cards and laundered the proceeds.

41. Thola was a fence for the merchandise provided by theft crew members, arranging for the items to be sent to him and his associates in Los Angeles, and paying the theft crew members for the items. Thola and his coconspirators sold many of these stolen or fraudulently purchased goods to Wireless World. Thola sold merchandise and gift cards to Wireless World at prices well below retail prices but still earned a profit from those sales because the goods had been procured through crime.

a. Thola Admitted Sale of Crime Proceeds to Wireless World

42. From approximately July 2021 through early September 2022, HSI operated a surveillance camera overlooking the parking lot area of Wireless World's warehouse, which I or another

investigator reviewed and logged daily. On September 1, 2022, Thola was seen delivering goods in Best Buy bags the Wireless World warehouse. On October 4, 2022, approximately one month after being seen on the surveillance camera at Wireless World, Thola received a wire transfer of \$20,000 to a JP Morgan Chase account (x7012) that he controlled.

43. In May 2025, I interviewed Thola in Los Angeles along with FBI Special Agents. Thola admitted to knowingly selling stolen or fraudulently purchased goods to Wireless World, and specifically to DELAFRAZ and DANESHGAR. Thola said that he communicated with DELAFRAZ and DANESHGAR using WhatsApp, and that he sold electronics and gift cards to Wireless World at a fraction of the retail price for those items. Thola explained that DELAFRAZ would sometimes provide him with money in advance of Thola's delivery of merchandise. Investigators have recovered a large collection of WhatsApp messages between DELAFRAZ and Thola that confirms this relationship and includes numerous discussions of outstanding payment balances between Wireless World and Thola.

44. Thola explained that at the Wireless World warehouse, he provided stolen and fraudulently acquired merchandise directly to DANESHGAR and DELAFRAZ. Thola said that he visited the warehouse on an almost daily basis, and that he saw individuals arrive at Wireless World throughout the day to deliver electronics and gift cards and/or receive payment for products from DANESHGAR, DELAFRAZ, or one of their employees. These observations are consistent with the steady flow of people

delivering items to the warehouse observed during surveillance of the Wireless World warehouse.

b. DELAFRAZ and Thola WhatsApp Chats Confirm Repeated Sales of Stolen Merchandise

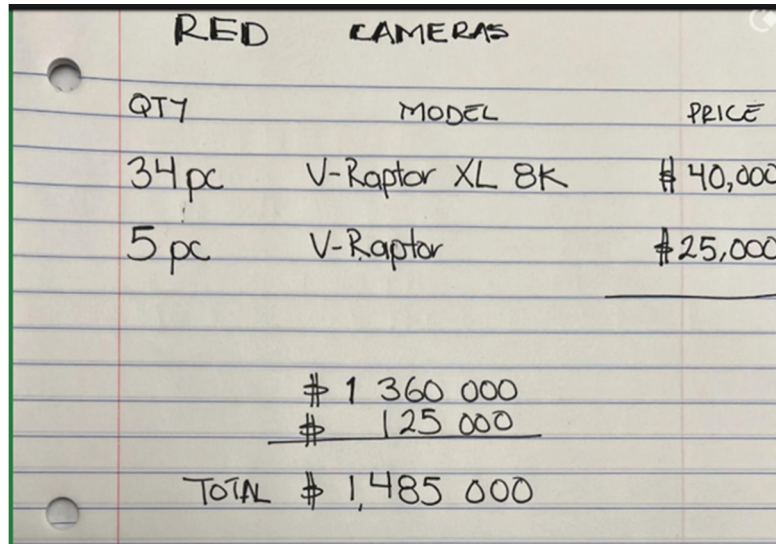
45. In August 2024, pursuant to a federal warrant, Thola's residence was searched, and an Apple iPhone 15 (the "Thola iPhone") was seized. Thola told investigators that this was the device that he used to communicate and conduct business primarily with DELAFRAZ, but also with DANESHGAR.

46. The Thola iPhone includes a WhatsApp conversation thread consisting of 846 messages and calls between Thola and DELAFRAZ from May 16, 2024 to August 27, 2024. I know that Apple released the iPhone 15 model in September 2023, and I believe that earlier discussions between Thola and DELAFRAZ likely took place on older devices.

47. From the Thola iPhone, Thola sent and received WhatsApp messages with Wireless World, primarily with DELAFRAZ, but also with DANESHGAR, using the same numbers that they used to communicate with Bai.

48. Thola told investigators that he frequently took pictures of invoices for DELAFRAZ and sent them via WhatsApp message as a record of agreed upon prices for merchandise that Thola offered to Wireless World. My review of Thola's WhatsApp communications confirmed this claim.

49. On July 2, 2024, Thola sent the following image to DELAFRAZ which shows the sale of high-end digital cameras at prices below the retail price.



QTY	MODEL	PRICE
34 pc	V-Raptor XL 8K	\$ 40,000
5 pc	V-Raptor	\$ 25,000
		\$ 1 360 000
		\$ 125 000
		TOTAL \$ 1,485 000

50. From my review of the device manufacturer's website in July 2025, I believe the item listed as "V-Raptor XL 8k" is a Red Digital Cinema camera that retailed for approximately \$44,995. From a camera distributor website, I also learned that the second item on the list, V-Raptor, likely refers to a camera called "V-Raptor X" which retailed for roughly \$34,250 at the time.

51. On August 13, 2024, Thola sent an image of an invoice listing devices identified by Universal Product Code ("UPC") which I learned during the investigation is a term widely used in the retail industry to identify products. I determined that the UPCs depicted in the image corresponded to Dahua brand electronic security cameras.

52. Thola told investigators that he would provide Wireless World with fraudulently purchased gift cards. In

WhatsApp messages, Thola and DELAFRAZ discussed situations where gift cards became "no good" or would no longer work. Based on my experience during this investigation and others, a gift card becoming "no good" refers to situations where gift cards, if fraudulently purchased, become unusable due to a victim's intervention through reporting fraud to their bank or law enforcement. For example, on July 23, 2024, DELAFRAZ sent Thola a WhatsApp message noting that a "bunch of cards" did not function.

53. Thola also communicated with DANESHGAR. For example, on June 28, 2024, Thola sent DANESHGAR messages trying to sell Dyson vacuums, including "544 pieces Dyson V8 Origin Extra." Thola then sent a screenshot of an ecommerce site listing the price for the vacuums as \$419 each and offered them for \$160. To this, DANESHGAR responded that the price was lower, saying "It's \$279 at sams club," and following up with a web screenshot showing that the vacuums were selling at Sam's Club for \$299.98. Thola responded by dropping his price for the vacuums to \$130. Based on this discussion, it is my understanding that DANESHGAR was negotiating with Thola to purchase the Dyson vacuums for less than half of the retail price, which is consistent with the purchase of stolen merchandise.

54. Eventually Thola offered Wireless World entire cargo shipments of suspected stolen goods for purchase. For example, on August 24, 2024, Thola sent an image of the interior of a cargo van full of what I believe to be stolen electronics. Thola asked "You buy my friend," to which DELAFRAZ responded

"Yea." Based on my training and experience, and knowledge about the interactions between DELAFRAZ and his suppliers, I know that DELAFRAZ and Wireless World, would sometimes decline to buy goods if they did not think they had a buyer overseas.

c. Payments from Wireless World to Thola

55. Between December 2018 and August 2024, bank accounts owned or controlled by Thola and his coconspirators received a total of approximately \$5.2 million from Wireless World Cathay Account #1. Those payments were primarily made through wire transfers. Wireless World sent payments for stolen or fraudulently purchased goods to approximately 10 different bank accounts controlled by Thola and his conspirators. Examples of these payments include the following:

a. On December 10, 2021, a confederate of Thola, on Thola's behalf, received a wire payment of approximately \$120,000 from Wireless World Cathay Account #1 into her account at Bank of the West.

b. On January 19, 2023, a confederate of Thola, on Thola's behalf, received a wire payment of approximately \$20,000 from Wireless World Cathay Account #1 into his Wells Fargo business account.

c. On October 18, 2022, a confederate of Thola, on Thola's behalf, received a wire payment of approximately \$30,000 from Wireless World Cathay Account #1 into his Wells Fargo personal account.

d. On March 29, 2024, a confederate of Thola, on Thola's behalf, received \$9,000 into his Bank of America account from Wireless World Cathay Account #1.

e. Wireless World Cathay Account #1 issued check number 7236 in the amount of \$14,000 made payable to "John Carlo Thola" and dated "8/27/24."

3. Coconspirator A

56. Coconspirator A was a supplier of fraudulently obtained goods involved with both Bai and Wireless World. On September 7, 2021, pursuant to a federal search warrant HSI and FBI Special Agents seized digital devices belonging to Coconspirator A. Among the devices seized and searched was a black iPhone Mini. I reviewed WhatsApp chats on that device between Coconspirator A and DELAFRAZ and DANESHGAR. Below are examples of relevant communications.

a. Communications with DELAFRAZ

57. On August 21, 2019, Coconspirator A sent DELAFRAZ a photograph of a notepad containing a handwritten list of Apple products. DELAFRAZ responded and asked Coconspirator A to send him an invoice. Coconspirator A responded with an invoice on August 21, 2019, listing the electronics and a total of \$55,225.

58. On September 18, 2019, Coconspirator A and DELAFRAZ had a series of communications where Coconspirator A sold DELAFRAZ Target and Best Buy gift cards. In those communications, in advance of payment from DELAFRAZ, Coconspirator A provided the card numbers, access codes, and corresponding dollar values. The Target cards were sold at

78.5% of the dollar value of the card and the Best Buy cards for 91%. Coconspirator A instructed DELAFRAZ that the card numbers needed to be used by the following day.

59. Later that day, DELAFRAZ informed Coconspirator A that one of the Best Buy card numbers was "no good." Coconspirator A responded the following day and asked if the cards had all been used yet. In reply, DELAFRAZ said that the Best Buy cards had been used, but not the Target cards.

60. On October 17, 2019, Coconspirator A sent DELAFRAZ additional gift card numbers and access codes in the following quantities: Best Buy (\$2,484), Target (\$10,000), and Apple (\$2,865). In response, DELAFRAZ asked how long he had to spend the cards, and Coconspirator A responded "[t]hey are good to hold. But I don't pay till it's spent." Coconspirator A later informed DELAFRAZ that the purchase price for the Best Buy and Apple cards was 92% of the face value, while the Target cards were 78.5% of face value.

a. Among the cards sent by Coconspirator A were two Target gift cards with a value of \$1,000 each. Information from the Target National Investigations Center ("TNIC") showed that these cards were funded, in part, using two other Target gift cards purchased by fraud victim R.H.R. in Louisiana in October 2019.

b. Based on my review of a Kenner Police Department report I learned that victim R.H.R, of Louisiana, reported to police that in October 2019 he received phone calls from an unknown individual who told him "his safety was not guaranteed"

and he and his sister would be subject to an accident that would result in bodily harm if funds were not provided to the caller in the form of gift cards (including Target cards). Victim R.H.R. stated he purchased the gift cards and provided them over the phone to the scammer.

61. On November 5, 2019, in a discussion about gift cards, DELAFRAZ asked about the time frames within which certain gift cards can be "run," and Coconspirator A responded that the Target cards needed to be "ran" within "24hrs."

62. On December 11, 2019, Coconspirator A sent DELAFRAZ screenshots of digital Best Buy gift cards totaling \$1,300.

63. On December 23, 2019, Coconspirator A and DELAFRAZ had the following exchange:

Participant	Message
DELAFAZ	gm. do you have any ipad air, ipad pro, series 5 watch?
Coconspirator A	no sir, federal investigation launched in oregon for gift cards
DELAFAZ	how u know?
Coconspirator A	one of the guys i deal with here told me
Coconspirator A	target sent out a statewide memo to oregon no more bulk due to ... anyone asking for more than usual refuse service completely. and an investigation has been going on and is still.

64. On January 13, 2020, Coconspirator A sent DELAFRAZ three photos of physical Best Buy gift cards with the card numbers and access codes scratched off the back.

65. On January 27, 2020, Coconspirator A and DELAFRAZ discussed money remittances. Coconspirator A asked that DELAFRAZ arrange for him to receive between \$100,000 to \$150,000 in cash in exchange for Coconspirator A wiring the same amount

of funds to a domestic or foreign bank account with a 0.5% fee added. DELAFRAZ informed Coconspirator A the cash pickup would occur approximately thirty miles away and he would make the drive, as he needed to pick up cash for himself as well.

66. On February 12, 2020, Coconspirator A sent DELAFRAZ two batches of Best Buy gift cards - one a list of numbers and access codes, the other a set of photos. The total value of these gift cards was \$6,462, and Coconspirator A informed DELAFRAZ that the sale price was 92% of face value.

b. Communications with DANESHGAR

67. On August 8, 2019, Coconspirator A sent a screenshot of a message thread with DELAFRAZ to DANESHGAR. In the included screenshot, Coconspirator A offered to provide Target gift cards to DELAFRAZ on a daily basis.

68. On September 9, 2019, Coconspirator A and DANESHGAR discussed a large dollar quantity of Target gift cards that "went bad." Coconspirator A indicated to DANESHGAR that "200tg I had for you went bad," and that the "168 I gave you is all bad." I understand this to mean that Coconspirator A had previously sold DANESHGAR 168 Target gift cards that had lost their value, and that an additional 200 Target gift cards that Coconspirator A had intended to sell to DANESHGAR also lost their value.

69. On September 23, 2019, Coconspirator A and DANESHGAR had the following exchange. Based on my participation in this investigation and knowledge of events involving Bai, I understand that Coconspirator A was checking in with DANESHGAR

after learning that Bai's business had been searched by the Fontana Police Department after some of Bai's runners (referred to by DANESHGAR as "the girls") had been encountered by law enforcement purchasing bulk quantities of electronics using gift cards derived from fraud.

Participant	Message
Coconspirator A	You good ?
DANESHGAR	Yessir you
Coconspirator A	Ya
Coconspirator A	You heard about blade right
Coconspirator A	I heard you heard
DANESHGAR	The girls ?
DANESHGAR	I saw that nuts

70. In sum, I located numbers and access codes for more than 800 Target gift cards in Coconspirator A's WhatsApp communications with DELAFRAZ and DANESHGAR. Information received from TNIC allowed me to identify approximately 24 phone scam victims linked to those Target gift cards. I confirmed the victims and their connection to the gift cards at issue through Target records and either state and local police department reports or my interviews victim or related witnesses.

c. Search of Coconspirator A's Residence and Car

71. On May 19, 2020, pursuant to a California state search warrant, the Los Angeles Police Department searched Coconspirator A's residence and car. I participated in the search. From my participation and my review of records related to the search, I know that the following items, among others, were found and seized during the search:

a. Approximately 23 laptops in manufacturer's boxes, many of which had stickers indicating that they had been purchased at Best Buy.

b. Approximately 1000 gift cards, consisting primarily of cards from Amazon, Walmart, and Target.

c. A letter addressed to DANESHGAR at an address in Encino, California.

d. An Apple store receipt from Tigard, Oregon, showing pickup confirmation for seven iPhone 11 devices on February 27, 2020.

e. Five Best Buy receipts showing the exchange of devices purchased online.

f. Five Best Buy receipts for curbside pickup of laptop computers purchased using names other than Coconspirator A's.

g. Six Target receipts showing the purchase of Apple electronics using gift cards.

4. Coconspirator B

72. Coconspirator B was a supplier of stolen and fraudulently obtained goods involved with Wireless World. Coconspirator B was regularly observed on surveillance cameras delivering goods to Wireless World. Coconspirator B's involvement in the procurement of illicit goods and supply of them to Wireless World is summarize below.

a. Thefts in Georgia

73. From my review of investigative reports and conversations with officers of the Cobb County Police Department ("PD") in Marietta, Georgia, I learned the following:

a. On or about March 21, 2020, victim W.M. reported to the Cobb County PD that he went hiking, that his vehicle was broken into, his credit cards were stolen from his wallet and used on the same day to make purchases. The investigation showed the following purchases:

i. JP Morgan Chase Mastercard (x4556) was used at a Target store in Marietta, Georgia to purchase, among other things, twelve \$500 gift cards.

ii. Visa card (x2143) was used at a GameStop store in Marietta, Georgia to purchase a Sony PlayStation 4, wireless controllers, and three games.

iii. American Express card (x1001) was used at a Target store in Marietta, Georgia to purchase two \$500 gift cards.

74. From my review of investigative reports and conversations with officers of the Roswell PD in Roswell, Georgia, I learned the following:

a. On March 21, 2020, victim M.Y. reported that, while hiking, her vehicle had been broken into and that six credit cards and \$200 in cash were stolen. M.Y. informed the Roswell PD that her credit cards were used at a Target store in Alpharetta, Georgia. A receipt obtained by officers from Target showed a purchase of two \$500 gift cards and a few other items

using a Discover card (x2939). M.Y. confirmed this was her stolen card.

b. On or about March 21, 2020, victims J.V. and C.M. also reported that their credit cards were stolen from inside a vehicle while they were hiking. The victims reported that the credit cards were used at the same Target store.

c. Officers from Cobb County PD and Roswell PD contacted the TNIC about the use of the credit cards reported stolen on March 21, 2020. TNIC confirmed the purchases at Target, provided gift card numbers for most of the transactions, and provided surveillance video showing the two subjects who purchased or attempted to purchase the gift cards in Marietta and Alpharetta.

b. Gift Cards Redeemed in Los Angeles

75. TNIC provided Cobb County PD with additional information about the use of the gift cards purchased in Georgia, including the following:

76. On March 22 and 23, 2020, the gift cards were redeemed at approximately thirteen different Target retail stores in the Los Angeles area.

77. The gift cards were used to purchase, among other things, 21 Apple Watch Series 5 watches.

78. TNIC identified two Target Circle Loyalty Program accounts linked with the use of the gift cards. I know from discussions with representatives of Target, and other law enforcement officers that Target offers shoppers a smartphone app that allows them to load gift cards electronically onto

their smartphones, and to link those cards with Target Circle Loyalty Program accounts.

79. On April 6, 2020, TNIC identified Coconspirator B as the registrant for one of the Target Circle Loyalty Program accounts used to redeem the gift cards.

80. On or about May 6, 2020, Cobb County PD Detective Ben Jackson provided multiple surveillance photographs and receipts that he received from Target in connection with the redemption of the gift cards in Los Angeles on March 22 and 23, 2020. On March 22, 2020, Coconspirator B was seen on surveillance at the several Los Angeles area Target stores making purchases or leaving the store with a purchase. FBI Special Agent Alyson Lundby matched images from Target surveillance with California DMV photographs of Coconspirator B.

81. Target also provided data which showed that between December 2019 and April 2020, there were 190 purchases made with Coconspirator B's account using 67 gift cards which were purchased using 37 different credit cards from 10 different states.

82. Target provided investigators with the credit card numbers used to purchase gift cards used in connection with Coconspirator B's Target Circle Loyalty account. Bank records, including statements and recorded customer service calls related to approximately 20 of those credit card accounts show that almost every account was closed because customers reported fraudulent purchases and most of the fraud was from unauthorized charges at Target.

83. FBI Special Agent Lundby conducted multiple interviews with the account holders whose bank cards had been used with Coconspirator B's Target Circle Loyalty account. Many provided statements that their card had been stolen during a theft from their vehicle. For example, victim J.N. advised he was hiking in Chatsworth and his credit card disappeared from his wallet which he left in his vehicle during the hike. J.N. received notifications on his phone that his card was being used at Target without his authorization. J.N. called his credit card company to have the card replaced but did not file a police report. I reviewed bank statements from J.N.'s CapitalOne credit card which showed a purchase of \$500 at a Target in Northridge on May 3, 2020.

84. In August 2021, Target provided credit card numbers and card holder information associated with the Target gift cards which had been loaded onto Coconspirator B's account and used for purchases since January 1, 2021. Target provided credit card holder information for gift cards used with Coconspirator B's account, which revealed approximately 40 different credit cards with various cardholder names used to purchase the gift cards.

85. Some of the cardholders matched victims that the FBI had already interviewed, and some matched names of theft victims identified in police reports. For example, seven gift cards used with Coconspirator B's account were purchased on February 7, 2021 at a Target store in Brentwood, Tennessee with a credit card belonging to victim D.B. A report from the Brentwood

Tennessee Police Department detailed that victim D.B.'s credit cards were stolen while he was on a run, and D.B. began receiving alerts from his bank notifying him of purchases being made at a Target store in Brentwood, Tennessee.

c. Search of Coconspirator B's Yahoo Account

86. In 2021, pursuant to a federal search warrant, FBI Special Agent Lundby searched and seized communications from Coconspirator B's Yahoo account and discovered the following:

a. The account was created on November 6, 2010 using Coconspirator B's name.

a. On or about May 10, 2020, an email from Home Depot to Coconspirator B's Yahoo account indicated that Coconspirator B had opened a Home Depot account and included an email confirmation for a Google Nest Cam Indoor security camera placed in his Home Depot virtual cart.

87. Home Depot informed the FBI that on May 10, 2020, Coconspirator B purchased six Google Nest Cam Indoor security cameras using a Home Depot gift card. Home Depot records show that a CapitalOne visa credit card was used to purchase six \$1,000 gift cards at a Home Depot in Chino. One of those gift cards was used to make the Nest purchases.

a. CapitalOne records for the credit card used to purchase the gift cards showed the card belonged to R.L., and that there were two transactions at a Home Depot store in Chino on May 9, 2020: one for \$3,000 and one for \$3,129.96. The statement showed the two charges were reversed and the card was closed due to fraud. On June 15, 2021, FBI Special Agent Lundby

interviewed R.L. who stated, among other things, he did not make these purchases and does not know how his card was compromised.

88. Between January and October 2020, Coconspirator B's Yahoo account received approximately 30 separate invoices from Wireless World. The titles of the email for each invoice referenced a "Purchase Order from Wireless World." Each invoice was itemized showed payments for electronics such as Apple products, Dyson vacuums, Nintendo, Sony gaming systems, and Google home products.

d. Surveillance of Coconspirator B

89. On May 11, 2021, an FBI surveillance team saw Coconspirator B visit a Target store in North Hollywood. Coconspirator B purchased two Apple Watches and was seen using the Target mobile application on one of his phones. Later that same day, Coconspirator B was seen at a Target store in Burbank, where he purchased two Apple Watch Series 6 devices.

90. Coconspirator B was seen at the Wireless World warehouse on multiple occasions, including the following:

a. On November 18, 2020, Coconspirator B entered the warehouse with a small package and what appeared to be 6 Apple Watch boxes.

b. On December 10, 2020, Coconspirator B arrived in a Dodge Ram and unloaded several boxes and a Nordstrom's bag at the warehouse. The Dodge Ram was observed again at the warehouse on or about December 29, 2020.

c. On December 15, 2020, Coconspirator B unloaded 8 Nordstrom bags containing white boxes and brought them into the warehouse.

d. On July 7, 2021, Coconspirator B was seen at the warehouse in a silver Toyota Camry and loaded what appeared to be a cart full of Apple iPhones from the car into the warehouse.

e. On July 12, 2021, Coconspirator B brought white boxes and plastic bags into the warehouse.

91. On August 31, 2021, Coconspirator B was seen visiting a Target in Los Angeles and purchasing two Oculus Virtual Reality ("VR") headsets using a Target gift card and placing the items in the trunk of the Toyota Camry. The following day, Coconspirator B was seen loading unknown items into the Toyota Camry then traveled to the Wireless World warehouse and unloading what appeared to be the same Oculus VR headsets along with a box of unknown items. That evening, Coconspirator B traveled to three separate Target locations in Los Angeles to purchase electronics. The following day, Coconspirator B again traveled to the Wireless World warehouse, where he spent approximately 30 minutes.

e. December 9, 2021 Search of Coconspirator B

92. On December 9, 2021, the FBI executed a federal search warrant on Coconspirator B and his car. The following items, among others, were found in Coconspirator B's possession and in his vehicle:

a. More than 150 gift cards, including 63 Home Depot cards, 49 Visa cards, and 51 Apple cards.

- b. 15 Apple iPhones in retail packages.
- c. 21 Apple Watch series 7s in retail packages.
- d. Approximately 34 pounds of suspected marijuana.

93. Based on research conducted by Home Depot personnel using a sample of approximately twenty Home Depot gift card numbers which investigators found in Coconspirator B's possession, I learned that all the gift cards were purchased with bank cards in other people's names.

a. Two Home Depot gift cards were purchased using a bank card in the name of theft victim S.X. of Georgia. On December 22, 2021, I spoke with S.X. over the phone. S.X. informed me she believed her cards may have been stolen on December 3, 2021, while her vehicle was left unlocked at a supermarket parking lot in Atlanta, Georgia. S.X. said when she called Chase Bank to report the incident, she learned the cards had already been used to make purchases at a Home Depot store. S.X. said she did make or authorize those purchases.

b. Twelve Home Depot gift cards were purchased using three bank cards stolen from victim S.H.M. From my review of a Cobb County Police report, I learned that Detective Ben Jackson spoke with S.H.M. on December 28, 2021. S.H.M. informed him that on December 3, 2021, she had four credit cards stolen from her purse which was inside her vehicle while she went. S.H.M. stated \$11,800 in gift cards were purchased at Home Depot with her stolen cards.

c. Five Home Depot gift cards were purchased using two bank cards stolen from victim S.H.K. Based on my review of

a U.S. National Park Service report, I learned S.H.K. reported to police that on December 3, 2021, while running in a park near Marietta, Georgia, her car keys fell from her pocket. S.H.K. said when she returned to her vehicle, she noticed she no longer had her keys but saw they were on "top of the vehicle." S.H.K. said she checked her wallet (which had been left inside the vehicle) and realized her credit cards were missing. S.H.K. said she then began receiving notifications of potential fraudulent usage on her credit cards. S.H.K. stated \$5,000 had been charged at Home Depot.

5. Coconspirators C & D

94. I also identified coconspirators C and D as suppliers of stolen and fraudulently obtained goods to Wireless World, which paid for the goods with wire transfers. Coconspirators C and D were seen on surveillance cameras operated by FBI and HSI delivering electronic merchandise to the Wireless World warehouse during 2020 and 2021. Coconspirators C and D's involvement in the procurement of illicit goods and supply of them to Wireless World is summarized below.

a. *Gift Card Schemes in the Los Angeles Area*

95. Based on interviews and proffers conducted with others engaged in the purchase and use of fraudulent gift cards, including Target gift cards, Coconspirators C and D knowingly sold fraudulently obtained merchandise.

96. Beginning in at least November 2020, Coconspirator C, through his company Red Mountain Trading Inc., and coconspirator D, through his company Sirui Electronics Inc., operated at a

warehouse location in La Puente. They regularly purchased large quantities of merchandise obtained from Target, Best Buy, and other retail stores using fraudulently obtained gift card redemption codes. Coconspirators C and D, and others believed to be their runners or employees were regularly observed unloading retail electronics from these and other vendors at the La Puente warehouse.

97. During the investigation into Coconspirators C and D, the FBI identified S.C., a runner who redeemed fraudulent gift cards for electronics. On April 29, 2021, and May 21, 2021, FBI Special Agents conducted interviews with S.C. During these interviews, S.C. provided the following information:

a. S.C. was recruited to work as a runner in early 2020. S.C. was provided with fraudulently obtained Target gift card codes by a handler, and S.C. would use the codes to purchase electronics from Target stores across Southern California and elsewhere.

b. Beginning around May 2020, S.C. also began communicating with Blade Bai using the WeChat communication platform. Bai regularly provide S.C. with product lists, including the price per item that Bai was willing to pay. S.C. would then procure this merchandise using fraudulently obtained Target gift cards and sell it to Bai. In addition to merchandise, Bai would also purchase physical Target gift cards from S.C., which S.C. would obtain by redeeming fraudulently obtained digital gift card codes at self-checkout stands and

converting those codes into physical gift cards bearing new gift card numbers.

c. S.C. used at least four Target Circle accounts to upload and store the digital Target gift card codes that S.C. used to purchase merchandise. One of those accounts reflected a total of over \$500,000 in merchandise purchased between July 31, 2020 and April 19, 2021.

98. S.C. also sold merchandise to Coconspirators C and D during 2020 and 2021. To conduct these transactions, S.C. would communicate with Coconspirators C and D through WeChat and would meet them at predetermined locations. At times Coconspirator C provided S.C. with Target gift card redemption codes which S.C. would use to purchase merchandise that Coconspirator C later retrieved.

*b. Confidential Human Source Sale of
Merchandise to Coconspirator D*

99. On September 8, 2021, at the FBI's direction, a Confidential Human Source ("CHS") communicated with Coconspirator D and provided him with a list of Apple products and other items purchased using Target gift cards, with a market value of approximately \$7,968. Coconspirator D offered to pay \$5,714 for the products.

100. The CHS ultimately delivered the merchandise to an employee at Coconspirator C and D's warehouse and received payment in cash for the electronics. FBI surveillance confirmed this transaction.

101. In messaging communications between the CHS and Coconspirator D, the CHS asked about Bai, who had already been charged for similar conduct. Coconspirator D acknowledged that Bai had been caught by law enforcement but reassured the CHS it was "nothing serious."

c. Payments from Wireless World

102. From my review of Wireless World's bank records, between 2019 and 2021, I identified \$1,429,070 in wire transfers to Coconspirators C and D's bank accounts from the Wireless World Cathay Accounts.

d. Communications with Wireless World

103. On November 4, 2021, FBI and HSI executed federal search warrants at the La Puente warehouse. An iPhone 12 Pro Max belonging to Coconspirator D was seized by the FBI. I identified WhatsApp messaging threads on that device between DELAFRAZ and Coconspirators C and D, summarized in part below.

a. DELAFRAZ discussed prices at which he was willing to purchase gift cards and consumer electronics, generally well below retail price. DELAFRAZ also said that he wanted to buy gift cards that were guaranteed not to expire.

b. On July 16, 2020, DELAFRAZ had the following exchange with Coconspirator C seeking gift cards guaranteed to remain good for a week in a message thread that also included Coconspirator D.

//

//

//

Participant	Message
DELAFAZ	I need a lot of product; Best Buy card can buy too; Visa card
Coconspirator C	What price for visa And(sic) how many day warranty
DELAFAZ	1 week should be ok; 89%
Coconspirator C	Ok; Can you do 3 days so I can give you a lot of Visa card; 3 days warranty
DELAFAZ	3 day is too little
Coconspirator C	Let me ask him
DELAFAZ	Takes time. I have to check them and use and wait for order to process
Coconspirator C	Yes we have it. But they only give us 3 days warranty; But we can give you like 100k each time; Only problem is time
DELAFAZ	What about Best Buy; 3 day I'm scared; Other people give big qty 1 week
Coconspirator C	No bestbuy card

c. In the same thread DELAFRAZ warned Coconspirator C about gift cards "going bad", which I understand to be his acknowledgement of the illicit source of the funds loaded on the gift cards and the risk that they would be cancelled.

Participant	Message
Coconspirator C	Do you buy money order
DELAFAZ	No
Coconspirator C	K
DELAFAZ	Visa , bestbuy; I buy a lot of these
Coconspirator C	Ok
DELAFAZ	But be careful. The cards go bad sometimes
Coconspirator C	I know. But you said. 7 day warranty; Is right
DELAFAZ	Yes 7 day is ok
Coconspirator C	Ok

d. On August 31, 2020, DELAFRAZ had the following exchange with Coconspirator C, and approximately a week later Wireless World send a wire transfer for \$134,156 to one of Coconspirator D's bank accounts.

Participant	Message
Coconspirator C	I have visa gift card for you
DELAFAZ	\$; What price
Coconspirator C	89%
DELAFAZ	Too high
Coconspirator C	What about that
DELAFAZ	I'm buying 85
Coconspirator C	You kill me boss; 87%
DELAFAZ	I can't; Everyone sells 85; How much is it
Coconspirator C	If you can do. Everyday 100 k
DELAFAZ	87 too high
Coconspirator C	Give me best price . We see each other everyday
DELAFAZ	85 nest (sic); I can't take 100 everyday; Too much; How long is guarantee
Coconspirator C	1 week
DELAFAZ	Too little
Coconspirator C	What mean too little; You mean time
DELAFAZ	1 week too short
Coconspirator C	Let do 86.50; What about that;
DELAFAZ	I can't really; No room
Coconspirator C	85% 7 days; Is ok
DELAFAZ	Need longer than 7 days; Too much risk for small money
Coconspirator C	Ok; What about 14 days; 500 each
DELAFAZ	Let me check and see how many I can buy

e. At times, including on September 28, 2020, as shown below, DELAFRAZ requested Target gift cards at discounted prices.

Participant	Message
DELAFAZ	Have target cards?
Coconspirator C	Yes can you do 77%
DELAFAZ	Yes; Howe (sic) much you have
Coconspirator C	Give. Me like hours; How many days warranty
DELAFAZ	Same as before; 45 day ok
Coconspirator C	No; Can we do 2 weeks . Like before
DELAFAZ	Do 4 week; I will buy a lot; Just make sure they aren't scratched

f. On September 30, 2020, DELAFRAZ asked Coconspirator C for \$100,000 worth of gift cards coupled with receipts. I recognize from my investigation of Bai that money mules would provide receipts to accompany gift cards laundered through returns to prove that the value was loaded onto the

cards. As noted above, loading returns from purchases using fraud-derived gift cards onto new physical cards is one method of laundering the proceeds of fraud and making it more difficult to trace the provenance funds on the new card.

Participant	Message
DELAFAZ	Bring me 100k
Coconspirator C	What price for me; 80%
DELAFAZ	Ok; 80
Coconspirator C	How many days warranty
DELAFAZ	30
Coconspirator C	30 days
DELAFAZ	Not scratched; With all receipts

104. In a separate WhatsApp thread including Coconspirators C and D, DELAFRAZ, and DANESHGAR, on June 30, 2021, after Coconspirator C sent an image of a smartwatch listed for sale on Best Buy for \$199.99, and asked how much Wireless World would pay, DANESHGAR replied "\$110."

105. Between August and November 2021, Coconspirators C and D were seen during video and physical surveillance delivering electronics, including Nintendo and Oculus products, to the Wireless World warehouse. The Wireless World van was also seen transporting goods from the La Puente warehouse to the Wireless World warehouse.

e. Communications with Coconspirator A

106. During my search of Coconspirator A's iPhone pursuant to the warrant discussed above, I located a series of communications on the messaging application WeChat with an individual using the moniker "Water Aqua," who I later learned was Coconspirator C. They primarily discussed transactions involving gift cards, and it was clear from their communications

that they understood the gift cards to be the proceeds of fraud. Some examples of relevant communications are summarized below.

a. In a discussion thread on June 3, 2019, Coconspirator A asked for Target gift cards and discussed pricing using terms like "75%" and "6.8," and specifically asking Coconspirator C for "2-hour cards" (i.e. cards that are guaranteed to be valid for at least 2 hours).

b. Later that day, Coconspirator A said that they wanted to purchase \$20,000 of gift cards from Coconspirator C daily. Coconspirator C noted "I am serious too. But I don't like touching that stuff," and "I don't want get any problem with cops."

c. On June 14, 2019, after discussing merchandise for several messages, Coconspirator C told Coconspirator A that they would provide Target gift cards at or around the rates they had previously discussed. Coconspirator A said that he wanted \$20,000 in gift cards daily and would pay \$13,000 cash nightly for the gift cards.

d. On August 18, 2019, Coconspirator C sent a screen shot of an NBC News article titled "San Diego Thieves Spend Target Gift Cards Loaded with Texas Woman's Life Savings." Coconspirator A responded "That is more than 1 month old. I saw that."

f. Search of Coconspirators C & D's Warehouse

107. On November 4, 2021, FBI and HSI executed search warrants at Coconspirator C and D's warehouse in La Puente. During the search the following electronics and gift cards,

among others, were seized: 239 Apple iPad Pros, 66 Oculus devices, 57 Nintendo Switch consoles, 1,695 Nintendo Switch games, 39 Xbox consoles, assorted gift cards, and Target retail store receipts.

108. On November 5, 2021, the day after the search in La Puente, on video surveillance, I saw Coconspirators C and D arrive at the Wireless World warehouse in a Toyota SUV. They got out of the vehicle and entered the warehouse. Shortly thereafter, I saw DANESHGAR and DELAFRAZ exit the warehouse alone and engage in conversation outside. Approximately one hour later, I saw DANESHGAR, DELAFRAZ, and Coconspirators C and D outside the warehouse. The four appeared to be engaged in conversation while smoking cigarettes for several minutes before Coconspirators C and D departed.

6. DELAFAZ and DANESHGAR Directly Purchased Electronics Using Gift Cards Funded with Fraud

109. In addition to receiving goods from the suppliers identified above, among others, at times DELAFRAZ and DANESHGAR purchased electronics using stolen credit cards and had those electronics delivered directly to the Wireless World warehouse or to other addresses associated with Wireless World.

a. *Nashville, Tennessee Credit Card Fraud*

110. In 2019, DELAFRAZ and DANESHGAR placed orders for electronics with retailers in Nashville, Tennessee using false names and stolen credit card information. They arranged for the shipments to be picked up by couriers and transported to FedEx shipping locations. DELAFRAZ and DANESHGAR then arranged for

FedEx to ship the parcels to addresses in the Los Angeles area. The details of those fraudulent purchases are set forth below.

111. In February and April 2019, Metro Nashville Police Department ("MPD") detectives investigated two incidents of credit card fraud connected to DELAFRAZ and DANESHGAR. Based on conversations with MPD detectives, and a review of investigative reports, I learned the following:

a. On February 5, 2019, a Nashville electronics wholesaler ("Victim Company 1") received an order over the phone for 34 Nest thermostats for \$9,710. The buyer said that his name was "Stephen Kane," and provided a Citibank card (x3913).

b. On February 8, 2019, a third-party courier service in Nashville picked up the purchase and transported it to a FedEx facility. Information received from FedEx showed that someone using the name Stephen Kane contacted FedEx to arrange for shipping to an address in Orlando, Florida. The FedEx store manager informed law enforcement that Kane had tried approximately seven different credit card numbers to pay the shipment fee.

c. According to the FedEx store manager, Kane then changed the destination from the address in Orlando, Florida to Postal Annex+, 321 N. Pass Ave., Unit #93, Burbank, California, where the goods were delivered on February 14, 2019.

d. Postal Annex + in Burbank, later provided information to law enforcement showing that at the time of the delivery, Unit #93 was rented to DELAFRAZ. I confirmed from public database searches that this address was also associated

with Virtual Wireless, one of the business entities owned by DELAFRAZ and DANESHGAR.

e. On February 13, 2014, Victim Company 1 was notified by Citibank that the purchase of Nest thermostats discussed above had been disputed by the cardholder. Citibank indicated that the cardholder, M.I, a resident of Michigan, reported the card lost or stolen on February 5, 2019.

f. On February 26, 2019, Stephen Kane again called Victim Company 1 and attempted to purchase 90 Nest thermostats for \$25,703.10 using a different Citibank card. The transaction was declined by Citibank. Later investigation showed that the holder of the Citibank card was E.B. of Wisconsin.

g. On April 3, 2019, a second Nashville electronics wholesaler ("Victim Company 2") received a telephone order from "Nathan Hoskins" for 42 Nest thermostats for \$9,550. Payment was made using a Citibank card, and the thermostats were picked up by a third-party courier who transported them to a FedEx location for further shipment.

h. On April 9, 2019, Victim Company 2 received additional orders from Hoskins. He purchased 48 Nest IQ cameras for \$16,518.60 using a Citibank card (x2721), and 48 Next thermostats for \$12,454.50 using a Citibank (x0027). These payments were both identified by Citibank as fraudulent uses of cards belonging to customers in Ohio and Florida, respectively. MPD was alerted, and instead of sending the products, they shipped dummy boxes that did not contain the Nest devices.

i. A third-party courier picked up the dummy boxes from Victim Company 2 and transported them to a FedEx store. Hoskins contacted the third-party courier and provided a shipment address. On April 12, 2019, the dummy boxes were shipped to Post Net, 9909 Topanga Canyon Blvd, Unit #155, Chatsworth, CA 91311.

j. The MPD report listed the FedEx shipment of dummy boxes was assigned tracking number 774948305607. FedEx records showed that shipment was paid using a FedEx account belonging to Wireless World.

k. Postal Net in Chatsworth later provided information to law enforcement showing that at the time of the delivery, Unit #155 was rented to DANESHGAR. On July 18, 2019, I interviewed the owner of the Postal Net store and showed him a photograph of DANESHGAR's California driver's license photo. The owner confirmed that DANESHGAR was the renter of Unit #155. At that time, Wireless World operated from a warehouse roughly half a mile from the Postal Net store.

b. Home Depot Orders Using Stolen Credit Cards

112. From my review of a Dupage County, Illinois Sheriff's Office ("DCSO") report dated June 2021, I learned the following:

a. Theft victim L.M. of Illinois reported that several credit cards belonging to her had been stolen in June 2021. L.M.'s credit cards were used at a Home Depot store in Naperville, Illinois on June 11, 2021, to buy seventeen \$500 Home Depot gift cards. Home Depot records show that the gift cards were used on June 16, 2021 to purchase 400 Amazon Fire

Sticks for \$15,996 in eight online orders. Those orders were made using an email address known to me to be used by DELAFRAZ.

b. Home Depot identified the orders had been placed using Charter Communications IP address 75.83.40.144. Charter Communications records showed that this IP address belonged to the Wireless World warehouse and the account listed DANESHGAR's phone number and his email address.

c. Home Depot further investigated the Fire Stick orders made from the Wireless World warehouse, and provided records to HSI showing approximately 35 gift cards were used to fund the purchase. Research into the additional cards revealed the following:

i. Three \$500 Home Depot gift cards were purchased with a Chase Bank card (x1270). Chase Bank informed HSI that the gift cards were purchased in fraudulent transactions at a Home Depot store in Carol Stream, Illinois on June 11, 2021.

ii. Four \$500 Home Depot gift cards were purchased with a Chase Bank card (x7928). Chase Bank informed HSI that the gift cards were purchased in fraudulent transactions at a Home Depot store in Carol Stream, Illinois on June 11, 2021.

iii. Seven \$500 Home Depot gift cards were purchased with a TD Bank card (x1618). TD Bank records show that the gift cards were purchased in fraudulent transactions at Home Depot stores in Oakbrook Terrace and Downers Grove, Illinois on June 11, 2021. The cardholder, B.A., in a recorded

call, said the card had been used for unauthorized charges at Home Depot after it was either lost or stolen.

113. From a review of a Maryland-National Capitol Park Police ("MNCPP") report dated in July 2021, I learned the following:

a. On July 24, 2021, theft victim D.F. of Maryland reported to the MNCPP that she had six credit cards stolen from her car while parked at a playground. D.F. reported that after returning to her vehicle, she received notifications some of her credit cards were used fraudulently at a nearby Home Depot store in Gaithersburg, Maryland.

b. MNCPP investigation revealed that multiple \$500 Home Depot gift cards were purchased using D.F.'s credit cards shortly after they were stolen.

c. Home Depot personnel identified that those gift cards were used, in part, to fund seven online purchase orders for 105 Nest cameras and 10 Roku Streaming Players on July 28, 2021, for a total of \$13,898.85. The devices were delivered to the Wireless World warehouse.

d. Home Depot indicated that 29 gift cards were used to fund this order. Twenty of those cards were purchased using victim D.F.'s credit cards.

i. Five of the additional gift cards used were purchased using a Discover credit card (x4750) belonging to C.J.W., also of Maryland, who disputed the transactions. In a recorded statement, C.J.W. informed Discover Card that while she

was at a picnic, her credit cards were stolen from her car and then used fraudulently.

ii. One of the additional gift cards used was purchased using a Chase Bank card (x4667). Chase Bank provided documentation to HSI showing that the card was fraudulently used at a Home Depot store in Frederick, Maryland on July 24, 2021.

c. Best Buy Online Orders Using Stolen Credit Cards

114. Based on my review of an Irvine Police Department report dated in March 2022, I learned the following:

a. On March 19, 2022, theft victim K.H.D. reported having an American Express card (x2017) stolen from her unattended locked vehicle in Irvine. Police noted obvious damage to the handle and keyhole of K.H.D.'s vehicle on the driver side door, consistent with forced entry. K.H.D. said she also received notifications on her cell phone of likely fraudulent transactions on her credit cards.

b. Best Buy records show that K.H.D.'s American Express card was used at a Best Buy store in Tustin on March 19, 2022, to purchase a \$250 Best Buy gift card. That gift card, in turn, was used as partial payment in an online order dated March 21, 2022, for five PlayStation gaming consoles, at a total cost of \$1,749.95.

c. Best Buy order details show the purchaser as DELAFRAZ under a reseller account in the name of Wireless World and the shipping address as the Wireless World warehouse.

d. In total, seven different Best Buy gift cards were used to fund this order. Best Buy records showed that at least one more of the gift cards used was also derived from a theft victim. That card was purchase using victim M.W.'s American Express card on March 5, 2022 at a Best Buy in Sherman Oaks. From a Glendale Police Department report, I learned that that M.W. reported that her wallet containing her credit cards had been stolen from her purse while shopping at a nearby grocery store, and that she received notices from her financial institutions that transactions were conducted using her cards in Sherman Oaks shortly after the theft.

115. Based on my review of a San Luis Obispo Police report dated May 2022, I learned the following:

a. On May 6, 2022, theft victim E.C. reported to police that his wallet had been stolen while he was at Pismo Beach and his credit cards had been used fraudulently.

b. E.C. reported his Chase Bank card had been used at a Best Buy store in San Luis Obispo for a transaction totaling \$2,543.74.

i. Best Buy provided records showing E.C.'s Chase Bank card had been used to purchase four \$500 Best Buy gift cards and a Dyson electronic product.

c. Best Buy personnel determined that one of the gift cards, in turn, was used on May 10, 2022, in an order for two Oculus Quest 2 VR devices for \$498. The online order listed DELAFRAZ with the Wireless World warehouse as the shipping address.

d. *Wireless World Purchases Identified by Home Depot*

116. Home Depot provided additional records to HSI about orders of electronic products made by Wireless World during May and June 2021 which also involved fraud and theft, including the following.

a. A May 26, 2021, online order for 20 Nest thermostats totaling \$3,980. This order was made using DELAFRAZ's email address and P.O. Box mailing address, with a delivery address of the Wireless World warehouse. The order was placed using the name of a known Wireless World associate who was often observed at the Wireless World warehouse

i. The order was paid for using seven \$500 and one \$480 Home Depot gift cards. Those cards, in turn, were purchased using three different bank cards.

ii. Two of the \$500 gift cards were paid for with victim S.J. of California's SchoolsFirst Federal Credit Union ("FCU") card (x1634). SchoolsFirst FCU records showed that the card had been flagged for fraud on May 15, 2021, but that a transaction totaling \$1,628.22 was successfully processed at a Home Depot store in Mission Viejo. S.J. reported on May 16, 2021, that her credit card had recently been stolen from her unattended vehicle and that she did not conduct or authorize the transactions.

117. A June 2, 2021, online order for 30 Chromecast streaming media players totaling \$926.40. This order was made using DELAFRAZ's email address and P.O. Box mailing address,

with a delivery address of the Wireless World warehouse. The order was made using the name of the same Wireless World associate as above.

i. The order was paid for using seven Home Depot gift cards. Those cards, in turn, were purchased using five different bank cards.

ii. Three of the gift cards were paid for using victim J.E.S. of Utah's America First FCU bank card (x8289). America First FCU records showed that these transactions were deemed fraudulent due to the cards being reported stolen or lost by J.E.S.

iii. One of the gift cards was paid for using victim H.T.C. of Alabama's American Express card (x2001). American Express reported to HSI they had determined H.T.C.'s card had been used fraudulently to make purchases at a Home Depot store in Birmingham, Alabama on May 24, 2021.

iv. One of the gift cards was paid for using victim J.M.K. of Virginia's CapitalOne Bank card (x2512). CapitalOne Bank reported to HSI that the transaction at the Home Depot was fraudulent.

v. Another of the gift cards was paid for using a Chase Bank card (x7709). Chase Bank provide records showing that card was used in a fraudulent transaction at a Home Depot store in Alexandria, Virginia on May 17, 2021 to buy the gift card.

e. *Wireless World Purchases Identified by Best Buy*

118. Best Buy provided additional records to HSI about orders of electronic products made by Wireless World from 2019 through early 2021 which also involved fraud and theft.

a. During this period, Best Buy identified approximately 37 online orders by Wireless World involving payment with gift cards. In total, about 237 different Best Buy gift cards were used by Wireless World to make purchases of electronics. The records show that Wireless World purchased consumer electronics, including Apple products, Google Chromecasts, Nest cameras, Ring doorbells, gaming consoles (Nintendo, PlayStation, Xbox) and HP laptops.

b. The orders included identifying information for DANESHGAR, DELAFRAZ and Wireless World.

119. Further investigation into a sample of the Best Buy gift cards used by Wireless World revealed the following connections to theft and or fraud.

120. Two \$500 Best Buy gift cards were used to purchase six Apple AirPods for \$959.94 on February 22, 2019.

a. Both gift cards were purchased at a Best Buy in Fairfield on February 15, 2019, using victim J.M.'s American Express credit card (x1032).

b. On March 2, 2022, I spoke with J.M. over the phone. J.M. said her credit cards were stolen from her parked car in Vallejo on February 15, 2019. J.M. said she reported the theft and fraud to the Vallejo Police Department.

121. Four \$500 Best Buy gift cards were used, in part, to purchase three Whirlpool refrigerators for \$1,887.47 on March 16 and March 17, 2020.

a. Each order listed DELAFRAZ's name and email, and DANESHGAR's phone number.

b. Best Buy records show the products were successfully picked up at a store in Los Angeles.

c. The four gift cards were purchased at a Best Buy in Santa Clarita on February 25, 2020, using victim E.M.'s Visa bank card (x6551).

i. Based on the review of a Ventura County Sheriff's Office report I learned E.M. had reported to local police she was victimized by an identity theft scheme beginning on February 25, 2020, and that \$23,000 transactions were made on the bank account tied to the x6551 card.

ii. E.M. learned through bank personnel that someone accessed her account and ordered a new debit card which was delivered by courier service on February 14, 2020 (and not received by E.M.).

d. An additional gift card used for the Whirlpool refrigerator purchase was identified by Best Buy. That gift card was funded with \$523.49 from the return of an Apple MacBook Pro on February 26, 2020, in Burbank.

i. The MacBook Pro had been purchased the day prior at a Best Buy store in Santa Clarita, in another fraudulent transaction using the x6551 card.

122. Two \$500 Best Buy gift cards were used, in part, to purchase four Apple iPad Pro 11-inch (128GB) models, one iPad Pro 11-inch (256GB) and Nintendo Switch 32GB Lite for \$4,299.94 on August 11, 2020.

a. The order was made in Wireless World's name and used the Wireless World warehouse as the delivery address.

b. One of the gift cards was purchased at a Best Buy in Irvine using victim S.P.'s Visa card (x0412) on July 19, 2020. Union Bank records show that this was a fraudulent transaction using a lost or stolen card.

c. The other gift card was funded on July 30, 2020, by the return of an Apple MacBook Pro at a Best Buy in Northridge. The MacBook Pro, in turn was purchased the prior day using three \$500 gift cards at a Best Buy in Canoga Park.

i. One of the gift cards used to purchase the MacBook Pro was purchased using victim J.I.'s CapitalOne bank card (x3965) at a Best Buy in Soquel Canyon on July 23, 2020. CapitalOne records show that this was a fraudulent transaction with a stolen card.

ii. The other two gift cards used to purchase the MacBook Pro were purchased using victim W.T.S.'s Travis Credit Union bank card (x4121) at a Best Buy in Colima on July 24, 2023. Travis Credit Union records show that this was a fraudulent transaction with a stolen card.

123. A \$500 Best Buy gift card was used to pay for two iPad Pro 11-inch (256GB) devices on August 27, 2020. The devices were shipped to the Wireless World warehouse.

a. The gift card was purchased using victim L.Z.'s JP Morgan Chase Bank card (x8724) at a Best Buy in Irvine on August 16, 2020. JP Morgan Chase Bank records show that this was a fraudulent transaction.

124. A Best Buy gift card was used, in part, to purchase four Whirlpool refrigerators for \$2,349.96 on March 17, 2020.

a. The shipping and billing information listed DELAFRAZ's name and P.O. box address and DANESHGAR's phone number.

b. The gift card was funded with \$1,818.50 on December 21, 2019 from the return of a MacBook Pro at a Best Buy in Sherman Oaks. The MacBook Pro, in turn was purchased the prior day using Navy Federal Credit Union ("NFCU") debit card (x1596) at a Best Buy in Corona.

i. NFCU records show that the x1596 card was opened fraudulently using victim R.F.'s name and that the Best Buy purchase was fraudulent.

ii. NFCU stated that R.F. reported being a victim of identity theft on December 18, 2019, the same day the account was opened telephonically.

*f. Wireless World Purchases from Best Buy
Identified Through UPS Records*

125. United Parcel Service records show over 700 shipments from Best Buy to the Wireless World warehouse in 2021. From research conducted by Best Buy personnel on a sample of those shipments, I learned that all of them corresponded to online orders for consumer electronics, including Apple iPads, AirPods,

and Nintendo devices. I also learned that the recipient was DELAFRAZ, and that in each instance where I was able to trace the funds used for the purchase, they originated with theft or fraud victims, as illustrated below.

126. A March 4, 2021, delivery contained three Apple MacBook Pro (512GB) devices purchased from Best Buy for a total of \$4,211.97. This purchase was funded in part with a Best Buy gift card that was purchased at a Best Buy in Santa Rosa on January 10, 2021. Chase Bank records show that this purchase was fraudulent.

127. An April 8, 2021, delivery contained twelve Dyson Corrale hair straighteners purchased from Best Buy for a total of \$4,799.88. This purchase was funded in part with a Best Buy gift card purchased in San Carlos with Chase Bank card (x0410) on March 13, 2021. Chase Bank records show that this purchase was fraudulent.

128. A September 1, 2021, delivery contained twenty-two Oculus Quest 2 VR headsets for a total of \$6,578.00. This purchase was funded in part with a Best Buy gift card purchased at a Best Buy in Marina with victim M.W.'s Chase Bank card (x0758) on August 13, 2021. Chase Bank records show that this purchase was fraudulent.

129. A December 8, 2021, delivery contained seventeen Amazon Echo Dot devices for a total of \$534.83. This purchase was funded in part with a Best Buy gift card purchased in November 2021 using victim J.J.'s American Express card (x1005). American Express records show that the x1005 card was used on

Best Buy's website to make \$1,537.80 in fraudulent purchases on November 20 and 30, 2021.

C. Wireless World Exports, Sales & Related Payments

130. From my participation in this investigation, I have learned that DELAFRAZ and DANESHGAR primarily sold and shipped high value electronics out of the United States. However, at times, and to a far lesser extent, they also sold electronics on various online vending platforms, including platforms operated by Walmart. Wireless World also sold and or provided merchandise to domestic partner businesses.

131. Based on customs and shipping records, I learned that Wireless World exported merchandise to international recipients. From inspections of those shipments, I know that they included merchandise that was the proceeds of criminal activity. In total, based on my review of U.S. Customs filings, Wireless World exported over \$611,000,000 in reported value in merchandise to destinations largely in the United Arab Emirates, Paraguay, Israel, Czech Republic, Poland, and Singapore between January 2019 and September 2025. The merchandise exported has almost exclusively been reported and observed during inspections as consumer electronics, including laptop computers, smart watches, streaming devices, iPads, game consoles, AirTags, AirPods, iPhones, MacBooks, and other high value electronics. The merchandise I've observed has appeared to have been in new or unused condition in manufacturer or distributor packaging. Wireless World does not appear to export used merchandise. The

identified recipients of those exports made payments to Wireless World.

132. During this investigation, law enforcement has conducted multiple inspections of export shipments made by Wireless World. In each instance, law enforcement collected serial numbers from electronics contained in the shipment and conducted further investigation into the sources and origins of those devices.

a. July 30, 2019 Inspection

133. On July 30, 2019, Customs and Border Patrol ("CBP") agents inspected a Wireless World shipment at the FedEx shipping hub in Memphis, Tennessee. The shipment consisted of a total of 10 boxes destined for a consignee in the United Arab Emirates ("Dubai Company #1"). The manifest for the export identified the contents as 208 "Tablets" and 24 "Apple Watches" with a declared value of \$114,961.

134. CBP inspected nine of ten boxes that made up the shipment and recorded the serial numbers for 18 of the items in the shipment, which included Apple iPads and Apple Watches (consistent with the manifest). Apple records, in turn showed that most of the devices were sold to Target. TNIC records showed that numerous of the exported devices were purchased with gift cards that were procured through fraud or that were the subject of customer complaints.

135. Based on information received from Target, I was able to identify the ultimate funding sources for several devices

contained in the July 30, 2019 shipment, including the devices discussed below:

a. An Apple iPad Air 64GB was purchased using funds originating from victims K.G. and H.M., both of Georgia. Victim K.G. reported that she purchased \$4,000 in Target gift cards and provided the numbers over the phone to scammers posing as representatives of the Social Security Administration. Victim H.M. reported providing gift cards to a scammer who purportedly needed them as payment for flight reservations that H.M. was attempting to make.

b. An Apple iPad Air 256GB was purchased using funds originating from victims P.S. of Wisconsin and M.S.M. of Texas. Victim P.S. reported that he purchased \$16,500 in Target and Walmart gift cards and provided the numbers over the phone to scammers posing as representatives of the Social Security Administration. Victim M.S.M. reported a similar fraud for \$16,000 of Target and Walmart gift cards.

c. An Apple iPad Pro 11in was purchased using funds originating from gift cards purchased by victims M.B. of Virginia and N.T. of New Jersey. Victim M.B. reported that he purchased \$16,000 in Target gift cards and provided the numbers over the phone to scammers posing as representatives of the Social Security Administration. TNIC indicated that all of the cards were redeemed in California to purchase high value electronics. Victim N.T. reported that, in response to a caller purporting to be from the Social Security Administration, she

purchased a \$999 Target gift card and a \$500 Target gift card and provided the numbers and codes to the caller.

d. An Apple iPad Pro 11in was purchased using funds originating from gift cards purchased by victim J.G. of Virginia. Victim J.G. reported that, in response to a caller purporting to be from the Social Security Administration, she purchased \$6,300 worth of Target gift cards and provided the numbers and codes to the caller.

b. August 20, 2019 Inspection

136. On August 20, 2019, together with another HSI Special Agent, I conducted an inspection of a shipment from Wireless World's warehouse to Dubai at a FedEx site near the Van Nuys airport. The manifest for the export identified the contents as 280 "Tablets" and 216 "Smart Watches" with a declared value of \$187,631.

137. I inspected three of thirteen boxes that made up the shipment and recorded the serial numbers for 67 of the items in the shipment, which included Apple iPads and Apple Watches (consistent with the manifest). Apple records showed that most of the devices were sold to Target. TNIC records, in turn showed that numerous of the exported devices were purchased with gift cards that were procured through fraud or that were the subject of customer complaints.

138. Based on information received from Target, I was able to identify the ultimate funding sources for several devices contained in the August 20, 2019 shipment, including the devices discussed below. Target identified multiple additional devices

whose purchases were associated with customer fraud complaints, but did not provide identifying information for the victims:

a. An Apple iPad Air 64GB was purchased using two Target gift cards. Victim J.R. of Arizona reported that those gift cards were purchased by her parents and provided over the phone to scammers posing as representatives of the Social Security Administration.

b. An Apple iPad Pro 256GB was purchased using three Target gift cards. Victim S.G. of Washington D.C. reported that he purchased those gift cards and provided them over the phone to scammers posing as representatives of the Social Security Administration.

c. An Apple iPad Pro 256GB was purchased using two Target gift cards, which were in turn loaded with funds from a third Target gift card. In an interview, Victim M.L. told me that he was fooled by scammers who called him claiming to be representatives of the Social Security Administration. Victim M.L. said that he provided three Target gift card numbers for cards valued at \$1,000 each to the scammers before realizing that he had been fooled. One of the cards provided to scammers by M.L. was used to fund the cards used to purchase the iPad Pro.

d. An Apple iPad Air 64GB was purchased using a Target gift card. Victim T.L. reported that numerous Target gift cards, including the card used to purchase the iPad were provided by him to scammers on the phone pretending to be representatives of the Social Security Administration.

e. An Apple iPad Pro 256GB was purchased using, in part, two gift cards that victim E.M. reported that she provided to scammers who called her claiming that there were problems with her bank account.

c. September 10, 2019 Inspection

139. On September 10, 2019, together with another HSI Special Agent, I conducted an inspection of a shipment from Wireless World's warehouse to Dubai at a FedEx site near the Van Nuys airport. The manifest for the export identified the contents as 246 "Tablets," 44 "Smart Watches," and 9 "Smart Pencils" with a declared value of \$119,831.

140. I inspected five of twelve boxes that made up the shipment and recorded the serial numbers for 173 of the items in the shipment, which included Apple iPads, Apple Watches, and Apple Pencils (consistent with the manifest). Apple records showed that most of the devices were sold to Target. TNIC records, in turn showed that numerous of the exported devices were purchased with gift cards that were procured through fraud or that were the subject of customer complaints. Information received from TNIC showed that the cards used to purchase many of the items were cards that contained funds that had been re-loaded onto gift cards from returned items that had, in turn, been purchasing using Target gift cards that were the proceeds of fraud.

141. Based on information received from Target, I was able to identify the ultimate funding sources for several devices

contained in the September 10, 2019 shipment, including the eighteen devices discussed below:

a. An Apple iPad Air 64GB was purchased, in part, using a gift card that victim A.A. provided to scammers over the phone. During an interview, A.A. informed me that she received a call from a scammer claiming that a rental vehicle in her name had been located near the Mexican border in connection with drug trafficking. She was told that she had to go through a payment process to avoid arrest and was instructed to purchase gift cards and provide them to the scammer over the phone.

b. An iPad Air 64GB was purchased using a Target gift card that victim I.H. of Texas reported providing to scammers on the phone pretending to be representatives of the Social Security Administration.

c. An iPad Air 64GB was purchased using three Target gift cards that victim A.B. of Washington reported providing to scammers on the phone pretending to be representatives of her bank. Victim A.B. reported providing \$11,000 in gift cards to the scammers.

d. An iPad Air 64GB was purchased using a Target gift card that victim N.S. of Arizona reported providing to scammers on the phone pretending to be representatives of the Social Security Administration. Victim N.S. reported providing \$7,993 in gift cards to the scammers.

e. An iPad Mini 64GB was purchased using a Target gift card that victim K.B. of Pennsylvania, reported providing

in response to a computer technical support scam. Victim K.B. reported providing \$5,200 in gift cards to the scammers.

f. An iPad Mini 64GB was purchased using Target gift card that victim S.M. of California reported providing to scammers on the phone pretending to be representatives of the Social Security Administration. Victim S.M. reported providing \$16,500 in gift cards to the scammers.

g. An Apple Watch series 4 and iPad Air 64GB were purchased using a Target gift card that victim P.F. of California reported providing in response to a computer technical support scam. Victim K.B. reported providing \$20,500 in gift cards to the scammers.

h. An Apple iPad Air 64GB was purchased using a Target gift card that victim G.N. of Georgia, according to his son, provided to scammers in response to a phone call.

i. An Apple iPad Mini 64GB was purchased with a Target gift card that victim L.M. of Ohio reported providing to scammers posing as government officials.

j. An Apple iPad Mini 64GB was purchased with a Target gift card that victim M.S. of New York reported providing to scammers posing as government officials.

k. An Apple iPad Mini 64GB and an Apple iPad Air 64GB were purchased using three Target gift cards that victim S.D. of Montana reported providing to a scammer.

l. Two Apple Pencils were purchased using a Target gift card that victim M.M. of Colorado reported providing in response to a computer technical support scam.

m. An Apple iPad Mini 64GB was purchased using two Target gift cards that victim D.B. of Florida reported providing to scammers pretending to be airline representatives.

n. An Apple iPad Air 64GB, an Apple iPad Air 64GB, an Apple iPad Pro 11 256GB, an Apple iPad Air 64GB, an Apple iPad Air 64GB, an Apple iPad Air 64GB, an Apple iPad Mini 64GB, and an Apple iPad Pro 11 256GB were purchases using eight Target gift cards that victim R.G. of Virginia reported providing to tech support scammers.

o. An Apple iPad Mini 64GB, an Apple iPad Mini 64GB, and an Apple Watch series 4 purchased with a Target gift card that victim R.L. of California reported providing to a scammer who contacted her about an issue with her social security number.

p. An Apple iPad Air 64GB purchased with a Target gift card that victim M.D. reported providing to a scammer claiming to work for the Federal Trade Commission.

d. May 28, 2020 Inspection

142. On May 28, 2020, together with another HSI Special Agent, I conducted an inspection of a shipment from Wireless World's warehouse to Dubai at a FedEx site near the Van Nuys airport. The manifest for the export identified the contents as 81 "Tablets" and 11 "Smart Watches" with a declared value of \$54,170.

143. Based on information received from Target, I was able to identify the ultimate funding sources for several devices contained in the May 28, 2020 shipment, including the three

devices discussed below. Based on communications with Target, I understand at this time that Target was not recording device serial numbers for online purchases, and thus was unable to provide details for many devices based on the serial number:

a. An Apple iPad mini 64GB purchased using a credit card reported stolen from victim K.C. of California.

b. An Apple iPad mini 64GB purchased using a credit card reported stolen from victim C.S. of Oregon on May 18, 2020.

c. An Apple iPad mini 64GB purchased using a credit card reported stolen from J.J. of California.

e. July 22, 2022 Inspection

144. On July 22, 2022, CBP agents inspected a Wireless World shipment at the FedEx shipping hub in Memphis, Tennessee. The inspection revealed that the shipment included many Apple products being sent to three companies in Dubai (including Dubai Company #1 and Dubai Company #2, discussed below). The total combined value of these exports was \$484,677. Serial numbers from those Apple products showed that they were originally sold to retailers including Amazon, T-Mobile, Walmart, Costco, and Best Buy. Apple records showed that twenty-one of the fifty-seven serial numbers recorded were items sold through Amazon.

f. August 6, 2024 Export

145. On August 6, 2024, Wireless World exported merchandise described in customs documents as "TABLETS/LAPTOPS, SMART WATCH, SMART PENCIL/KEYBOARDS, HEADPHONES" to a consignee ("Dubai Company #2") with an address in the Dubai Airport Free Zone.

The total value of these shipments to Dubai Company #2 on this date was \$572,138.

146. On August 7, 2024, Dubai Company #2 paid \$607,595 by bank wire to Wireless World Cathay Account #1.

147. On August 8, 2024, Wireless World exported merchandise described in customs documents as "TABLETS/LAPTOPS, SMART WATCH, HEADPHONES" to Dubai Company #1 with an address in the Dubai Airport Free Zone. The total value of the shipment to Dubai Company #1 was \$334,286.

148. On August 9, 2024, Dubai Company #1 paid \$297,567 by bank wire to Wireless World Cathay Account #2. From a review of Wireless World financial records, I know that between November 2019 and July 2022 Dubai Company #1 paid over \$19.6 million to Wireless World Cathay Account #1 and between October 2022 and August 2024, paid over \$55.5 million to Wireless World Cathay Account #2.

g. August 19, 2025 Inspection

149. On August 19, 2025, HSI conducted surveillance at Wireless World's MaxOutDeals warehouse in Delaware. During the afternoon hours, a FedEx Express truck was observed arriving at the location and departing the warehouse after seemingly receiving a shipment. HSI Special Agents followed the FedEx Express truck which ultimately arrived at a FedEx facility in the Linwood/Marcus Hook, Pennsylvania, area where they conducted a border search. HSI observed the shipment sealed with packing tape bearing the Wireless World name. Numerous Apple AirPods 4, some of which had "P.C. Richard" retail stickers affixed to the

boxes, as well as iPads and Dell laptops were also seen. Based on internet research, I learned that P.C. Richard is a name used by P.C. Richard & Son, a chain of electronics retail stores based in New York.

150. HSI Special Agents recorded 45 Apple serial numbers during the inspection. Apple records for 20 of the items show that 17 were sold by Amazon, while the other three were sold by Walmart, Target, and Costco. CBP records show that these shipments, made under Wireless World's d.b.a. 2D Distribution from the MaxOutDeals Delaware warehouse were worth \$509,284. The recipient for the shipment was Dubai Company #1.

i. August 22, 2025 Inspection

151. On August 19, 2025, while HSI conducted surveillance at Wireless World's MaxOutDeals warehouse, a shipment was observed departing the warehouse by FedEx Freight truck. HSI Special Agents conducted mobile surveillance of the FedEx Freight truck and observed the truck travel directly to a FedEx facility in North East, Maryland. At the facility, HSI was permitted to view the outside of the palletized shipment which displayed a FedEx label bearing tracking number 883698087624 and the address of a third-party exporting service ("Shipper-1") in the Miami, Florida where it was being sent. The sender address was the MaxOutDeals warehouse.

152. On August 22, 2025, I inspected the shipment bearing FedEx tracking number 883698087624 at Shipper-1's customs bonded warehouse in the Miami, Florida area. FedEx records show this

shipment traveled from Maryland to Shipper-1 in Florida and was bound for export to a recipient in Paraguay.

153. During my inspection, I saw Apple iPads and Dell laptop computers. Several of the Apple products had labels which I recognized as Amazon order numbers. I recorded approximately 25 Apple iPad serial numbers. Shipper-1 provided me the documentation for the export, including an invoice to the buyer in Paraguay valuing the shipment at \$56,308. The invoice showed the provider as Wireless World and included the Wireless World warehouse address in Van Nuys, along with DELAFRAZ's email address. The items on the invoice were being sold for less than or near the retail price for those good on Amazon. For example, one product listed, "MW2U3WA; Apple-MacBook Pro 14-inch Apple M4 chip Built for Apple Intelligence-16GB Memory-512GB" was being sold for \$1,314, as compared to the sale price of \$1,426 on Amazon as of September 7, 2025.

D. Fraudulent Economic Impact Disaster Loan

154. In addition to the money laundering discussed above, DELAFRAZ and DANESHGAR also fraudulently applied for and received a Small Business Administration ("SBA") loan and ultimately commingled the \$1.325 million received from the SBA with the proceeds of the money laundering discussed above.

155. On June 26, 2020, Wireless World applied to the SBA for an Economic Impact Disaster Loan ("EIDL"), made available due to the COVID-19 pandemic.

a. The application claimed that Wireless World had gross revenues in 2019 of \$16,163,228 and a cost of goods sold

of \$15,279,299, meaning Wireless World saw an overall net profit of \$883,929 in 2019.

156. As part of the EIDL application, applicants must swear that "all information in your application and submitted with your application is true and correct to the best of your knowledge and that you will submit truthful information in the future."

157. The loan application also includes the following notice and warning:

Whoever wrongfully misapplies the proceeds of an SBA disaster loan shall be civilly liable to the Administrator in an amount equal to one-and-one half times the original principal amount of the loan under 15 U.S.C. 636(b). In addition, any false statement of misrepresentation to SBA may result in criminal, civil, or administrative sanctions including, but not limited to: 1) fines and imprisonment, or both, under 15 U.S.C. 645, 18 U.S.C. 1001, 18 U.S.C. 1014, 18 U.S.C. 1040, 18 U.S.C. 3571, and any other applicable laws; 2) treble damages and civil penalties under the False Claims Act, 31 U.S.C. 3729; 3) double damages and civil penalties under the Program Fraud Civil Remedies Act, 31 U.S.C. 3802; and 4) suspension and/or debarment from all Federal procurement and non-procurement transactions. Statutory fines may increase if amended by the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015.

158. On July 1, 2020, DANESHGAR electronically signed his agreement to all conditions of the EIDL loan for application #3306863320 using DocuSign software.

159. In a subsequent modification of the loan when additional funds were requested, DELAFRAZ was added as a second signatory for the loan. DELAFRAZ also used DocuSign software.

160. DANESHGAR and DELAFRAZ directed the SBA to deposit, through a wire transfer, the initial EIDL loan of \$156,900 to

Wireless World Cathay Account #1. The loan was disbursed as an advance payment of \$7,000 on July 1, and the remaining \$149,900 was deposited on July 2, 2020.

161. DANESHGAR and DELAFRAZ requested additional EIDL funds to cover what they claimed were losses due to the ongoing COVID-19 pandemic. On November 17, 2021, a second wire transfer of \$350,000 was deposited to Wireless World Cathay Account #1.

162. On November 17, 2021, Wireless World Cathay Account #1 received three additional wires, commingling the EIDL funds and other wires. On November 18, 2021, Wireless World Cathay Account #1 was used to send \$40,000 to 6 and 7 Wholesale Cars, a business account controlled by coconspirator Thola.

163. On December 10, 2021, a third wire transfer was sent by the SBA to Wireless World Cathay Account #1 for \$821,100. This brought the total EIDL funds received by Wireless World to approximately \$1.325 million.

164. On December 10, 2021, two additional wires were received from electronics-focused businesses in Malaysia and Latin America and commingled with the EIDL and other funds.

165. On December 10, 2021, Wireless World Cathay Account #1 was used to send a \$120,000 wire transfer to a Driver Power Rentals account controlled by a coconspirator of Thola.

E. Surveillance of Wireless World

166. During this investigation the FBI and HSI have conducted physical surveillance and use surveillance cameras to observe the operation of the Wireless World warehouse. That surveillance is summarized below.

1. Physical Surveillance (2019)

167. HSI conducted physical surveillance at the previous Wireless World location in Chatsworth in August and September 2019. During that surveillance, DELAFRAZ and DANESHGAR were regularly seen at the warehouse. The Wireless World van was also regularly present. HSI observed deliveries being made by FedEx and also by numerous individuals who arrived in passenger vehicles and delivered boxes to the warehouse.

2. FBI Surveillance Camera (2020)

168. In February 2020, the Wireless World warehouse moved to its current location in Van Nuys. From approximately August 12 to October 17, 2020, the FBI operated a surveillance camera outside the Wireless World warehouse. Review of the footage revealed, among other things, the following:

a. DELAFRAZ and DANESHGAR were regularly present at the Wireless World warehouse during business hours, as was Coconspirator F.

b. Items were delivered to the warehouse throughout the day, including by traditional couriers (FedEx, UPS), and numerous individuals in personal vehicles.

c. Items observed being delivered included Apple products, vacuums (Dyson, Roomba, Shark), Nest cameras, and Nintendo products.

d. Coconspirator G was observed at the warehouse on approximately three occasions:

i. On August 13, 2020, Coconspirator G emptied duffle bags filled with iPads, MacBooks, Apple Watches, cameras

and headphones onto a rolling cart and then entered the warehouse.

ii. On September 2, 2020, Coconspirator G delivered roughly 25 Apple products from the trunk of his Toyota Camry.

iii. On September 23, 2020, Coconspirator G offloaded approximately 40 to 50 Apple products at the warehouse.

e. On August 14, 2020, Coconspirator B was observed entering the warehouse carrying three items resembling Apple Watches.

f. On August 25, 2020, Coconspirator B delivered a box into the warehouse from a white Mercedes vehicle.

g. On September 1, 2020, Coconspirator C was seen delivering multiple boxes to the warehouse.

h. On October 15, 2020, Coconspirator C delivered multiple boxes including Nintendo Switches.

i. On September 1, September 29, and October 9, 2020, Coconspirator E offloaded several dark colored boxes resembling Shark vacuums into the warehouse.

j. On August 14, 2020, a large box bearing the Home Depot logo was offloaded from the Wireless World van into the warehouse.

k. On September 4, 2020, several boxes were offloaded from the Wireless World van including gaming consoles, and Target store shopping bags containing Apple products.

3. HSI Surveillance Camera (2021)

169. From approximately July 13, 2021, through December 31, 2021, HSI operated a surveillance camera at the Wireless World warehouse in Van Nuys. The following are some observations not previously discussed in this affidavit.

a. DELAFRAZ, DANESHGAR and Coconspirator F continued to be seen at the business daily.

b. Merchandise and packages were largely delivered by individuals in passenger vehicles and in over 30 instances were seen in conjunction with retail store shopping bags. The merchandise observed being delivered to the warehouse included Apple, Dyson, Microsoft, and other electronics.

c. Frequent deliveries of boxes and packages were made by FedEx and UPS shipping services.

d. The Wireless World van was used frequently by warehouse employees to take items or merchandise in and out of the warehouse.

e. DELAFRAZ was seen 18 times bringing merchandise into the warehouse, often Apple products, from his white Tesla.

f. DANESHGAR was seen eight times arriving at the warehouse in various vehicles (the Wireless World van, a U-Haul van, and Dodge Ram truck) and providing boxes or items that were taken into the warehouse.

g. Coconspirator B was seen on 21 occasions dropping off merchandise. Coconspirator B used various vehicles and often delivered seemingly full shopping bags to the warehouse, some of which bore Target and Home Depot retail store logos.

Items delivered appeared to be Apple iPhones, Oculus products, and Nintendo products.

h. Coconspirator F was seen eight times taking boxes from his dark colored Tesla sedan into the warehouse.

i. Coconspirator E was seen on 16 occasions delivering merchandise, mostly Shark brand products.

j. Conspirator G and an associate were observed driving a Range Rover and a silver Dodge Charger delivering items appearing to be retail merchandise on over 20 occasions.

4. HSI Surveillance Camera (2022)

170. HSI operated a surveillance camera at the Wireless World warehouse between approximately January 1 and September 9, 2022. Merchandise continued to arrive at the warehouse in a similar fashion as previously seen. DELAFRAZ and DANESHGAR and Coconspirator F were observed at the warehouse daily. Coconspirators Thola, B, E, and G were all observed continuing to deliver consumer electronics.

5. Physical Surveillance (2025)

171. On August 19, 2025, FBI Special Agents conducted physical surveillance outside the Wireless World warehouse.

a. At approximately 8:45 a.m. a white Tesla arrived at 16141 Leadwell Street in Van Nuys. An individual, who appeared to be DELAFRAZ, exited the Tesla, unlocked the gate, and entered.

b. At approximately 9:15 a.m., a white utility van arrived at the business and was guided into the parking lot by the individual believed to be DELAFRAZ. An unknown male exited

the warehouse driving a forklift and proceeded to unload the contents of the utility van.

c. Between approximately 9:20 a.m. and 10:15 a.m. agents observed one individual on foot and one individual in a dark colored Tesla arrive at the warehouse.

d. Agents reviewed public information for businesses surrounding the Wireless World warehouse. This led agents to discover that the adjacent warehouse at 16135 Leadwell Street, which appeared to share a wall with 16141 Leadwell Street (the Wireless World warehouse), was registered to MaxOutDeald (which I believe to be misspelling of "MaxOutDeals," one of the business names used by DANESHGAR and DELAFRAZ). MaxOutDeald purports to be a "retail buying group," that purchases electronics; this is the same description that MaxOutDeals provides on its website. Google reviews of MaxOutDeald praised "Ben" and "Sam", who I believe to be DANESHGAR and DELAFRAZ. One Google review stated, "It's been a pleasure to work with Sam and Ben every step of the way."

e. Based on the foregoing, I believe that, in addition to using the Wireless World warehouse space, DANESHGAR and DELAFRAZ are also using the adjacent warehouse space to conduct the same money laundering scheme. I believe that the use of the MaxOutDeals name for both this space in Los Angeles and for the warehouse in Delaware is likely an attempt to further conceal Wireless World's activities in the wake of the Bai and Thola Indictments.

F. Ongoing Wireless World Operations

1. Changed Shipping Patterns

172. After Thola and his coconspirators were arrested in August 2024, investigators observed changes in the way that DELAFRAZ and DANESHGAR conducted shipments of goods. From FedEx shipping records I learned that prior to August 2024 most Wireless World exports were sent directly from the Wireless World warehouse in Van Nuys or from the greater Los Angeles area. After August 2024, FedEx shipping records showed that Wireless World export shipments shifted from Los Angeles to Delaware and Miami. In Delaware, exports came from a warehouse registered to MaxOutDeals and located at 161 Cirillo Circle, New Castle, Delaware (the MaxOutDeals warehouse). In 2023, MaxOutDeals was trademarked by Wireless World. After Thola's arrest, which was publicized on local and national news, DELAFRAZ and DANESHGAR began to send Amazon and Apple shipments to the MaxOutDeals warehouse instead of the Wireless World warehouse.

2. June 2025 Inspection in Miami

173. Based on my review of U.S. Customs records, Wireless World exports merchandise to Paraguay, among other foreign destinations. I determined that exports to Paraguay routinely departed through the Port of Miami (Florida). Customs records also referenced third-party shipping services, including a customs bonded warehouse operator ("Shipper-1") used by Wireless World to receive merchandise to be exported at a customs bonded warehouse operated by Shipper-1.

174. On June 13, 2025, Shipper 1 granted HSI access to the customs bonded warehouse where Wireless World's merchandise was pending exportation. I observed, affixed to outer wrapping of the Wireless World shipments, labels showing that the shipments originated from the MaxOutDeals warehouse. I examined Wireless World's outbound shipments and observed numerous Apple products in cardboard boxes and sealed with packing tape marked "wirelessworld.us." I saw Apple products, some of which also bore markings indicating the merchandise had originated from Amazon before it was acquired by Wireless World.

175. Shipper-1 provided invoices that accompanied the Wireless World merchandise. Each invoice listed Wireless World as the seller.⁸ These invoices displayed the Apple products I observed as well as the cost at which the items were being sold. Based on my review of one of the invoices ("Invoice 9380"), it appeared that Wireless World was selling the Apple products at prices that were often lower than those of major U.S. retailers like Target, Amazon, Best Buy, Walmart, and Apple.⁹ Shipper-1's records showed that the Apple products had been shipped, in part, from the Wireless World warehouse in Van Nuys.

⁸ From discussions with an employee of Shipper-1, I understand that Shipper-1 had received shipments purporting to come from a variety of different businesses in the U.S. for export, but many of them were accompanied by Wireless World invoices. I believe that Wireless World is using various names, including MaxOutDeals, 2D Distribution, and Kripto Mobile to conceal the true source of the shipments.

⁹ Online price research was conducted on July 13, 2025 through retail websites.

176. I reviewed Invoice 9380 and made several observations about items on that invoice:

a. Wireless World listed an item described as "Apple-MacBook Pro 14-inch Apple M4 chip Built for Apple Intelligence - 16GB -1TB SSD", with a price of \$1,545.00. Based on my research, I saw the same Apple product being sold on Amazon.com for \$1,599.99 and for \$1,799.00 on Apple.com.

b. Wireless World listed an item described as "Apple Watch SE (Gen2) 44mm Starlight - GPS" with a price of \$200.00. Based on my research, I saw the same Apple product being sold on Apple.com for \$279.00, and for \$199.00 on Amazon.com.

c. Wireless World listed item "Apple - AirPods Pro (2nd generation)" as being sold at the unit price of \$176.00, I observed this Apple product being sold on Target.com and Apple.com for \$249.00 and \$237.00 on Amazon.com.

177. Pursuant to legal process served to retailers Walmart, Target, and Apple in February 2025, I learned that Wireless World does not have any bulk purchasing agreements in place with those retailers that would allow them to acquire Apple products at wholesale prices, although Wireless World does have a reseller classification with Best Buy which may allow them to purchase items tax free.

178. During 2024 and 2025, and at other times during the investigation, HSI and FBI operated surveillance cameras overlooking the Wireless World warehouse in California. A summary of observations from those cameras by HSI personnel showed that in 2025, as in prior years, merchandise was

regularly seen being supplied to Wireless World by individuals carrying retail-style shopping bags into or near the business.

179. From June 2025 through early September 2025, Wireless World exported approximately \$42,337,645 in reported value of consumer electronics mostly using the Van Nuys address and beginning in August 2025 to early September 2025 exported an additional \$8,913,760 in reported value of consumer electronics under the name 2D Distribution using the MaxOutDeals warehouse address. Wireless World continued to receive payments from international recipients in connection with those exports, and from June 2 to July 2, 2025, received over \$5,000,000 in payments to the Wireless World Cathay Bank Accounts. Based on my review of Cathay Bank financial records I observed that Wireless World also began using Wireless World Cathay Account #3, under the name 2D Distribution, to receive funds for exported consumer electronics.

180. On June 14 and June 20, 2025, Wireless World shipped exports listing values of \$153,659 and \$163,197 (totaling \$316,856) for merchandise consisting of "LAPTOPS/TABLETS, SMART WATCH, HEADPHONES" to Dubai Company #1. On July 2, 2025, Dubai Company #1 paid \$548,000.00 by bank wire to Wireless World Cathay Account #3. Between February 2022 and June 2024, Dubai Company #2 paid Wireless World over \$116 million in total to the Wireless World Cathay Accounts.

181. Based on recent records Wireless World continued to export to Dubai Company #1 throughout 2025. The most recent

wire from Dubai Company #1 was for approximately \$217,965 on July 15, 2025.

182. Based on internet searches I identified a business using the website www.maxoutdeals.com listing an address at 161 Cirillo Cir, New Castle, Delaware 19720 (the MaxOutDeals warehouse). Google records show that the MaxOutDeals website belongs to Wireless World and the account holder was DANESHGAR.

183. During August 2025 HSI conducted surveillance at the MaxOutDeals warehouse.¹⁰ During that surveillance inbound shipments of boxes from UPS, FedEx and Amazon were seen. Additionally, HSI observed warehouse workers retrieve shipments from a separate warehouse nearby indicating a similar method of operation to how DANESHGAR and DELAFRAZ used P.O. Box locations in the Los Angeles area to receive merchandise purchased with fraud proceeds.

//

//

//

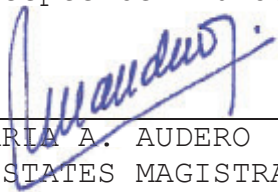
¹⁰ During the surveillance I learned several warehouses operate at 161 Cirillo Circle, New Castle, DE, however "161-A" is the unit specific to MaxOutDeals.

V. CONCLUSION

184. For all the reasons described above, there is probable cause to believe that DELAFRAZ and DANESHGAR have committed a violation of 18 U.S.C. § 1956(h).

/s/ Christopher Cutaia
CHRISTOPHER CUTAIA, Special Agent
Homeland Security Investigations

Attested to by the applicant in
accordance with the
requirements of Fed. R. Crim.
P. 4.1 by telephone on this 8th
day of September 2025.



HON. MARIA A. AUDERO
UNITED STATES MAGISTRATE JUDGE