AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Massachusetts

United States of America
v.
CRAIG CLAYTON

Case No. 23-6002-MPK

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Jan. 1, 2019 to Jan. 10, 2022 in the county of Essex in the _____ District of Massachusetts, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 1956(h), (a)(1)(B)(i); 18 U.S.C. § 1512	Conspiracy to Commit Money Laundering; and Obstruction of Justice

This criminal complaint is based on these facts:

See attached affidavit of Special Agent Lori Robinson

☑ Continued on the attached sheet.

/s/ Lori Robinson
Complainant's signature

Lori Robinson, Special Agent, HSI
Printed name and title

Sworn telephonically in accordance with Fed. R. Crim. P. 4.1

Date: February 21, 2023

City and state: Boston, MA

UNITED STATES DISTRICT COURT DISTRICT OF MASSACHUSETTS

Page Kelley
Judge's signature

Hon. M. Page Kelley, Chief U.S. Magistrate Judge
Printed name and title

AFFIDAVIT OF SPECIAL AGENT LORI ROBINSON IN SUPPORT OF COMPLAINT AND APPLICATION FOR SEARCH AND SEIZURE WARRANTS

"We are already 'money mules' complicit in their offenses. It just opens us up to charges."
– Craig CLAYTON, March 24, 2020 e-mail to CC-2.

"Do we have any dirt on [Victim] we use to distract the police?"
-- Craig CLAYTON, July 31, 2021 WhatsApp message to CC-3.

"Let's move to Signal. Whatsapp can be tapped."
-- Craig CLAYTON, August 30, 2021 WhatsApp message to CC-3.

***

I, Lori Robinson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI") assigned to the Boston, Massachusetts Field Office. I have been employed as a Special Agent with HSI since 2014. I have investigated and assisted other agents in investigating numerous cases involving a variety of criminal violations including money laundering, fraud, identity theft, narcotics, and smuggling. I have received on-the-job training as well as participated in DHS-sponsored training courses on these types of investigations. My investigations and training have included the use of surveillance techniques and the execution of search, seizure, and arrest warrants.

2. The HSI New England El Dorado Financial Task Force, the Internal Revenue Service – Criminal Investigation, the United States Postal Inspection Service, and I are currently investigating CRAIG CLAYTON ("CLAYTON") for money laundering and conspiracy to commit money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957; obstruction of justice, tampering with, and retaliating against a witness and victim, and conspiracy to commit the same, in violation of Title 18, United States Code, Sections 1512, 1513, and 371; making false statements to a federal agent, in violation of Title 18, United States Code, Section

1001; mail fraud, wire fraud, bank fraud, and conspiracy to commit the same, in violation of Title 18, United States Code, Sections 1341, 1343, 1344, and 1349; and operating an unlicensed money transmitting business, in violation of Title 18, United States Code, Section 1960 (collectively, the "Target Offenses").

3. In summary, as set forth in detail below, there is probable cause to believe that from in or about January 2019 to the present, CLAYTON agreed with known and unknown persons to use his business, Rochart Consulting, to launder the proceeds of internet fraud schemes, principally using bank accounts that CLAYTON opened and held in the names of shell companies on behalf of Rochart's clients. In total, CLAYTON laundered tens of millions of dollars through those shell company bank accounts. In recorded phone calls with an undercover agent, CLAYTON stated, among other things, that his clients include "fugitives." During a later interview with federal agents, CLAYTON attempted to obstruct a federal investigation by making false statements.

4. I submit this affidavit in support of a criminal complaint charging CLAYTON with conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h) and 1956(a)(1)(B)(i); and obstruction of justice, in violation of Title 18, United States Code, Section 1512(c)(2).

5. I also submit this affidavit in support of an application for a warrant to search the residence of CLAYTON located at 52 Parkside Drive, Cranston, Rhode Island 02910 ("the Clayton Residence" or "the Subject Premises"), which is described in more detail in Attachment A to the warrant to search the Clayton Residence. For the reasons stated herein, there is probable cause to believe that evidence, fruits, and instrumentalities of the Target Offenses, as described in more detail in Attachment B to the proposed warrant, will be found in the Clayton Residence, including on cellular phones and computers belonging to CLAYTON and CC-1.

6. I also submit this affidavit in support of applications for seizure warrants for the following property:

a. Any and all funds held by Navigant Credit Union ("Navigant") in, or on behalf of, bank account number 752359165 in the name of Providence Sanitizer Inc. ("Target Account 1");

b. Any and all funds held by Navigant in, or on behalf of, bank account number 752364961 in the name of Sustainable Agriculture Technology Inc. ("Target Account 2");

c. Any and all funds held by Navigant in, or on behalf of, bank account number 750698962 in the name of Rochart Inc. ("Target Account 3");

d. Any and all funds held by Navigant in, or on behalf of, bank account number 752025711 in the name of Rochart Inc. ("Target Account 4"); and

e. A 2016 Mercedes GLC 300, VIN #WDC0G4KB9GF085486 (the "Target Vehicle"), located at the Subject Premises, and collectively with Target Accounts 1 through 4, the "Target Assets".

7. The facts in this affidavit come from my participation in this investigation, including, among other things: listening to consensually recorded telephone calls between CLAYTON and an undercover agent; my and other agents' review of records, including documents, e-mails, and text and instant messages seized in connection with the execution of Court-authorized search warrants;[1] interviews that I and other law enforcement agents have conducted; my training and experience; and information obtained from other agents and witnesses.

[1] I previously submitted an affidavit in support of an e-mail search warrant for craig.clayton@rochartgroup.com. *See* 21-MJ-2445-MBB (D. Mass.). I previously submitted an affidavit in support of a search warrant for the Subject Premises. *See* 21-SW-585-PAS (D.R.I.).

8. In submitting this affidavit, I have not included every fact known to me about this investigation. Rather, I have included only those facts that I believe are sufficient to establish probable cause for (1) the criminal complaint charging CLAYTON with conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h) and 1956(a)(1)(B)(i), and obstruction of justice, in violation of Title 18, United States Code, Section 1512(c)(2); (2) the search warrant for the Subject Premises; and (3) the seizure warrants for the Target Assets.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

A. Relevant Individuals, Entities, and Background

9. CLAYTON lives in Rhode Island at the Subject Premises. According to his website, CLAYTON formerly worked for a large accounting firm as an accountant. The below picture comes from a WhatsApp message that CLAYTON sent to an undercover agent. I have personally met CLAYTON, and the picture fairly and accurately represents his appearance.

10. According to public records and documents seized pursuant to search warrants, in or about 2017, CLAYTON founded the company Rochart, Inc., d/b/a Rochart Consulting ("Rochart"). According to those records, CLAYTON is the owner and operator of Rochart, which purported to be a financial consulting and "virtual CFO" business. According to its website, Rochart provided several services, including among other things, "US banking solutions" for foreign nationals. At all times relevant to this Affidavit, CLAYTON operated Rochart from the Subject Premises and, based on records seized during the execution of a search warrant, stored business-related files and computer equipment there.

11. CC-1 is CLAYTON's spouse and lives at the Subject Premises. According to records seized from the execution of search warrants, including CLAYTON's e-mails, and as set forth in further detail below, CC-1 assists CLAYTON with Rochart's business, executes bank account deposits and withdrawals for Rochart clients, and has a Rochart e-mail address from which she communicates with Rochart clients.

12. Based on public records and documents seized pursuant to search warrants, CC-2 operates a company ("Company-1") that markets itself as providing solutions for global entrepreneurs to do business remotely in the United States. CC-2 and Company-1 act as a foreign client recruiter and marketing director for Rochart and CLAYTON. Based on, among other things, bank account transfers from CLAYTON to CC-2, I believe that CC-2 resides in Ukraine.

13. CC-3 is a client of CLAYTON and Rochart. In communications seized pursuant to search warrants, CC-3 told CLAYTON that he lives in Dubai.

14. In general, the Bank Secrecy Act, 31 U.S.C. § 5311 *et seq.*, as amended in 2001 by the USA PATRIOT Act (collectively, "BSA") and regulations promulgated by the Financial Crimes Enforcement Network ("FinCEN"), require that banks in the United States implement and

administer anti-money laundering ("AML") and know-your-customer ("KYC") programs. Among other things, banks are required to take steps to learn about their customers, particularly foreign customers, to monitor account activity, and to collect and verify information regarding customers opening bank accounts on behalf of businesses, including information regarding the true beneficial owners of business bank accounts.

15. Based on my training, experience, and the investigation in this case, I am aware that foreign nationals seeking to launder criminal proceeds through the United States banking system often attempt to conceal their identities by paying a "straw owner" to create a shell or front company (a company having no legitimate business purpose) in the United States, and then instructing that straw owner to open bank accounts through which to launder and transfer abroad the criminal proceeds on behalf of the true beneficial owners of the funds.

16. Based on my training, experience, and the investigation in this case, I am familiar with different types of fraud schemes committed via the internet. One such online fraud scheme known as a "romance scam" generally involves perpetrators creating fictitious profiles on online dating or social media platforms, gaining the trust of potential victims, and then directing those victims to transfer money under false pretenses.

17. Another type of online scam is generally referred to as "elder fraud" because these types of schemes target the elderly. Although elder fraud can take a variety of forms, it generally involves a perpetrator contacting an elderly victim, gaining the trust of the victim, and using high-pressure tactics to convince the victim to transfer money under false pretenses.

18. Based on my training and experience, I know that online fraud schemes, including romance scams and elder fraud, are often committed by perpetrators outside of the United States. These schemes, however, frequently involve the use of the United States banking system and of

conspirators in the United States to launder and/or access the fraud proceeds. For example, romance scams commonly involve conspirators opening bank accounts in the United States because, among other reasons, victims cannot transfer—or are more suspicious of transferring—money to international bank accounts. Further, it is difficult for international conspirators to open bank accounts in the United States under the BSA. And based on my training and experience, I know that persons who launder fraud proceeds often try to conceal the nature of the fraudulent schemes and the disposition of the proceeds by incorporating shell companies and opening the bank accounts in the names of the corporations.

B. The Money Laundering Scheme

Overview of the Money Laundering Scheme
and CLAYTON's Obstruction and False Statements

19. Starting no later than in or about January 2019, CLAYTON, CC-2, and Rochart clients perpetrated a concealment money laundering scheme using dozens of bank accounts that CLAYTON opened in Massachusetts and Rhode Island. CLAYTON opened those accounts in the names of numerous shell companies that did not have legitimate offices in the United States, employees, business transactions, or revenue. For nearly all of those accounts, CLAYTON listed the company's address as either the Subject Premises or an apartment in Slatersville, Rhode Island where he previously lived. For nearly all the accounts, CLAYTON and CC-1 are the only signatories—that is, the pertinent bank account records do not list any other beneficial owners or controllers, including foreign persons.

20. Bank records show that when CLAYTON opened a bank account for a shell company, he identified himself as the company's "manager," "president," or other leader. Many of the companies were incorporated by or at the direction of CLAYTON in Delaware, Wyoming, or Rhode Island only shortly before he opened the bank accounts.

21. As several examples detailed below demonstrate, CLAYTON generally conducted the money laundering scheme, in exchange for fees paid to Rochart by clients, as follows. First, CLAYTON incorporated a shell company in the United States on behalf of a foreign client of Rochart. Then, CLAYTON opened one or more business bank accounts for the company, typically at a bank in Rhode Island or Massachusetts. In opening the accounts, CLAYTON generally did not disclose to the bank that he was opening the account on behalf of a foreign individual or shell company. CLAYTON then created, or directed his foreign client to create, an online banking profile for the purposes of controlling the account and sending wire transfers from the United States bank account to foreign bank accounts controlled by the client.

22. Once CLAYTON formed the shell company and opened the bank account, Rochart's foreign clients then directed co-conspirators and victims of fraudulent schemes—including romance scams and elder fraud—in the United States to send money to the bank accounts opened by CLAYTON, via wire transfers, as well as via money orders, checks, and cash that were mailed to the Subject Premises. CLAYTON and CC-1 laundered those money orders, checks, and cash, which were often sent to CLAYTON in structured amounts, by depositing them into the bank accounts, also sometimes in multiple transactions. Based on my training and experience, and as CLAYTON discussed in encrypted communications with CC-3 that are discussed below, I know that individuals laundering criminal proceeds often attempt to evade law enforcement and bank-regulator scrutiny by dividing large financial transactions—including deposits and withdrawals—into a series of smaller transactions. These incoming wire transfers and deposits did not have any legitimate business purpose connected to the shell company. Rochart's clients and CLAYTON then used the online banking credentials to rapidly authorize and send wire transfers abroad,

including to bank accounts in China, Switzerland, Austria, Hong Kong, Thailand, Singapore, India, Ukraine, Malaysia, Poland, and Turkey.

23. Thereafter, the U.S. bank accounts were generally either liquidated by CLAYTON's co-conspirators, closed by CLAYTON with minimal balances, or frozen by the banks pending investigations by the banks of fraud and money laundering. When the accounts were closed or frozen at one bank, CLAYTON often opened an account at a different bank for the same Rochart client in the name of the same shell company, or he created a new shell company for the same Rochart client, and repeated the process.

24. CLAYTON admitted to CC-2 in an e-mail on or about March 24, 2020 that he knew that his activity was illegal, stating that their use of bank accounts and execution of monetary transfers made them "complicit in their [Rochart's clients'] offenses" and "opens us up to charges."

25. Bank records reviewed by investigators in this case show that from January 2019 to present, CLAYTON opened approximately 80 bank accounts for more than 65 different companies that received approximately $48 million.

26. For example, and as further detailed below, for one of Rochart's clients, CC-3, CLAYTON created at least five different shell companies, and he opened at least 14 bank accounts at seven different banks (including in Massachusetts). The accounts that CLAYTON opened for CC-3 received and laundered more than $35 million, including proceeds of fraud. When banks and members of law enforcement began to investigate CLAYTON, Rochart, and its clients, CLAYTON attempted to cover-up the money laundering scheme by, among other things, falsely telling the banks and law enforcement that the shell companies he created for CC-3 were legitimate businesses. And as further detailed below, CLAYTON instructed CC-3 to find "dirt" on an elderly

victim from whom CC-3 stole nearly $200,000 so that they could mislead and obstruct bank and law enforcement investigations.

27. In or about 2021, CLAYTON described the nature of his scheme during recorded conversations with an undercover law enforcement agent posing as a potential Rochart client. During those conversations, CLAYTON bragged about having clients who were fugitives from justice, probed the undercover agent about any connections to law enforcement and said "[w]e don't deal with anyone who has law enforcement connections," and described his scheme as follows: "we incorporate a company, set-up a bank account, . . . and the money starts rolling."

28. In or about December 2021, federal law enforcement agents executed a court-authorized search warrant at the Subject Premises and seized, among other things, CLAYTON's communications with CC-3 on encrypted messaging applications, some of which are detailed below. For example, CLAYTON told CC-3 via WhatsApp that he was concerned law enforcement was "digging into our business," and he discussed fake cover stories that he would provide law enforcement and bank compliance personnel if questioned.

29. After execution of the search warrant, and during the course of a Grand Jury investigation, CLAYTON agreed to be interviewed by federal agents pursuant to a standard proffer agreement with the United States Attorney's Office for the District of Massachusetts. During an interview conducted in Boston in or about January 2022, CLAYTON corruptly attempted to obstruct, influence, and impede an official proceeding by making several false statements about the money laundering scheme to federal agents.

30. By January 2022, as a result of the execution of the search warrant and meeting with federal law enforcement, CLAYTON knew that his conduct was under scrutiny. However, there is probable cause to believe, as set forth below, that CLAYTON nevertheless continued his

money laundering scheme by using an online payment processing service rather than fraudulent bank accounts.

PJT International

31. According to public records, on or about August 22, 2019, CLAYTON incorporated PJT International, LLC ("PJT International") in Delaware. Investigators have not identified any office, employees, business, customer base, or revenue for PJT International.

32. On or about January 3, 2020, CLAYTON opened a Bank of America checking account in the name of PJT International (the "PJT International BoA Account") at a branch in Rhode Island. In opening the account, CLAYTON listed himself as the "manager" of PJT International, and he listed himself as the sole authorized signatory on the account. CLAYTON did not indicate that any foreign persons owned, controlled, or directed any part of PJT International's purported business.

33. From in or about January 2020 to March 2020, the PJT International BoA Account received more than $175,000 in wire transfers and deposits, including from individuals in the United States, and shortly after each incoming transfer and deposit, the funds were wired to foreign bank accounts in Hong Kong and Singapore, among other countries.

34. For example, Victim-1, whom law enforcement has interviewed, was a romance scam victim who sent money under false pretenses to the PJT International BoA Account opened by CLAYTON. Victim-1 lived in Texas. In or about September 2019, Victim-1 met an individual on an internet dating website. The individual told Victim-1 that he was a member of the U.S. military deployed in the Middle East. Victim-1 and the individual developed an online relationship. The purported military member requested that Victim-1 send him money for a variety of purported reasons, including to pay for costs to repatriate a significant sum of money that he

had located abroad. From in or about September 2019 to April 2020, Victim-1 wired money to various bank accounts at the instruction of the purported military member and other individuals who contacted her on behalf of the military member.

35. For example, on or about February 25, 2020, Victim-1 wired approximately $40,000 to the PJT International BoA Account. On or about the same day, more than $33,000 was wired from the PJT International BoA Account to a bank account in Poland.

36. On or about March 6, 2020, the PJT International BoA Account was liquidated and closed by CLAYTON at a branch in Rhode Island.

37. Based on the investigation, it appears that the true beneficial owners of the PJT International BoA Account and controllers of the PJT International "business" paid CLAYTON fees for his services. For example, on or about February 3, 2020, and again on or about March 2, 2020, wire transfers of $150 were sent from the PJT International BoA Account to a bank account in the name of "Rochart Inc." for "monthly maintenance fees."

Cryson

38. In or about September 2019, CLAYTON and CC-2 began a business relationship with CC-3. CC-3 contacted CLAYTON and CC-2 by e-mail regarding opening U.S. bank accounts, and CC-3 told CLAYTON and CC-2 that it was important to conduct his U.S. banking "without being so much noticed." In response, CLAYTON and CC-2 advised CC-3 via e-mail that they would establish a shell company in Delaware and proceed to open U.S. bank accounts in CLAYTON's name secretly on behalf of CC-3. For example, on or about September 15, 2019, CC-2 e-mailed CC-3, copying CLAYTON: "Your information is confidential with Delaware."

39. On or about September 16, 2019, CLAYTON incorporated Cryson Trading LLC ("Cryson") in Delaware. Investigators have not identified any office, employees, business,

customer base, or revenue for Cryson, which purports to be a trade company. Upon receipt of Cryson's federal tax identification number (EIN), CLAYTON e-mailed CC-3: "This is great. We are now ready to travel to the branch and set up the account."

40. On or about October 22, 2019, CLAYTON opened a JP Morgan checking account in the name of Cryson (the "Cryson JP Morgan Account") at a branch in Rhode Island. In opening the account, CLAYTON listed himself as the "manager" of Cryson, and he listed himself as the sole authorized signatory on the account. CLAYTON did not disclose CC-3's involvement in the business or indicate that any foreign persons owned, controlled, or directed any part of Cryson's purported business.

41. On or about October 23, 2019, CLAYTON sent the account information for the Cryson JP Morgan Account to CC-3. In the e-mail, CLAYTON wrote, "Please advise the Login ID you would prefer to use for Online Banking . . . Using that login ID and US Cellphone Number, we will generate your Online Banking profile and send you an email requesting that you login and establish your password."

42. Meanwhile, CLAYTON and CC-2 discussed how much they would charge CC-3 for establishing Cryson as a shell company and opening U.S. bank accounts for him. For example, CLAYTON and CC-2 exchanged several e-mails discussing how much they were going to charge CC-3. CC-2 asked CLAYTON, "sorry to bother but just to double check – we would charge [CC-3] with $900 per month . . . correct? No % on incoming amounts as we thought before? Flat fee is better here, right?" CLAYTON responded, " I think flat fee would be better."

43. From in or about October 2019 to in or about December 2019, the Cryson JP Morgan Account received more than $1.3 million in wire transfers and deposits from individuals in the United States. Banks records that investigators have reviewed do not contain any identifiable

bona fide commercial transactions by Cryson related to the transfers and deposits. Rather, consistent with the pattern described above, CC-3 used the online banking credentials to authorize and send wire transfers to foreign bank accounts shortly after the funds were received.

44. According to bank records, in or about December 2019, JP Morgan closed the account due to suspected fraud and money laundering. On or about December 15, 2019, CLAYTON e-mailed CC-3 and CC-2, notifying them that "JPMC closed the Cryson Trading account for potentially fraudulent activity."

45. Less than one month later, CLAYTON and CC-3 discussed opening another bank account for CC-3 in the name of Cryson even though JP Morgan closed the previous one for fraudulent activity. On or about January 9, 2020, CC-3 e-mailed CLAYTON and CC-2 and wrote, "Can you open Cryson Trading in Bank of America?"

46. On or about the next day, January 10, 2020, CLAYTON opened a Bank of America checking account in the name of Cryson (the "Cryson BoA Account") at a branch in Rhode Island. In opening the account, CLAYTON listed himself as the "manager" of Cryson, and he listed himself as the sole authorized signatory on the account. CLAYTON did not indicate that any foreign persons owned, controlled, or directed any part of Cryson's purported business.

47. From in or about January 2020 to in or about August 2020, the Cryson BoA Account received more than $4.5 million in wire transfers and deposits, including the proceeds of an elder abuse scam perpetrated over the internet, in violation of Title 18, United States Code, Section 1343. Shortly after each incoming deposit or wire transfer, the funds were wired abroad to foreign bank accounts, principally in China.

48. CLAYTON knew that CC-3 was using Cryson to launder criminal proceeds. For example, on or about March 24, 2020, CLAYTON e-mailed CC-2 a list of Rochart clients, writing,

"[W]e have the following Bad Actors at the moment." Next to Cryson, CLAYTON wrote "AML," which is a common abbreviation for anti-money laundering. CLAYTON proposed charging these "bad actors" a one-time premium fee of $5,000 to $9,000 that would compensate CLAYTON and Rochart for the loss of monthly fees when the bank accounts were inevitably closed due to fraud. CLAYTON justified this proposed premium, writing "we will lose out on the [monthly] fees we would normally charge. 150 [per month] * 5 years = 9,000 USD." CC-2 asked CLAYTON about potentially closing the bad actors' accounts based on the "fraud / ML," and told CLAYTON that "reopening them anywhere else means we are contributing to scams / ML." CLAYTON responded, in part: "we are already 'money mules' complicit in their offenses," which "opens us up to charges," and he stated that the one-time "fee also ensures our silence if there are issues." CC-2 responded by saying he did not think Rochart clients would pay the fee, telling CLAYTON: "[T]here are cheaper ways to get bank account. E.g. luring regular people into their scheme." CLAYTON replied that he would "try" the one-time fee with Cryson and "see what they say."

49. On or about April 15, 2020, CLAYTON sent CC-2 an e-mail in which he proposed a "bad actor strategy" of opening a new bank account for a Rochart client whose bank accounts had been subjected to bank scrutiny for fraud or money laundering, and then negotiating a fee with the client for continuing to launder their funds through a new account. CLAYTON recommended to CC-2 that they open new bank accounts with a bank that had more "slack" compliance processes. In a later e-mail addressing the same issue, CLAYTON called his idea a "penalty amount for being a bad actor," and he proposed an amount of $2,000 to $5,000. In response to CC-2 telling CLAYTON that Rochart clients would find a cheaper "money mule" rather than pay the fee, CLAYTON responded via e-mail: "The hope is that what we are offering they cannot get elsewhere—an account wholly operated by them, not needing a US person. That should be worth

something." Based on my experience and training, I understand CLAYTON's statement to be an admission that he and CC-2 were committing bank fraud, in violation of Title 18, United States Code, Section 1344. CLAYTON further told CC-2 that he could not continue to be a signatory on such accounts without further compensation "because the risks for us are too high." CLAYTON also told CC-2 that an important service to provide such "bad actors" was depositing cash and Western Union money orders.

50. On or about May 10, 2020, CLAYTON sent CC-2 another e-mail in which he acknowledged that Cryson and CC-3 were "known Bad Actors," and in discussing how to best serve such clients in the future, CLAYTON stated that "a vital piece of the puzzle for the Bad Actors is the ease of sending wires." Later, on or about the same day, CLAYTON told CC-2 via e-mail that Cryson and CC-3 had agreed to a $5,000 "bad actor" fee.

51. In or about June 2020, CLAYTON wrote a "strategic thinking" document for CC-2. CLAYTON wrote that they had "initial success" with JP Morgan and Bank of America, "followed by a ban when a bad actor does something." CLAYTON wrote that "the higher number of accounts the higher the likelihood of being banned" by banks, and that he and Rochart were becoming "unable to find suitable B+M [brick and mortar] banks," and that their business would be "doomed to failure once we run out of B+M banks." Based on those observations, CLAYTON wrote that Rochart's "only long term strategy that will work" was: "take more risk, for more returns . . . keep the number of accounts low to reduce likelihood of being banned . . . minimize detection . . . get big or get out."

52. On or about May 26, 2020, CLAYTON e-mailed CC-3 about how to best continue the money laundering scheme while evading detection by law enforcement and compliance scrutiny from banks. Among other things, CLAYTON proposed that for money orders that CC-3

directed to be sent to CLAYTON's shell company bank accounts, "amounts must be irregular—no more rounded to the nearest $10,000." Based on my training and experience, I know that banks and law enforcement often scrutinize transactions in round numbers, because such transactions lack indicia of bona fide commerce. For example, it is common for items to be priced to 99 cents on the dollar or for services to reflect taxes and costs, which do not usually add up to round numbers. I understand that the creation of irregular amounts indicates an effort to disguise an illicit financial transaction as the product of bona fide commercial activity.

53. On or about May 26, 2020, in the same e-mail exchange, CLAYTON proposed that CC-3 set-up multiple "overseas accounts for the wires" from CLAYTON's shell companies, and that the business names for those accounts should reflect involvement in industries that would be consistent with the shell company. In exchange for a $12,000 fee, CLAYTON proposed setting up two new shell corporations for CC-3, and told him that "throughout the process everything is under our control, despite the outward appearance to the bank." CLAYTON outlined a process through which he could accept money to the shell companies' accounts in the form of money orders, checks, and wire transfers, and then allow a representative of CC-3 to make outgoing "international wire transfers." In response, CC-3 told CLAYTON that he wanted the process to be "safe and secured" and that "I don't want my name to be in any of these process[es]." CLAYTON responded, "your name is not on any of it. You need to come up with a name and email address for the [banking] login only." CLAYTON also suggested that they should set-up websites for the shell companies so that they appeared to be legitimate businesses. In a separate e-mail, CLAYTON told CC-2 that he would give him 20 percent of Rochart's revenue from CC-3.

54. Separately, on or about May 24, 2020, CLAYTON e-mailed CC-2 about several clients he identified as "bad actor[s]" whose accounts were under scrutiny by JP Morgan. CLAYTON told CC-2, "I think we may need to ask them [for approval] to setup new LLC's. Their names may be tarnished in the banking system." CLAYTON also told CC-2 that they needed "to come [up] with a fee for the transfer" to new bank accounts.

55. Victim-2, whom law enforcement has interviewed, was the victim of an elder fraud scheme who, in or about June 2020 (following the e-mails discussed above) sent money under false pretenses to the Cryson BoA Account that CLAYTON opened on behalf of CC-3. Victim-2 lived in Missouri.

56. In or about the summer of 2019, Victim-2 bought a five-year subscription for antivirus software from a company named BTP BG-Supple. On or about June 25, 2020, Victim-2 received a phone call from a person who claimed to be an employee of the antivirus software company. The purported employee informed Victim-2 that the company was going out of business, and that the company would refund him $1,000 for his remaining antivirus subscription. The employee directed Victim-2 to a website where he entered his online banking information so that the company could send him a refund. The employee then told Victim-2 that he had mistakenly transferred $100,000 to Victim-2's bank account rather than the $1,000 refund. The employee instructed Victim-2 to "return" the $100,000 by obtaining a cashier's check and mailing it to a mailing address in Woodside, New York. The purported employee told Victim-2 to make the check payable to Cryson Trading LLC.

57. On or about June 26, 2020, Victim-2 mailed the $100,000 check payable to Cryson to that location as directed.

58. On or about June 29, 2020, the $100,000 check from Victim-2 was deposited into the Cryson BoA Account at a branch in New Jersey. Shortly thereafter, Victim-2 contacted his bank, which notified him that his account never received a $100,000 transfer. The bank told Victim-2 that the $100,000 cashier's check had been drawn on his account.

59. On or about July 15, 2020, the $100,000 check was charged back on the Cryson BoA Account and returned. Based on this investigation and my training and experience, Bank of America's standard practice in the event of a charge-back is to shred the original check, retain a scanned copy, and send an image of the scanned check—which is considered a legal negotiable copy—to the receiving account holder, in this case, CLAYTON.

60. On or about July 22, 2020, CLAYTON deposited the $100,000 check from Victim-2 into the Cryson BoA Account at a branch in Rhode Island. On or about July 24, 2020, Bank of America returned the $100,000 check and charged it back on the Cryson BoA Account.

61. In or about August 2020, CLAYTON closed and liquidated the Cryson BoA Account.

62. Thereafter, and as further detailed below, CLAYTON and CC-3 abandoned the Cryson name, discussed how it was difficult to continue their scheme at large, national banks with robust compliance processes and anti-money laundering controls, and they discussed alternative, smaller banks to launder funds for CC-3. CLAYTON did not open another bank account for CC-3 in the name of Cryson, or for any other CC-3-related entity at either Bank of America or JP Morgan.

63. For example, on or about August 15, 2020, CC-3 e-mailed CLAYTON and CC-2, "So finally BoA is closed now. When will your other set up is ready to use [*sic*] . . . meanwhile if you can open other banks let me know but within 15 days max."

64. CC-3 paid CLAYTON fees for his services in connection with laundering funds through Cryson. For example, in or about May, June, and July 2020, wire transfers for approximately $150, which were identified as "monthly management fees," were sent from the Cryson BoA Account to a bank account controlled by CLAYTON in the name of "Rochart Inc."

Providence Sanitizer, Sustainable Agriculture Technology, Farmers Market Purveyors, and XIM

65. Following the closure of the Cryson JP Morgan Account and Cryson BoA Account, CLAYTON and CC-3 discussed how to continue the scheme with new shell companies and bank accounts. For example, in or about September 2020, CC-3 e-mailed CLAYTON and CC-2, "Boss its [*sic*] six months now, last time you said first week of September you will get access for that also now 20 days passed. It will be nice if you can straight away inform me whether you can do it or not."

66. Thereafter, CLAYTON incorporated four new shell companies to launder money for CC-3. They were: Providence Sanitizer Inc. ("Providence Sanitizer"), Sustainable Agriculture Technology Inc. ("Sustainable Agriculture"), Farmers Market Purveyors Inc. ("Farmers Market"), and XIM Trade Inc. ("XIM"). Based on bank records and documents seized pursuant to search warrants, each of those four entities was merely a shell company with no legitimate pre-existing or ongoing business; CLAYTON incorporated them solely for the purpose of concealing CC-3's identity and laundering money for CC-3 through U.S. bank accounts before the proceeds were wired abroad for CC-3 and CC-3's clients. After the Cryson accounts were closed and CLAYTON and CC-3 abandoned Cryson, CLAYTON opened at least 12 bank accounts at five different banks (not JP Morgan and Bank of America) in the names of these four companies for CC-3, and over the course of approximately one year, those accounts received approximately $30 million.

67. Public records show that on or about September 8, 2020, CLAYTON incorporated Providence Sanitizer in Rhode Island.

68. Bank records show that soon after Providence Sanitizer's incorporation, CLAYTON opened several bank accounts at various banks in the company's name. For example, on or about September 21, 2020, CLAYTON opened several bank accounts in the name of Providence Sanitizer at a Citizens Bank branch in Massachusetts. CLAYTON later opened additional accounts in the name of Providence Sanitizer at different banks. For example, on or about May 13, 2021, CLAYTON opened a Navigant checking account in the name of Providence Sanitizer (the "Providence Sanitizer Navigant Account") at a branch in Rhode Island. In opening these accounts, CLAYTON listed himself as the "President" of Providence Sanitizer, and he listed himself as the sole authorized signatory on the account. CLAYTON did not indicate that any foreign persons owned, controlled, or directed any part of Providence Sanitizer's purported business.

69. Based on my review of bank records, the Providence Sanitizer accounts that CLAYTON opened frequently received large wire transfers and deposits of cash and money orders from individuals in the United States. These transfers and deposits had no legitimate business purpose because, as explained below, Providence Sanitizer was not a real company. In the bank records that I reviewed, I could not identify any bona fide commercial transactions, such as for payroll, services, lease payments, or purchases of supplies or inventory. CLAYTON told CC-3 that the company purported to sell hand sanitizer through distributors in the United States. The bank records for Providence Sanitizer do not include any transactions consistent with that line of business. Instead, the bank records show that shortly after the incoming wire transfers and deposits, the funds were transferred from CLAYTON's accounts to bank accounts abroad. In total,

CLAYTON opened and operated at least four bank accounts in the name of Providence Sanitizer for CC-3, which received and laundered at least $16.8 million.

70. On or about January 8, 2018, CLAYTON incorporated Sustainable Agriculture in Delaware.

71. As with Providence Sanitizer, CLAYTON opened several bank accounts at various banks in the name of Sustainable Agriculture on behalf of CC-3. For example, on or about September 30, 2020, CLAYTON opened several bank accounts in the name of Sustainable Agriculture at a Citizens Bank branch in Massachusetts. CLAYTON later opened additional accounts in the name of Sustainable Agriculture at different banks. For example, on or about May 25, 2021, CLAYTON opened a Navigant checking account in the name of Sustainable Agriculture at a branch in Rhode Island. In opening these accounts, CLAYTON listed himself as the "President" of Sustainable Agriculture, and he listed himself as the sole authorized signatory on the account. CLAYTON did not indicate that any foreign persons owned, controlled, or directed any part of Sustainable Agriculture's purported business.

72. Based on my review of bank records, the Sustainable Agriculture accounts that CLAYTON opened frequently received large wire transfers and deposits of cash and money orders from individuals in the United States. These transfers and deposits had no legitimate business purpose because, as explained below, Sustainable Agriculture was not a real company. Shortly after the incoming wire transfers and deposits, the funds were transferred from CLAYTON's accounts to bank accounts abroad. In total, CLAYTON opened and operated at least four bank accounts in the name of Sustainable Agriculture for CC-3, which received and laundered at least $6.9 million in proceeds.

73. After the closure of Cryson's bank accounts and CLAYTON's and CC-3's decision to abandon that shell company, on or about September 28, 2020, CLAYTON told CC-3 that he had set-up two shell companies, Providence Sanitizer and Sustainable Agriculture, and was in the process of opening new bank accounts to continue the scheme. CLAYTON wrote an e-mail to CC-3 telling him about the fake business purposes of the shell companies: "Finally after months of work and changes in banks three times, together with changes to the incorporations, we have finally arrived at the moment where we can begin testing . . . We have set up two corporations: 1) Providence Sanitizer Inc . . . sells hand sanitizers through distributors, located throughout the United States; 2) Sustainable Agriculture Technology Inc. . . . sells organic fertilizers and micro algae products through distributors." As with Providence Sanitizer, the bank records for Sustainable Agriculture do not contain transactions consistent with a bona fide business that distributed fertilizers and algae.

74. As to Sustainable Agriculture, which CLAYTON incorporated in 2018, CLAYTON wrote to CC-3: "This is a corporation we have owned for a while, and was recently resuscitated." Attached to the e-mail, CLAYTON provided CC-3 with instructions about how co-conspirators could deposit or transfer proceeds into the bank accounts for these two companies, including wire transfers, money orders, cash deposits, checks, and Stripe payments. As to Stripe, which is an online payment processor for retailers, CLAYTON proposed that he could provide a fake invoice from Providence Sanitizer and Sustainable Agriculture to justify the payment. CLAYTON told CC-3 that remote cash and money order deposits would "raise flags for US banks," and directed all cash and money orders to be mailed to him for deposit.

75. In response to CLAYTON, CC-3 asked why CLAYTON was incorporating two new companies rather than the one to replace Cryson: "What is the use of two companies

[Providence Sanitizer and Sustainable Agriculture] you opened?" CLAYTON replied via e-mail, on or about October 5, 2020: "We chose two companies to spread the load a little in case there are large volumes of cash involved. It also provides a safety valve if one of the accounts get suspended." Based on my training and experience, I know that persons laundering money often divide criminal proceeds among multiple entities and accounts to limit the volume and value of potentially suspicious transactions and therefore to disguise and to conceal the nature of underlying illicit activity.

76. Further, on or about October 5, 2020, CC-3 asked CLAYTON about how they would execute the outgoing foreign wire transfers and how to justify such wires in response to inquiries from banks: "How can we transfer money internationally . . . like what answers we will reply to bank on such transfers?" On or about the same day, CLAYTON replied with instructions on how to send the proceeds of the scheme abroad while minimizing the risk of detection by banks and law enforcement: "We recommend more than one account for wires out. The accounts should resemble the industry of each of the participants i.e. chemical company for [Providence] Sanitizer, and agriculture for [Sustainable Agriculture] Technology."

77. As set forth above, CLAYTON agreed to launder additional proceeds for CC-3, and "spread the load" away from accounts in the name of Providence Sanitizer and Sustainable Agriculture, by incorporating additional shell companies.

78. On or about January 11, 2021, CLAYTON incorporated Farmers Market in Rhode Island.

79. Soon after the company's incorporation, CLAYTON opened several bank accounts at various banks in the company's name. For example, on or about January 19, 2021, CLAYTON opened several bank accounts in the name of Farmers Market at a Citizens Bank branch in

Massachusetts. CLAYTON later opened additional accounts in the name of Farmers Market at different banks. For example, on or about March 15, 2021, CLAYTON opened a TD Bank account in the name of Farmers Market at a branch in Rhode Island. In opening these accounts, CLAYTON listed himself as the "President" of Farmers Market, and he listed himself as the sole authorized signatory on the account. CLAYTON did not indicate that any foreign persons owned, controlled, or directed any part of Farmers Market's purported business.

80. Based on my review of bank records, the Farmers Market accounts that CLAYTON opened frequently received large wire transfers and deposits of cash and money orders from individuals in the United States. These transfers and deposits had no legitimate business purpose because Farmers Market was not a real company. Shortly after the incoming wire transfers and deposits, the funds were transferred from CLAYTON's accounts to bank accounts abroad. In total, CLAYTON opened and operated at least three bank accounts in the name of Farmers Market for CC-3, which received and laundered at least $4.7 million in proceeds.

81. As the volume of transactions in these accounts increased, CLAYTON expressed concern to CC-3 about the risk of detection and proposed opening additional bank accounts and incorporating yet another shell company. For example, on or about February 6, 2021, CLAYTON sent a WhatsApp message to CC-3 telling him that they had "processed" $4.3 million for two of the shell companies in the previous three months, and asked "how big is this going to get? . . . and we are adding a third company. Does this mean total for the year of [$]25m?" CC-3 replied: "Almost if we won't have problem till year [end]. I want to continue as much as we can."

82. On or about February 10, 2021, CLAYTON notified CC-3 that a victim had reported being defrauded into sending money to one of CLAYTON's accounts in the name of Providence Sanitizer at Citizens Bank. He wrote: "Tread carefully my friend. Just spoke to the

Citizens Fraud team. . . . We need to return the wire asap." On or about the same day, CC-3 asked CLAYTON for the online banking login information to authorize outgoing wire transfers: "Pls give access for farmers purveyors inc in our citizen login."

83. CLAYTON expressed concerns to CC-3 that it was becoming difficult to justify the number of outgoing wires from the Providence Sanitizer accounts using a cover story of paying "suppliers." To minimize the risk of detection and account closure, CLAYTON then proposed creating a new corporation in the "trade association" industry for CC-3. On or about February 11, 2021, CLAYTON sent CC-3 a WhatsApp message: "The new plan is designed to provide a better explanation of the number of wires." For example, as to Providence Sanitizer, CLAYTON wrote: "As a distributor of Sanitizers, there should not be so many different suppliers. . . . We need a better story to cover the number of wire transfers to a large number of suppliers." CLAYTON wrote: "Using the trade association was the answer."

84. On or about the same day, CLAYTON proposed re-using the Cryson name in a WhatsApp message to CC-3. CC-3 responded: "Don't use Cryson, use some other name." CLAYTON replied: "Ok. Will work on the name . . . all of it is just for show to justify all the wires." CLAYTON then asked CC-3: "How about XiM Trade Inc. a company providing benefits to traders. . . . the new structure should allow you to scale to [$]50m USD per annum." CC-3 responded: "Superb!!"

85. On or about February 25, 2021, CLAYTON told CC-3 via e-mail that he had opened another bank account for Providence Sanitizer: "We have been working on this solution for a while. Yesterday we travelled interstate to meet with bankers @ Wells Fargo in the state of Connecticut. They have no local branches in Rhode Island. We opened an account with them for Providence Sanitizer Inc."

86. On or about the same day, CLAYTON e-mailed CC-3, "This is a proposal to cover the cost of establishing XIM Trade account and the Wells Fargo account . . . In view of our relationship, we are prepared to offer the following: 1) Setup = 2,500 USD in total for both setups…2) Monthly fees = 1,500 USD in total for both . . . If you are OK with this we will deduct the setup fees and start work on XIM Trade Inc." CC-3 expressed some hesitation about creating another corporation without a fee reduction for outgoing international wire transfers: "How we will justify XIM for all the wires and reduction of wire fees?" On or about February 27, 2021, CLAYTON explained, "We need XIM to justify all the wires going to different people . . . ." CLAYTON further wrote: "The volumes are increasing and we need to do XIM to ensure that the story holds and we can handle the volume."

87. On or about March 1, 2021, CC-3 agreed to CLAYTON's proposal and wrote, "Craig, if you are insisting so much on this part, then please make it sure [*sic*] our wire charges get reduced."

88. On or about March 11, 2021, CLAYTON incorporated XIM in Rhode Island. XIM is a shell company with no U.S. office, employees, business, customer base, or revenue. On or about March 12, 2021, CLAYTON sent CC-3 a message via WhatsApp: "We should plan on additional banks for ProSan [Providence Sanitizer], SAT [Sustainable Agriculture] and FMP [Farmers Market] to spread the load."

89. Based on a review of documents and communications seized pursuant to search warrants, I know that CLAYTON and CC-1 frequently communicated by their Rochart e-mail accounts, and that CC-1 frequently executed banking deposits and withdrawals on behalf of CLAYTON and Rochart. For example, on or about May 26, 2021, CLAYTON e-mailed Navigant to notify the bank that CC-1 would be depositing a cashier's check payable to Sustainable

Agriculture and withdrawing a cashier's check from the same Navigant Sustainable Agriculture account payable to XIM.

90. On or about March 1, 2021, CC-3 e-mailed CLAYTON to tell him that he would be receiving seven checks via mail payable to various shell companies that CLAYTON had set-up for CC-3. CC-3 directed CLAYTON to deposit the checks "not altogether." CLAYTON forwarded CC-3's email to CC-1, who directed CLAYTON: "We need to deposit on check date."

91. On or about March 20, 2021, CLAYTON sent CC-3 a WhatsApp message to tell him that he had received concerns from a bank regarding certain transactions: "We have an account review coming up on Monday. Pray for us that things go well. . . . We are sure that the current volume will be the subject of some discussion. We will be sticking to the XIM story to explain the big checks." CC-3 replied: "I feel you will manage it by XIM story is good option." Further, on or about April 11, 2021, CLAYTON told CC-3 in a WhatsApp message: "With [t]he right storyline and my ownership of XIM there should be no problem."

92. On or about March 29, 2021, CC-3 e-mailed CLAYTON to ask "who has complete knowledge of our business transactions and deals" and "who is the one who takes charge . . . in case of your absence." On or about the next day, CLAYTON responded: "My wife is involved in the business . . . she does all the banking and knows what is going on." CC-3 replied to CLAYTON that it was "nice to hear" that CC-1 "has complete knowledge of our business" and asked CLAYTON to introduce him to CC-1. On or about the same day, CLAYTON e-mailed CC-3, copying CC-1 at her Rochart e-mail address, to introduce her: "This is an introduction to my wife . . . She currently assists me in the practice as an Executive Account Manager and Banking Specialist. Her position is equivalent to a partner." On or about the same day, CC-1 responded to CC-3: "Please let me know how I may be able to help."

93. On or about March 31, 2021, CLAYTON and CC-3 discussed, via WhatsApp, meeting in Singapore to discuss business. CLAYTON told CC-3 that he "had clients and banking connections there."

94. On or about April 14, 2021, CLAYTON sent CC-3 a WhatsApp message: "How big is this going to get? We are currently averaging 300-400k per working day = 80m++ per annum." CC-3 responded: "If you want to increase we can go up to USD 1m daily transfers but than [sic] it will be very risky if not planned properly." CLAYTON replied: "Before we go to 1m per day, I will have to fly to Dubai to meet you, so we can talk." CC-3 told CLAYTON: "Dubai is open and there is not any risk."[2]

95. On or about April 16, 2021, CLAYTON told CC-3 via WhatsApp that PNC Bank had placed a hold on one of CLAYTON's accounts in the name of Sustainable Agriculture. CC-3 responded: "What about the money stuck in accounts, it's USD 180k around!!" CLAYTON replied that he would attempt to resolve the hold, stating: "If it was easy – everyone would be doing it."

96. On or about April 21, 2021, CLAYTON notified CC-3 via WhatsApp that Wells Fargo was closing one of their accounts in the name of Providence Sanitizer due to "multi-state cash deposits" that were indicative of fraud. CLAYTON proposed opening an account in the name of XIM to replace the Providence Sanitizer account, but CC-3 responded: "Even if they open what is the guarantee they won't close that also."

97. CC-3 encouraged CLAYTON to explore smaller banks with less stringent anti-money laundering controls. For example, on or about April 21, 2021, CC-3 told CLAYTON via

[2] On or about March 31, 2021, CLAYTON told CC-3, via WhatsApp, that he may have to "run away to Dubai" due to his banking activity.

WhatsApp that "big banks create[] more problems," and on or about the next day wrote, if they continued to use accounts at larger banks, "USA revenue team will come to our door, big banks will find potential crime in it. I feel only small regional banks we can do such things, big banks understand that we don't even have company websites and we are doing business in millions…" CLAYTON responded on or about April 22, 2021 that even smaller banks were raising compliance and anti-money laundering issues: "We have had trouble with all the Citizens accounts except FMP [Farmers Market]. First was ProSan [Providence Sanitizer], then SAT [Sustainable Agriculture], now Rochart. We need to slow things down, ride out the storm, and plan for a better way."

98. As banks began to close CLAYTON's accounts in the name of Providence Sanitizer, Farmers Market, and Sustainable Agriculture, and before he was able to open a bank account in the name of XIM, CLAYTON directed CC-3 to have proceeds laundered through bank accounts in the name of Rochart itself. For example, on or about May 10, 2021, CLAYTON told CC-3 via WhatsApp: "Looks like the 40k transfer to SAT [Sustainable Agriculture] will stick. We should setup the Rochart [outgoing] wires and we will transfer from SAT to Rochart and send the wires this morning . . . Do not send more deposits for ProSan [Providence Sanitizer] or SAT. We have no way of depositing them. Rochart and FMP [Farmers Market] are OK."

99. On or about May 10, 2021, CLAYTON sent a message to CC-3 via WhatsApp: "Bad news. Received mail this morning that Citizens is closing all accounts." CLAYTON told CC-3: "We have been approved for Navigant so, we will open ProSan [Providence Sanitizer] and SAT [Sustainable Agriculture] with them." Later the same day, CLAYTON opened a TD Bank checking account in the name of XIM (the "XIM TD Account") at a branch in Rhode Island. In opening the account, CLAYTON listed himself as the "Owner" of XIM, and he listed himself as

the sole authorized signatory on the account. CLAYTON did not indicate that any foreign persons owned, controlled, or directed any part of XIM's purported business.

100. Two days later, on or about May 12, 2021, CC-3 asked CLAYTON via WhatsApp, "[W]ill it be safe depositing money orders one shot 50k in [TD] bank for you the way you did in citizen[s] or will you do in parts[?]" CC-3 told CLAYTON that deposits above $10,000 would attract "attention." CLAYTON responded, "Will probably split it up and go to more than one TD branch." Based on my experience and training, I understand CLAYTON to have indicated that he would structure transactions specifically to avoid detection of the ongoing money laundering scheme.

101. On or about May 14, 2021, CLAYTON sent a WhatsApp message to CC-3 to tell him that Wells Fargo was investigating a $9,000 fraudulent transfer into an account in the name of Providence Sanitizer. CLAYTON wrote: "We have to return 9k from the WF account. . . . This needs to be done quickly to avoid trouble with the FBI."

102. Meanwhile, CLAYTON charged CC-3 thousands of dollars per month for executing the laundering scheme, and CLAYTON was compensated by directly withdrawing funds from the accounts of the shell companies. For example, on or about June 1, 2021, CLAYTON sent CC-3 a message via WhatsApp: "Fees for this month will be 4,000 USD, reflecting the extra work we are involved in. From which account would you like us to take it?" CC-3 responded: "Take from Navigant SAT [Sustainable Agriculture]." On or about July 12, 2021, CLAYTON asked CC-3 via WhatsApp: "Fees. Our fees for this month = 4,000 USD. Which account do you want us to draw from." CC-3 responded: "Providence Navigant."

103. On or about June 4, 2021, CC-3 asked whether they would continue to use Farmers Market accounts in the future. CLAYTON told CC-3, via WhatsApp: "Focus on XIM . . . it is the

best storyline for the circumstances." Six days later, on or about June 10, 2021, CLAYTON told CC-3 via WhatsApp: "May need to close FMP [Farmers Market]—the storyline is not holding up. Everything good with XIM." Further, on or about June 23, 2021, CLAYTON sent CC-3 a WhatsApp message: "FMP [Farmers Market] TD too many questions. No questions about XIM."

104. On or about July 17, 2021, CLAYTON told CC-3 via WhatsApp: "At the moment we are banned from five banks . . . we are running out of banks locally." CC-3 responded: "We can form new company and then start again with these banks." CLAYTON replied: "We are banned not the company. Anything associated with me is banned . . . working on another solution."[3] As set forth further below, there is probable cause to believe that the "solution" to using banks that CLAYTON referenced was using online payment processors, such as Stripe.

Victim-3 and CLAYTON's False Statements to Law Enforcement and Banks

105. Victim-3 was the victim of an elder fraud scheme who was induced under false pretenses to send money to the Providence Sanitizer Navigant Account opened by CLAYTON and to whom CLAYTON ultimately returned money from the XIM TD Account. Victim-3 is a resident of California. Specifically, Victim-3 was targeted by a series of telephone scams. After Victim-3 was initially defrauded of several thousand dollars, he was contacted by an individual posing as an FBI agent. The purported FBI agent told Victim-3 that he could help Victim-3 capture the fraudsters who had previously targeted him, in exchange for a down payment.

106. On or about June 29, 2021, Victim-3 withdrew a $190,000 cashier's check from a Bank of America account in his name. As directed by the purported FBI agent, Victim-3 made

[3] On or about April 2, 2021, CLAYTON e-mailed CC-2 to notify him that a Rochart client had "attracted the attention of the fraud department," and that the client's account with Bank of America would soon be closed. CLAYTON further told CC-2: "We should offer to open an account for him [the client] with another bank (for free) and transfer management to [CC-1]."

the check payable to Providence Sanitizer, and he sent the check via FedEx to the Clayton Residence in Cranston, Rhode Island. The purported FBI agent told Victim-3 that CLAYTON was an attorney assisting him with the "investigation" into the return of Victim-3's money.

107. On or about July 2, 2021, CC-3 sent CLAYTON a WhatsApp message with a photograph of the $190,000 check, and wrote, "you have got cashier check of 190k, please deposit in Navigant today."

108. On or about July 2, 2021, as captured by Navigant security cameras, CLAYTON deposited Victim-3's $190,000 cashier's check into the Providence Sanitizer Navigant Account via a drive-up ATM, with his spouse CC-1 in the passenger seat:

109. On or about July 21, 2021, upon receiving a report of the fraudulent $190,000 cashier's check, a police detective contacted CLAYTON by telephone. CLAYTON answered the phone and confirmed his identity. The detective informed CLAYTON that he was investigating a reported fraud incident involving Victim-3. CLAYTON confirmed that he operated his business, Rochart, from the Clayton Residence, and that Providence Sanitizer was one of the businesses for which he provided services. When asked about the $190,000 cashier's check, CLAYTON said the money was for a large order of sanitizers. When asked for additional information, such as an invoice, to support the sanitizer order, CLAYTON told the detective that there was no invoice because the sanitizer order was placed by phone. During a subsequent call the same day, CLAYTON told the detective that he would reimburse Victim-3. Navigant froze CLAYTON's accounts, including the Providence Sanitizer account.

110. On or about July 21, 2021, CLAYTON e-mailed the detective asking how long the investigation would take and said: "If these investigations take months, then I have [to] do some serious restructuring of my personal and business finances." In response to the detective's request for an invoice reflecting a purported $190,000 sanitizer order that Victim-3 placed, CLAYTON wrote: "I have reached out to the contractor in the Philippines who handles the orders, and the Chinese supplier. Neither of them want to cooperate at this point."

111. On or about July 21, 2021, CLAYTON sent a WhatsApp message to CC-3 to notify him of Victim-3's report of fraud and the inquiry from law enforcement. CLAYTON told CC-3: "We have a problem. The only way to fix this is to return the money. We need to do so asap."

112. The following day, CLAYTON sent via UPS a $190,000 cashier's check to Bank of America for the benefit of Victim-3. The UPS packaging slip showed a return address for CLAYTON at the Clayton Residence. The cashier's check was drawn from the XIM TD Account,

not a Providence Sanitizer account. CLAYTON told CC-3 via WhatsApp: "Will draw funds from XIM TD."

113. On or about the same day, CLAYTON sent CC-3 a WhatsApp message about the false cover story he gave the agent: "Ok funds returned. Story is [Victim-3] ordered sanitizers and then changed his mind. Order cancelled. Please ensure your client follows this line . . ." Meanwhile, CLAYTON expressed his willingness to continue working for CC-3, writing: "Working through the police issues today. Will handle wires later." CLAYTON and CC-3 agreed that CLAYTON would attempt to convince Navigant to unfreeze their accounts using the false cover story.

114. On or about July 23, 2021, CLAYTON spoke with a Navigant security manager and attempted to provide the false cover story as grounds for releasing the funds in his accounts. CLAYTON told the Navigant employee that Victim-3 placed a $200,000 sanitizer order by calling an answering service for Providence Sanitizer in the Philippines and ordering "200,000 units" of sanitizer stock.

115. On or about July 26, 2021, CLAYTON spoke with a second Navigant employee and attempted to provide another false cover story. He told the employee that a "new vendor" of Providence Sanitizer that he contracted with inadvertently sent the money to him from Victim-3.

116. On or about July 31, 2021, with the Navigant accounts controlled by CC-3 and CLAYTON still frozen due to the fraud targeting Victim-3, CC-3 asked CLAYTON via WhatsApp for a status update from law enforcement and Navigant. CLAYTON asked CC-3 to find "dirt" on Victim-3: "Nothing moving there. Do we have any dirt on [Victim-3] we [can] use to distract the police?" CLAYTON added: "The police are taking too much interest in our business . . . need something."

117. On or about August 2, 2021, CC-3 again asked, via WhatsApp: "Any news on Navigant?" CLAYTON responded, via WhatsApp message: "Nothing. I need dirt on [Victim-3]." CLAYTON again expressed concern to CC-3 that law enforcement was "digging into our business."

118. During a subsequent call with CLAYTON on or about August 4, 2021, the detective asked CLAYTON why Victim-3's money was returned from an account in the name of XIM, rather than Providence Sanitizer. CLAYTON responded that Providence Sanitizer and XIM are "different companies that do different things," but that CLAYTON is the sole owner of both companies, which according to him, had no foreign owners or investors. CLAYTON stated that he operated both companies from the Clayton Residence, and that he occasionally processed Providence Sanitizer payments through the XIM TD Account "because wire transfers are easier through TD [Bank] and really difficult at Navigant."

119. On or about the same day, CLAYTON sent a WhatsApp message to CC-3, notifying him that law enforcement's investigation was "getting serious," and stating that he may need "support" from CC-3 and other co-conspirators.

120. Two days later, on or about August 6, 2021, CLAYTON told CC-3 via WhatsApp that he "moved funds from XIM for safekeeping" because he was concerned that law enforcement "may freeze this account." He told CC-3, "I am hiring a lawyer to defend me," and told CC-3 that he may need him and co-conspirators to "chip in to cover his fees."

121. On or about the same day, CLAYTON told CC-3 via WhatsApp that they needed to be cautious continuing the scheme: "We are taking things very slowly until this is sorted out."

122. On or about August 17, 2021, CLAYTON expressed concern to CC-3 that law enforcement was investigating why CLAYTON attempted to refund Victim-3's fraudulent check

from XIM, rather than Providence Sanitizer, when law enforcement contacted him. He wrote, via WhatsApp: "I am concerned that that the police may place a freeze on XIM Trade, because that is where the [Victim-3] refund came from, and they know it."

123. On or about the same day, CLAYTON sent CC-3 a retention agreement with the criminal defense lawyer that he initially hired to defend him. Via WhatsApp, CLAYTON told CC-3: "See attached from attorney. Be careful how you spread this around. In the wrong hands, it would be dangerous for us."

124. As the law enforcement investigation continued, CLAYTON discussed with CC-3 creating fake purchase orders and supply invoices for Providence Sanitizer that would justify the deposits, incoming wires, and outgoing wires. For example, on or about August 21, 2021, CLAYTON told CC-3 via WhatsApp: "We need documentation—payments in, wire out, that includes an element of sanitizers. Let's move to Signal. WhatsApp can be tapped." Based on my training and experience, I know that Signal is a mobile instant messaging application that is end-to-end encrypted and provides users with the option to have "disappearing" messages (messages that auto-delete after they are read).

125. On or about September 30, 2021, CLAYTON and CC-3 discussed, via the encrypted messaging application Signal to which they transitioned their conversation—due to CLAYTON's concern that WhatsApp could be "tapped"—hiring an "in your face NY attorney" to "shak[e] the trees" and convince the banks to release some of the money that CLAYTON was laundering for CC-3 through Providence Sanitizer and the other shell companies' bank accounts.

The Undercover Calls

126. On or about May 18, 2021, an undercover IRS-CI agent, posing as a representative of foreign nationals who were seeking assistance in opening bank accounts in the United States, placed a consensually recorded phone call to CLAYTON's cell phone number, ending in -3818.

127. The undercover agent introduced himself to CLAYTON. CLAYTON offered his services, stating, in substance, that the first step would be for him to form U.S. limited liability companies or corporations on behalf of the foreign nationals. CLAYTON stated that he was experienced in and willing to "set-up a company owned by [him], but controlled by the client." CLAYTON told the undercover agent that he knew certain banks that were "not as stringent" with respect to anti-money laundering regulations, but that many banks "make it quite difficult" because they "don't like foreign-owned LLCs." CLAYTON said one bank's compliance "requirements" included "need[ing] to know who the person is that actually owns the account," which "puts [CLAYTON's] clients off."

128. CLAYTON further explained his process to the undercover agent, stating that "we incorporate a company, set-up a bank account, advise the client, and the money starts rolling." When asked what information CLAYTON would need from the foreign nationals to incorporate the companies and open the accounts on their behalf, he said, "I don't need anything from you at all." CLAYTON also stated, in substance, that he did not want to be responsible for the outgoing wire transfers from the accounts he opened. Accordingly, he said his practice was to give foreign individuals access to the online banking accounts, although he would remain the "sole signer on the account," because banks do "not allow us to delegate signing authority" to foreign nationals. CLAYTON warned the agent that the clients should refrain from making too many cash deposits into the accounts, so as not to draw attention, and that the "biggest single risk in U.S. banking at

the moment is cash." CLAYTON told the agent that he charged clients a minimum of $1,000 per month, up to a maximum of $5,000 per month for clients "moving" $1 million per month, adding, "by the way, we do have clients moving that much."

129. On or about May 21, 2021, the undercover agent placed a second consensually recorded telephone call to CLAYTON. The undercover agent and CLAYTON discussed setting up an in-person meeting in order to further explore CLAYTON creating corporations and opening bank accounts for the agent's clients. During the call, CLAYTON gathered background information from the undercover agent. In doing so, CLAYTON asked whether the agent or any of his family members "were associated with law enforcement." CLAYTON added, "We don't deal with anyone who has law enforcement connections." CLAYTON further asked the agent whether any of his clients were fugitives from justice. CLAYTON stated, "Believe me, I have had two or three clients who were."

130. In or about July 2021, prior to setting up an in-person meeting, CLAYTON sent the undercover agent a message via the encrypted messaging application WhatsApp. CLAYTON wrote, "I am not able to take on any new clients at the moment. I will contact you when the situation clears. Looking at 2-3 month delay."

131. Based on the timing of the events, I believe the "situation" referred to by CLAYTON involved the investigation of the fraud targeting Victim-3, as discussed above.

***

132. In total, CLAYTON created at least five different shell companies for CC-3 in the United States, and opened and managed at least 14 bank accounts, through which CLAYTON, CC-3, and others laundered more than $35 million.

C. CLAYTON's False Statements to Federal Agents and Use of Stripe

133. In or about January 2022, accompanied by counsel, CLAYTON met with federal agents pursuant to a standard proffer agreement with the United States Attorney's Office in Boston. At that meeting, CLAYTON was informed that he would likely face federal money laundering charges. Law enforcement also warned him that lying to or seeking to mislead federal agents is a crime. Nevertheless, despite knowing that proceedings to charge him with federal crimes were possible and being warned not to lie to agents, CLAYTON made several materially false statements. For example, CLAYTON told federal agents that he directed CC-3 to switch their communications to Signal because he was worried his WhatsApp communications were being "tapped" by competitors, not by law enforcement. Further, CLAYTON initially denied ever misleading banks or members of law enforcement about CC-3's accounts, but later admitted that he did mislead them but only because they "would not understand" his business.

134. There is probable cause to believe that CLAYTON, subsequent to that proffer, has continued to launder funds for Rochart clients. For example, CLAYTON has a Stripe account for a purported custom, casual apparel business Cozy based in Delaware. The mailing address for Cozy's Stripe account is the Clayton Residence. Stripe is a payment services provider that allows merchants to accept credit and debit cards on the internet. From in or about March 2022 (shortly after his proffer with law enforcement agents) through in or about November 2022, this account has authorized more than $5.5 million in purported orders from individuals within the United States for Cozy apparel, a significant increase in volume from prior to that period. These payments often occurred minutes apart and originated from the same payors, which based on my training and experience, is indicative of one individual running card payment details programmatically, and is not consistent with a retail merchant's expected business activity. For example, on or about

October 6, 2022, within a span of two minutes, one individual using a unique Stripe payor identifier (but 11 different names) made 11 different purported purchases of Cozy apparel, all for $255.94. Four days later, on or about October 10, 2022, within a span of minutes, one individual using the same unique Stripe payor identifier (but 10 different names) made 10 different purchases of Cozy apparel, all for $255.94. Further, hundreds of the transactions executed by the Cozy Stripe account have been reported to Stripe as fraudulent. Additionally, records from Stripe indicate that while the Stripe account is registered in the name of CLAYTON at the Subject Premises in Rhode Island, the overwhelming majority of IP addresses that have been used to access the Cozy Stripe account originate in Vietnam. Collectively, these facts are consistent with CLAYTON substituting the use of Stripe for bank accounts to execute a similar money laundering scheme.

PROBABLE CAUSE TO BELIEVE THE SUBJECT PREMISES CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES

135. I have probable cause to believe that the Subject Premises, as described in Attachment A to the proposed warrant, contains fruits, evidence, and instrumentalities of the Target Offenses, as described in Attachment B.

136. As summarized above, the fraud targeting Victim-3 demonstrates that there is probable cause to believe that the Clayton Residence contains evidence, fruits, and instrumentalities of the Target Offenses. Victim-3 was directed to mail his $190,000 check to the Clayton Residence. Further, CLAYTON has listed the Subject Premises as the address for many of the bank accounts he opened, including on behalf of CC-3, and the Subject Premises is the address for the Cozy Stripe account.

137. Based on my training and experience, I know that locations occupied by a target often contain evidence that will aid in establishing the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the government to establish and prove

each element or alternatively, to exclude the innocent from further suspicion. Accordingly, I believe that it is likely that the Subject Premises, the Clayton Residence, will contain evidence of the Target Offenses, including without limitation, bank account opening documents, monthly statements, debit cards, ATM and banking receipts; documents concerning the formation of various shell companies; computers and telephones used to communicate with co-conspirators; and cash.

138. Although a number of months have passed since some of the bank accounts discussed above have been active and since a search warrant was previously executed at the Subject Premises, I believe that evidence of the Target Offenses will nevertheless be found at the Subject Premises due to, in part, CLAYTON's continued activity in processing funds via Stripe. As discussed below, I expect that cellular phones and/or computers owned and used by CLAYTON will contain evidence of the Target Offenses, and in my experience, cellular phones and computers are typically found where targets reside. Further, targets tend not to discard computers and cellular phones in my experience, and even if they do, targets frequently "backup" their computers and cellular phones to new devices, the cloud, or external hard drives, which may be found at the Subject Premises.

139. Based on my training and experience, individuals who perpetrate fraudulent schemes and/or launder the proceeds also keep ledgers of proceeds, similar to drug traffickers, that often are found where they reside.

140. As discussed below, I have probable cause to believe that evidence of the Target Offenses will be found on cell phones used by CLAYTON and CC-1. Based on my training and experience, users of cell phones typically carry such devices on their person, even when in their residences, and this warrant authorizes the search of all such devices in the Subject Premises.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

141. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

142. Based on my training, experience, and information provided by other law enforcement officers, I also know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

143. I am aware of a report from the United States Census Bureau that shows that in 2016, among all households nationally, 89 percent had a computer, which includes smartphones, and 81 percent had a broadband Internet subscription. Specifically, in 2016, when the use of smartphone ownership was measured separately for the first time, 76 percent of households had a smartphone and 58 percent of households had a tablet, and 77 percent of households had a desktop or laptop computer. Further, according to the Pew Research Center, as of 2019, 96 percent of adult Americans own a cell phone, and 81 percent own a cell phone with significant computing capability (a "smartphone").

144. From my training and experience, I am aware that personal computer systems are generally capable of creating, receiving, and otherwise processing computer files generated at or to be used at a business, such as e-mail, word-processing documents, photographs, and spreadsheets.

145. Here, as set forth *supra*, CLAYTON and CC-1 used e-mail to communicate with CC-3 and CC-2.

146. Further, CLAYTON used his cell phone, which is a smartphone, to communicate with the undercover agent. After his initial call with the undercover agent, CLAYTON began to communicate with the undercover agent via WhatsApp, an encrypted messaging application available on smartphones. CLAYTON communicated with the undercover agent via WhatsApp from in or about May 2021 through in or about July 2021, and he communicated with CC-3 via WhatsApp on a near-daily basis, exchanging several thousand messages.

147. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B in computer hardware, computer software, smartphones, and storage media.

148. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media (in particular, computers' internal hard drives) contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of

peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence

relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Finally, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

149. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence: storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements: analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system

and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, in executing the warrants, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

150. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this affidavit is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

151. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with CLAYTON, his wife CC-1, or Rochart.

152. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Investigative Team may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNLOCKING A DEVISE USING BIOMETRIC FEATURES

153. I know from my training and experience, as well as from information found in publicly available materials, that some models of cell phones made by Apple and other manufacturers offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

154. On the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to five fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ill enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in eight hours and the passcode or password has not been entered in the last six days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via

Touch ill exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

155. The passcode(s) that would unlock CLAYTON's and CC-1's cell phone(s) are not currently known to law enforcement. Thus, it may be useful to press the finger(s) of CLAYTON and CC-1 to the devices' fingerprint sensors or to hold the devices up in front of their faces in an attempt to unlock the devices for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

156. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of CLAYTON and CC-1 to the sensor of the cell phone devices described in Attachment B or to place the devices in front of their faces for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

PROBABLE CAUSE FOR SEIZURE WARRANTS

A. The Target Accounts

157. On or about July 31, 2021, Navigant froze all of the funds on deposit in the following Target Accounts opened by CLAYTON in the names of Providence Sanitizer, Sustainable Agriculture, and Rochart, Inc.

Account Name	Target Account	Account No.	Balance as of July 31, 2021
Providence Sanitizer	Target Account 1	x9165	$138,803.01
Sustainable Agriculture	Target Account 2	x4961	$72,627.50
Rochart Inc.	Target Account 3	x8962	$5,276.18
Rochart Inc.	Target Account 4	x5711	$14,660.21

158. On or about May 13, 2021, CLAYTON opened Target Account 1 in the name of Providence Sanitizer, on behalf of CC-3, at Navigant in Rhode Island. On the account opening documents CLAYTON indicated that he was the President and the only officer of the business, as well as the 100% beneficial owner. As set forth above, CLAYTON incorporated Providence Sanitizer to launder money, and the transfers and deposits into Target Account 1 had no legitimate business purpose because Providence Sanitizer was not a real company.

159. On or about May 25, 2021, CLAYTON opened Target Account 2 in the name of Sustainable Agriculture, on behalf of CC-3, at Navigant in Rhode Island. On the account opening documents CLAYTON indicated that he was the President and only officer of the business, as well as the 100% beneficial owner. As set forth above, CLAYTON incorporated Sustainable Agriculture to launder money, and the transfers and deposits into Target Account 2 had no legitimate business purpose because Sustainable Agriculture was not a real company.

160. As set forth above, CLAYTON used Rochart as a means to launder criminal proceeds for his clients under the guise of financial consulting services. On or about March 9, 2017, CLAYTON opened Target Account 3 in the name of Rochart Inc. at Navigant. On or about September 3, 2020, CLAYTON opened Target Account 4 at Navigant in the name of Rochart Inc. CLAYTON and his wife, CC-1, are the two signatories on this account.

161. Based on the foregoing, there is probable cause to believe that any and all funds on deposit in the Target Accounts represent property involved in money laundering and are subject to forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1).

B. The Target Vehicle

162. On or about September 17, 2019, CLAYTON opened a JP Morgan checking account in the name of Rochart client Teracoaster International LLC ("Teracoaster") ending in

x9256. From in or about September 2019 to July 2020, the Teracoaster JP Morgan account received approximately $338,000 in suspicious deposits and incoming wire transfers, including numerous cash deposits structured just under $10,000. Shortly after each cash deposit, an outgoing wire transfer was sent from the Teracoaster JP Morgan account to foreign bank accounts, including in Singapore and Malaysia. In an e-mail that CLAYTON sent CC-2 on or about May 10, 2020, CLAYTON listed Teracoaster as one of the "Bad Actor" clients of Rochart. On or about July 29, 2020, the Teracoaster JP Morgan account was closed due to suspected fraud and money laundering, with a balance of approximately $79,441, and on or about the same day, JP Morgan issued a cashier's check to Teracoaster for that amount, with the Clayton Residence as the listed address. On or about September 11, 2020, the $79,441 check to Teracoaster was deposited in Target Account 4 in the name of Rochart. On or about September 18, 2020, the $79,441 was transferred from Target Account 4 to Target Account 3 in the name of Rochart.

163. On or about May 21, 2020, CLAYTON purchased the Target Vehicle from a Mercedes-Benz dealership in Rhode Island, using a cashier's check from Target Account 3 for the purchase price of approximately $23,794.55. At the time of the purchase, the balance in Target Account 3 was approximately $28,142.40. CLAYTON purchased the Target Vehicle in the name of his spouse, CC-1.

164. Based on the foregoing, there is probable cause to believe that the Target Vehicle represents proceeds from property involved in money laundering and is subject to forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1).

SEIZURE AUTHORITY

165. Pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1), any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957, or 1960 of this title, or any property traceable to such property, is subject to forfeiture.

166. This Court has authority to issue a civil seizure warrant pursuant to Title 18, United States Code, Section 981(b)(2), which states that "[s]eizures pursuant to this section shall be made pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure." This Court also has authority to issue the requested criminal seizure warrant pursuant to Title 21, United States Code, Section 853(f), as incorporated by Title 18, United States Code, Section 982(b), which authorizes "the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant."

167. A restraining order, pursuant to Title 18, United States Code, Section 853(e), will not be sufficient to preserve the Target Accounts for forfeiture given the ease with which funds may move out of the accounts via wire transfer, electronic funds transfer, or otherwise, and despite best intentions, financial institutions cannot guarantee that money restrained, but not seized, will be available for forfeiture at a later time. Similarly, given the ease with which vehicles can be concealed, destroyed, or removed from the jurisdiction, based on my training and experience, a restraining order will not be sufficient to preserve the Target Vehicle for forfeiture.

168. Pursuant to Title 18, United States Code, Section 981(b)(3), and Title 21, United States Code, Section 853(l), a seizure warrant may be issued by a judicial officer in any district in which a forfeiture action against the property may be filed, and may be executed in any district in which the property is found.

CONCLUSION

169. Based on the information described above, there is probable cause to believe that CLAYTON has committed conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h) and 1956(a)(1)(B)(i), and obstruction of justice, in violation of Title 18, United States Code, Section 1512(c)(2). Further, there is probable cause to believe that that evidence, fruits, and instrumentalities of the Target Offenses (as described in Attachment B) will be found at the Clayton Residence (as described in Attachment A to the proposed respective warrant). Finally, there is probable cause to believe that the Target Assets are subject to forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1).

Respectfully submitted,

/s/ Lori Robinson

Lori Robinson, Special Agent
Department of Homeland Security

SUBSCRIBED and SWORN to telephonically in accordance with Fed R. Crim. P. 41(d)(3) on this ___ day of February 2023.

February 21, 2023

HONORABLE M. PAGE KELLEY
Chief United States Magistrate Judge
District of Massachusetts

ATTACHMENT A – THE CLAYTON RESIDENCE

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched, pictured below, is located at 52 Parkside Drive, Cranston, Rhode Island 02910. The property is a two-story, single-family residence. The number "52" is clearly displayed by the front door. The house includes a detached garage located in the back of the house. The siding is a mixture of brick and white vinyl siding. The brick covers the first floor of the house while the white vinyl siding covers the top half.

The area to be searched at the Clayton Residence includes all rooms, annexes, garages, attics, basements, porches, curtilage, mailboxes, trash containers, debris boxes, storage lockers, locked containers and safes, lockers, sheds, and any visible structures and outbuildings

associated with the Clayton Residence and shall extend into desks, cabinets, safes, briefcases, backpacks, wallets, purses, digital devices, and any other storage locations within the Clayton Residence.

ATTACHMENT B

ITEMS TO BE SEIZED

I. For the period of January 1, 2019 to the present, all records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of money laundering and conspiracy to commit money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957; obstruction of justice, tampering with and retaliating against a witness and victim, and conspiracy to commit the same, in violation of Title 18, United States Code, Sections 1512, 1513, and 371; making false statements to a federal agents, in violation of Title 18, United States Code, Section 1001; mail fraud, wire fraud, bank fraud, and conspiracy to commit the same, in violation of Title 18, United States Code, Sections 1341, 1343, 1344, and 1349; and operating an unlicensed money transmitting business, in violation of Title 18, United States Code, Section 1960 (collectively, the "Target Offenses"), including but not limited to:

A. Records and tangible objects pertaining to the following:

1. Craig CLAYTON;
2. Corazon Bautista;
3. Rochart Consulting;
4. GetBiztoUSA;
5. Providence Sanitizer; Cryson Trading; PJT International; XIM Trade, and other companies founded or owned by Craig CLAYTON;
6. Potential victims and co-conspirators in romance scams, elder fraud, and other fraudulent schemes, including the individuals identified as Victims-1 through 3 in the supporting affidavit;
7. Banking and money transfers, and the payment, receipt, transfer, or storage of

money or other things of value, including the opening of, access to, and/or use of bank accounts in the names of or associated with third persons, including bank statements, deposit tickets, deposit items, checks, money orders, cashier's checks, official checks, bank drafts, wire transfer instructions and receipts, checkbooks, check registers, passbooks, withdrawal slips, credit memos, debit memos, signature cards, account applications, automatic teller machine receipts, safe deposit box applications, safe deposit box keys, pre-paid debit and credit cards, debit and credit card statements, charge slips, receipts, financial statements, balance sheets, income statements, cash flow statements, ledgers, journals, accounts receivable, accounts payable, leases, brokerage statements, and any other items evidencing the obtaining, disposition, secreting, transfer, or concealment of assets;

8. The access and use of money service businesses, such as Western Union and/or Moneygram; online bank transfer services, such as TransferWise, Veem, Zelle, Venmo, Stripe, or Paypal; and cryptocurrency accounts and cryptocurrency exchanges, such as Bitcoin;
9. United States currency, money orders, or cashier's checks related to or obtained from fraud, and any currency counting equipment;
10. The e-mail account craig.clayton@rochartgroup.com, and all other Rochart e-mail accounts;
11. The purchase or lease of real estate, vehicles, precious metals, jewelry, or other items obtained with fraud proceeds.
12. Identification cards, driver's license cards, passports, visas, and travel

documents.

13. Communications by, between and among, and/or relating to CLAYTON and known and unknown conspirators, relating to the Target Offenses.

14. The identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators involved in the Target Offenses, including calendars, address books, telephone or other contact lists, correspondence, receipts, and wire transfer or fund disposition records, and communications relating to the same;

15. The occupancy, ownership, purchase and/or lease of the Clayton Residence;

16. The use, ownership, possession, and control of computers, tablets, cellular telephones, and/or other cellular and digital devices seized from the Clayton Residence and/or CRAIG CLAYTON and any landline telephones, internet service, or IP addresses associated with the CLAYTON Residence;

17. Accounts held with companies providing Internet access or remote storage;

B. Records and tangible objects pertaining to the payment, receipt, transfer, or storage of money or other things of value by Craig CLAYTON or Corazon Bautista,

including, without limitation:

1. Bank, credit union, investment, money transfer, and other financial accounts;

2. Brokerage accounts;

3. Tax statements and returns;

4. Business or personal expenses; and

5. Income, whether from wages or investments.

C. Records and tangible objects pertaining to the travel or whereabouts of any of the individuals listed above.

D. Records and tangible objects pertaining to the existence, identity, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above.

E. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of the attachment of other computer hardware or storage media;

3. evidence of counter-forensic programs and associated data that are designed to eliminate data;

4. evidence of when the computer equipment was used;

5. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and

F. Records and tangible objects relating to the ownership, occupancy, or use of the

premises to be searched (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers).

II. All Computer hardware, computer software, and storage media reasonably believed to contain the items described in paragraph I. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

III. During the execution of the search of the Subject Premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of Craig CLAYTON and Corazon Bautista to the sensor of any of the smartphones described above, or to hold the device(s) in front of their faces.

DEFINITIONS

For the purpose of this warrant:

A. "Computer Equipment" means any computer hardware, computer software, mobile phones, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an

encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally identifiable information of victims; or the fruits or instrumentalities of crime. For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.

Criminal Case Cover Sheet **U.S. District Court - District of Massachusetts**

Place of Offense: **Category No.** I **Investigating Agency** HSI / IRS

City Swampscott / Boston **Related Case Information:**

County Essex / Suffolk Superseding Ind./ Inf. _____ Case No. 23-6002-MPK
Same Defendant _____ New Defendant _____
Magistrate Judge Case Number _____
Search Warrant Case Number 21-2445-MBB
R 20/R 40 from District of _____

Defendant Information:

Defendant Name Craig Clayton Juvenile: ☐ Yes ☑ No

Is this person an attorney and/or a member of any state/federal bar: ☐ Yes ☑ No

Alias Name _____

Address (City & State) 52 Parkside Drive, Cranston, Rhode Island 02910

Birth date (Yr only): 1949 SSN (last4#): 6825 Sex M Race: _____ Nationality: _____

Defense Counsel if known: John Walsh Address JohnGWalshLaw@gmail.com

Bar Number 555649 617-851-2429

U.S. Attorney Information:

AUSA Ian Stearns Bar Number if applicable _____

Interpreter: ☐ Yes ☑ No List language and/or dialect: _____

Victims: ☑ Yes ☐ No If yes, are there multiple crime victims under 18 USC§3771(d)(2) ☑ Yes ☐ No

Matter to be SEALED: ☑ Yes ☐ No

☑ Warrant Requested ☐ Regular Process ☐ In Custody

Location Status:

Arrest Date 02/23/2023

☐ Already in Federal Custody as of _____ in _____.
☐ Already in State Custody at _____ ☐ Serving Sentence ☐ Awaiting Trial
☐ On Pretrial Release: Ordered by: _____ on _____

Charging Document: ☑ Complaint ☐ Information ☐ Indictment

Total # of Counts: ☐ Petty _____ ☐ Misdemeanor _____ ☑ Felony 2

Continue on Page 2 for Entry of U.S.C. Citations

☑ **I hereby certify that the case numbers of any prior proceedings before a Magistrate Judge are accurately set forth above.**

Date: 02/16/2023 Signature of AUSA: */s/ Ian J. Stearns*

District Court Case Number (To be filled in by deputy clerk): 23-6002-MPK

Name of Defendant Craig Clayton

U.S.C. Citations

	Index Key/Code	Description of Offense Charged	Count Numbers
Set 1	18 U.S.C. § 1956(h)	Conspiracy to Commit Money Laundering	1
Set 2	18 U.S.C. § 1512	Obstruction of Justice	2
Set 3			
Set 4			
Set 5			
Set 6			
Set 7			
Set 8			
Set 9			
Set 10			
Set 11			
Set 12			
Set 13			
Set 14			
Set 15			

ADDITIONAL INFORMATION: THIS CASE WOULD BE ASSIGNED TO JUDGE BOWLER UNDER THE PRIOR PROCEEDINGS RULE. THE GOVERNMENT DEFERS TO THE CLERK'S OFFICE AND THE COURT AS TO WHETHER IT SHOULD BE REFERRED BACK TO JUDGE BOWLER OR REMAIN WITH THE EMERGENCY MAGISTRATE JUDGE.