2020R00458/JHS/SER

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. Michael A. Hammer
	:	
v.	:	Mag. No. 23-10168
	:	
CHRISTOPHER JAMES SCANLON	:	**CRIMINAL COMPLAINT**
	:	

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

SEE ATTACHMENT A

I further state that I am a Special Agent with the U.S. Attorney's Office for the District of New Jersey, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Jason Annuziato, Special Agent
U.S. Attorney's Office
District of New Jersey

Special Agent Annuziato attested to this Affidavit by telephone pursuant to F.R.C.P. 4.1(B)(2)(A) on this 20th day of April, 2023.

Hon. Michael A. Hammer
United States Magistrate Judge

ATTACHMENT A
(Conspiracy to Control and Own an Unlicensed Money Transmitting Business)

From at least as early as in or around 2015 through in or around 2019, in the District of New Jersey, and elsewhere, the defendant,

CHRISTOPHER JAMES SCANLON,

did knowingly and intentionally conspire and agree with others to conduct, control, manage, supervise, direct, and own all or part of an unlicensed money transmitting business, as that term is defined in Title 18, United States Code, Section 1960(b)(1), affecting interstate and foreign commerce, and which failed to comply with the money transmitting business registration requirements under Title 31, United States Code, Section 5330 and regulations prescribed thereunder, contrary to Title 18, United States Code, Section 1960(a).

In violation of Title 18, United States Code, Section 371.

ATTACHMENT B

I, Jason Annuziato, am a Special Agent of the U.S. Attorney's Office for the District of New Jersey. The information contained in the complaint is based upon my personal knowledge, as well as information obtained from other sources, including: (a) statements made or reported by various witnesses with knowledge of relevant facts; (b) my review of publicly available information; (c) information received from other investigators; and (d) my review of evidence, including business records, bank records, and other documents. Because this complaint is being submitted for a limited purpose, I have not set forth every fact that I know concerning this investigation. Where the contents of documents and the actions and statements of others are reported, they are reported in substance and in part, except where otherwise indicated. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

1. At all times relevant to this Criminal Complaint:

a. Under Title 31, United States Code, Section 5330 and accompanying regulations, any person who owned or controlled a money transmitting business ("MTB") must have registered the business (whether or not the business is licensed as a money transmitting business in any state) with the Secretary of the Treasury not later than the end of the 180-day period beginning on the date on which the business was established. This registration is accomplished with the Financial Crimes Enforcement Network ("FinCen"), a bureau of the Treasury Department.

b. FinCen's mission was to safeguard the United States financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. FinCen carried out its mission, in part, by receiving and maintaining financial transaction data, and analyzing and disseminating that data for law enforcement purposes. FinCen was responsible, in part, for detecting and deterring financial crime.

c. Defendant Christopher James Scanlon ("Scanlon") was a United States citizen who resided in Utah and later moved to London, England. Scanlon was the President, Chief Executive Officer, and Founder of the brands Aurae Lifestyle and Club Swann. Scanlon was also the owner of PMA Media Group, Inc. ("PMA"), and, as explained herein, the indirect owner of AU Card, LLC, AU Card Ltd., and Nvayo Ltd ("Nvayo").

d. PMA was incorporated in Delaware with its principal place of business in Utah. PMA was wholly owned by Scanlon, who served as its Director. PMA directly owned AU Card, LLC and indirectly owned Nvayo, among other entities. PMA was not registered as an MTB with FinCen.

e. AU Card, LLC, which does business as "Aurae Lifestyle," and "Club Swann," was a Delaware limited liability company with its principal place of business in Utah. PMA was the sole member of AU Card, LLC. Scanlon was the Director of AU Card, LLC. AU Card, LLC is the 100% owner of AU Card Ltd. Throughout the course of the conspiracy, AU Card, LLC maintained bank accounts at several different U.S. financial institutions, including at Banks-1, -2, and -3. AU Card, LLC was not registered as an MTB with FinCen.

f. AU Card Ltd. was a pass-through entity that entered into contracts with third-parties for the benefit of Aurae Lifestyle. AU Card Ltd. was the direct owner of Nvayo, and was directly owned by AU Card, LLC. AU Card Ltd. was not registered as an MTB with FinCen.

g. Nvayo was a company registered in the United Kingdom. Nvayo was wholly owned by AU Card Ltd., which was wholly owned by AU Card, LLC, which was wholly owned by Scanlon. Nvayo maintained a license in the United Kingdom to provide e-money wallets on behalf of Aurae Lifestyle customers. AU Card Ltd. acquired Nvayo in or around August 2017. Nvayo was not registered as an MTB with FinCen.

h. Customer-1 was a resident of New Jersey and a customer of Aurae Lifestyle. In or around 2021, Customer-1 pleaded guilty to U.S. federal charges for conspiring to violate the federal anti-kickback statute and conspiring to defraud the IRS.

i. Customer-2 was a resident of California and a customer of Aurae Lifestyle. Customer-2 was previously convicted in or around 2001 of a federal charge for conspiring to engage in mail and wire fraud, which arose in connection with a long distance phone card scam. In or around 2018, the U.S. Securities and Exchange Commission ("SEC") brought a civil enforcement action against Customer-2 and his entity ("Fraud Entity-1") alleging various federal securities violations that occurred between in or around October 2015 and in or around 2017 ("Fraud Scheme-1"). The SEC alleged that Fraud Scheme-1 was a Ponzi and pyramid scheme. In or around 2023, the SEC achieved a settlement with Customer-2 and Fraud Entity-1, which required Customer-2 and Fraud Entity-1 to jointly and severally disgorge more than approximately $20 million.

j. Customer-3 was a resident of Colorado and a customer of Aurae Lifestyle. In or around December 2019, Customer-3 was charged in a federal indictment ("Indictment-1") with conspiracy to commit wire fraud in connection with a large-scale cryptocurrency mining scheme ("Fraud Scheme-2"), which took place between in or around 2014 and in or around December 2019.

k. Customer-4 was a citizen of the United States and a customer of Aurae Lifestyle. In or around December 2019, Customer-4 was charged in

Indictment-1 with conspiracy to commit wire fraud in connection with Fraud Scheme-2.

l. Customer-5 was a resident of California and a customer of Aurae Lifestyle. In or around 1997, Customer-5 was convicted of a federal charge for distributing methamphetamine, and was sentenced to a federal term of imprisonment of 145 months, followed by 5 years of supervised release. In or around December 2019, Customer-5 was charged in Indictment-1 with conspiracy to promote an unregistered security in connection with Fraud Scheme-2. In or around September 2020, Customer-5 pleaded guilty to conspiring to promote an unregistered security in connection with Fraud Scheme-2 and to subscribing to a false tax return.

m. Lawyer-1 was an attorney licensed to practice law in the State of Utah and a customer of Aurae Lifestyle. Lawyer-1 assisted Customer-3, Customer-4, and others with transmitting significant amounts of money obtained through Fraud Scheme-2, including through Lawyer-1's Aurae Lifestyle account.

n. Bank-1, Bank-2, and Bank-3 were U.S. financial institutions.

o. Cryptocompany-1 and Cryptocompany-2 had their principal places of business in Illinois and New Jersey, respectively.

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

Aurae Lifestyle

2. PMA, AU Card, LLC, AU Card Ltd., and Nvayo (collectively, the "AU Entities") operated together at Scanlon's direction to provide fiat and cryptocurrency financial services to their customers, including by transferring fiat and cryptocurrency to third parties on behalf of, and sometimes between, their customers, and liquidating cryptocurrency on behalf of their customers. The AU Entities were an MTB as that term is defined in Title 31, United States Code, Section 5330(d).

3. Scanlon conspired with others, including his Chief Legal Officer, to conduct, control, manage, supervise, direct, and own the AU Entities.

4. According to a record produced by AU Card, LLC, between in or around 2015 and in or around 2019, more than approximately 100 U.S.-based

individuals worked for the AU Entities, including a Controller and the AU Entities' General Counsel.

5. According to a consolidated balance sheet prepared for PMA and AU Card, LLC, as of approximately June 30, 2019, PMA and AU Card, LLC had assets worth close to approximately $35 million held in safeguarded savings and checking accounts.

6. The U.S. Attorney's Office for the District of New Jersey ("DNJ") and the Internal Revenue Service, Criminal Investigation ("IRS-CI") have been investigating Scanlon and others in connection with their ownership and operation of Aurae Lifestyle, a service that purported to be a concierge service but, in reality, operated as an unlicensed private bank for its customers and had operations in the United States and other foreign jurisdictions.

7. While AU Card, LLC did provide some concierge services, the AU Entities' revenue was primarily derived from providing customers with financial services. For example, in or around January 2019, Scanlon wrote and sent an email to several employees of the AU Entities, in which he stated: "It has been a business wide effort in producing a truly world class 'challenger bank' type application, with the added benefit of being able to liquidate crypto currency through our concierge arm." Scanlon touted further how the AU Entities had "[p]rocessed and maintained financial control over the many millions of dollars of member load, transfer, and wire transactions which account for over 95% of our net income."

8. Scanlon owned and controlled the AU Entities, and he acted as the primary "relationship manager" (i.e., a customer service representative) for several high-net-worth customers of the AU Entities operating under the Aurae Lifestyle brand. Scanlon often communicated with customers about financial transactions using phone messaging applications, using encrypted messaging applications.

9. Customers were charged high fees to become "members" of Aurae Lifestyle and to conduct financial transactions through their Aurae Lifestyle accounts. Aurae Lifestyle further offered a bespoke solid gold debit card to "members" at an exorbitant rate. For example:

a. In or around July 2015, AU Card, LLC issued an invoice to a customer with a listed address in New York, in the approximate amount of $60,000 for an Aurae Elite Lifestyle membership. AU Card, LLC's bank account at Bank-2 was listed at the bottom of the invoice, along with instructions to wire the funds to the Bank-2 account.

b. In or around July 2018, AU Card, LLC issued an invoice to Customer-4, with a listed address in Nevada, in the approximate amount of $28,000 for an Aurae Elite Lifestyle membership and a

14K custom yellow gold MasterCard. AU Card, LLC's bank account at Bank-2 was listed at the bottom of the invoice, along with instructions to wire the funds to the Bank-2 account.

c. In or around January 2019, AU Card, LLC issued an invoice to a trust, and also to Lawyer-1, in the approximate amount of $28,000 for an Aurae Elite Lifestyle membership and a 14K custom yellow gold MasterCard. AU Card, LLC's bank account at Bank-2 was listed at the bottom of the invoice, along with instructions to wire the funds to the Bank-2 account.

d. In or around May 2019, AU Card, LLC issued an invoice to a customer in the approximate amount of $49,500 for an Aurae Elite Lifestyle membership and a 14K custom yellow gold MasterCard. AU Card, LLC's bank account at Bank-2 was listed at the bottom of the invoice, along with instructions to wire the funds to the Bank-2 account.

e. In or around December 2019, AU Card, LLC issued an invoice to a customer in the approximate amount of $44,750 for an Aurae Elite Lifestyle membership and a 14K custom yellow gold MasterCard. AU Card, LLC's bank account at Bank-2 was listed at the bottom of the invoice, along with instructions to wire the funds to the Bank-2 account.

10. In addition to the high "membership" fees and the expensive debit cards, customers were charged significant fees to conduct fiat wire transfers, sometimes approximately 1% of the amount of the wire.

11. Aurae Lifestyle was attractive to a particular type of customer because it provided customers the ability to engage in financial transactions without immediate scrutiny or detection by U.S. financial regulators and provided customers with access to the U.S. financial system when they otherwise would be barred from obtaining a U.S. bank account. Further, and illustrative of Aurae Lifestyle's purpose, a social media account for Aurae Lifestyle promised its customers "discretion."

12. For example, Aurae Lifestyle customers were permitted to transfer money to other Aurae Lifestyle customers in a manner that would not be detected by banks or U.S. regulators unless regulators were able to obtain customer records from the AU Entities. This provided "discretion" because, at times, the AU Entities attempted to use foreign privacy laws and the location of Nvayo's registration to hide records related to its customers from U.S. regulators and law enforcement, including DNJ and IRS-CI.

13. In practice, and as highlighted in the examples below, the AU Entities used accounts at Bank-1, Bank-2, and Bank-3 to provide money transmitting services to their customers without properly registering with FinCen.

14. Records from Bank-1 reflect that between in or around January 2018 through in or around February 2019, AU Card, LLC received more than approximately $37 million from Nvayo by wire transfer into its account at Bank-1 (the "AU Bank-1 Account"), and AU Card, LLC sent approximately $24 million in wire transfers to Nvayo.

15. Records from Bank-2 reflect that between in or around January 2019 through in or around January 2020, AU Card, LLC received more than approximately $28 million from Nvayo by wire transfer into a Bank-2 account. Records from Bank-2 reflect that at least approximately five of these wire transfers have a IMAD number on the wire transfer, which I know from my training and experience, generally speaking, means that the wire was conducted through the Fedwire system.

16. The AU Entities also maintained accounts at several U.S.-based cryptocurrency companies, including Cryptocompany-1 and Cryptocompany-2, to facilitate money transmitting services to their customers that involved cryptocurrency. Again, during this time period, the AU Entities were not properly registered with FinCen.

a. According to records obtained from Cryptocompany-1, in or around 2018, AU Card, LLC engaged in over 160 digital asset trades that involved over $150 million. In or around 2019, AU Card, LLC engaged in over 5,900 digital asset trades that involved over $35 million.

b. Records obtained from Bank-1 reflect that from in or around January 2018 through in or around January 2019, the AU Bank-1 Account received more than approximately $157 million from a bank account controlled by Cryptocompany-1, and AU Card, LLC wired approximately $1.3 million to a bank account controlled by Cryptocompany-1 from the AU Bank-1 Account.

c. Records obtained from Bank-2 reflect that from in or around February 2019 through in or around April 2019, an AU Card, LLC, Bank-2 account received more than approximately $13 million from a bank account controlled by Cryptocompany-1, and AU Card, LLC wired approximately $1.6 million to a bank account controlled by Cryptocompany-1 from the AU Card, LLC Bank-2 account.

d. Scanlon, on behalf of AU Card, LLC, entered into loans with Cryptocompany-2 so the AU Entities could have liquidity involving

cryptocurrency and cash. Under the loan agreements, Cryptocompany-2 provided AU Card, LLC with a loan for millions of dollars in exchange for AU Card, LLC using bitcoin as collateral. For example, in or around November 2019, AU Card, LLC loaned approximately $2 million from Cryptocompany-2 and put up approximately 395 bitcoin as collateral on the loan.

17. In or around 2021, the U.S. Financial Controller for PMA (the "PMA Controller") sent an email admitting that the AU Entities would use AU Card, LLC's accounts at Bank-2, Bank-3, and Cryptocompany-1 to facilitate transactions on behalf of customers of the AU Entities. The PMA Controller provided an example that involved a hypothetical customer who wanted to purchase bitcoin through an account provided by the AU Entities. According to the PMA Controller, the AU Entities could facilitate such a transaction using U.S.-based companies, including U.S. financial institutions.

18. Further, Scanlon operated the AU Entities without appropriate regard for the applicable U.S. financial regulatory system and viewed the penalties for regulatory noncompliance as insignificant. For example, in an exchange with another person working with the AU Entities, Scanlon acknowledged that the AU Entities were moving "fast," but Scanlon reasoned that moving fast is "how we win." Scanlon continued: "in the end, if the regulators come and scrutinize . . . they tell you what you have done wrong, slap you on the wrist with a fine, and you remediate."

Customer-1

19. Customer-1 managed a marijuana distribution business. According to Customer-1, in or around 2016, Customer-1 met Scanlon at a professional football game in East Rutherford, New Jersey. Customer-1 told Scanlon that Customer-1 ran a medical marijuana business. During this football game, Scanlon recruited Customer-1 to use Aurae Lifestyle, which at the time was an unlicensed money transmitting business. Scanlon told Customer-1 that Scanlon knew a lot of people in that business and offered that he (Scanlon) had a business that could serve as a sort of bank for Customer-1's business. This was appealing to Customer-1 because U.S. banks were unwilling to service his marijuana distribution business.

20. Thereafter, Customer-1 opened an Aurae Lifestyle account. Scanlon told Customer-1 that some of Scanlon's clients needed cash, so Scanlon would give them the cash he received from other clients and would credit their Aurae Lifestyle accounts appropriately. Indeed, sometime thereafter Scanlon instructed Customer-1 to provide cash to another Aurae Lifestyle customer, which Scanlon then caused to be credited to Customer-1's Aurae Lifestyle account.

21. Scanlon thereafter met Customer-1 at a location in New York City. At this meeting, Customer-1 handed Scanlon a bag full of cash, which Customer-1 understood would be provided to an Aurae Lifestyle customer who needed cash.

22. Records of Customer-1's Aurae Lifestyle account reflect large transactions credited to his Aurae Lifestyle account. For example, the records reflect that in or around December 2016, approximately $40,000 was credited to Customer-1's Aurae Lifestyle account. The explanation for the credit is "credit - other charge adjustment." On or about the same day, the records reflect a charge at a restaurant in New Jersey (the "New Jersey Café").

23. In or around December 2016, Scanlon exchanged messages with Customer-1 about his Aurae Lifestyle account. Approximately two days before Customer-1's Aurae Lifestyle records reflect the $40,000 credit to his account and the charge from the New Jersey Café, Scanlon discussed that he would travel to the New York area to personally deliver Customer-1's gold card to him. In response to Scanlon asking where he should meet Customer-1, Customer-1 sent Scanlon a map screenshot of the New Jersey Café, and Scanlon agreed to meet Customer-1 there the following morning.

24. In or around May 2017, Scanlon sent Customer-1 a text message offering to meet Customer-1 in another city and said: "I can meet you there- we need 600" "Up to you brother :)." A few days later, Scanlon asked Customer-1, "600 doable? Meet in Vegas?"

25. In or around June 2018, Scanlon instructed Customer-1 to provide cash to another Aurae Lifestyle customer, Customer-2. Customer-1 flew to Los Angeles, California and gave Customer-2 thousands of dollars in cash. During the transaction, Customer-1 was on the phone with Scanlon. The cash provided by Customer-1 to Customer-2 was derived from the sale of marijuana.

26. In or around June 2018, Scanlon sent Customer-1 a text message that said Scanlon had "good news" and instructed Customer-1 to call him in the morning. A few days later, Customer-1 asked for a location, in response to which Scanlon sent a hotel in Southern California in the general vicinity of Los Angeles. On or about the day before the over $300,000 card-to-card transaction was posted to Customer-1's Aurae Lifestyle account, Customer-1 and Scanlon exchanged the following messages:

Scanlon	**Customer-1**
	Just landed in LA
Wow! I just spoke to [Customer-2's first name] Ok if I give him your number?	
	Wait still need to go collect

Will meet him later on
Just give me his number

You bet bro

Thank you my friend
Please let him know i am
flying back tonight my flight
is at 7:30
Sorry to keep bothering you

Will do bud
He needs to be done by 6

27. In or around June 2018, Customer-1's Aurae Lifestyle account records reflect a "card to card" transfer to Customer-1's Aurae Lifestyle account of over approximately $300,000.

Customer-2

28. Customer-2 conducted over $38 million worth of financial transactions through his Aurae Lifestyle account between in or around 2018 and in or around 2019.

29. For example:

a. According to an email from Scanlon sent to Customer-2, in or around August 2017 and in or around December 2017, the AU Entities credited Customer-2's Aurae Lifestyle account the equivalent of approximately $1 million in exchange for bitcoin from Customer-2 on each occasion.

b. In or around March 2018, Customer-2 messaged Scanlon and requested that Scanlon wire approximately $1.25 million from Customer-2's Aurae Lifestyle account to another U.S. business bank account. Thereafter, Scanlon and another U.S.-based employee of the AU Entities caused a wire transfer to be executed from the AU Bank-1 Account in the approximate amount of $1.25 million to another U.S. business bank account as requested by Customer-2.

c. In or around June 2019, Customer-2 wired approximately $3.5 million to an account controlled by the AU Entities for the purpose of purchasing bitcoin. The AU Entities charged Customer-2 approximately $3.427 million for the bitcoin and charged approximately $6,250 for the transaction. Scanlon instructed several AU Entity employees, including the Financial Controller of Nvayo Ltd. (the "Nvayo Controller"), to wire money to a Bank-2

account, with instructions to then send the money from the Bank-2 account to another U.S. bank account at Bank-3, and to then transfer the money to Cryptocompany-1 to complete the transaction. The Nvayo Controller later emailed Scanlon to confirm that a payment request of $2.6 million from Nvayo to Bank-2 had been requested.

Customer-3

30. This investigation has revealed that Customer-3 moved millions of dollars derived from Fraud Scheme-2 through his Aurae Lifestyle account.

31. For example:

a. In or around August 2018, Scanlon directed his employees of the AU Entities to conduct a wire transfer of approximately $2.5 million for Customer-3 through his Aurae Lifestyle account.

b. In or around March 2019, Scanlon directed his AU Entities employees to conduct a wire transfer for Customer-3 of approximately $3 million, to be sent through AU Card, LLC's Bank-2 account.

c. In or around April 2019, Customer-3 transferred approximately $1 million from his Aurae Lifestyle account to Lawyer-1's Aurae Lifestyle account.

d. In or around June 2019, Scanlon directed his AU Entities employees to conduct a wire transfer for Customer-3 of approximately $750,000 to be sent through the AU Card, LLC's Bank-2 account to a bank in Australia.

e. In or around July 2019, Scanlon directed his AU Entities employees to conduct a wire transfer for Customer-3 of approximately $400,000 to be sent through AU Card, LLC's Bank-2 account. Customer-3 was charged approximately $4,000 by Aurae Lifestyle as a wire transfer fee for this transaction.

f. In or around December 2019, Customer-3 sent bitcoin to a wallet provided to Customer-3 by Scanlon in order to receive fiat currency in return through his Aurae Lifestyle account. In response to Customer-3's request, Scanlon directed his AU Entities employees to transfer approximately $2.965 million from AU Card, LLC's network account at Bank-3 to AU Card, LLC's operating account at Bank-3. Scanlon then instructed the employees to send approximately $2.965 million from the Bank-3 operating account to

AU Card, LLC's Bank-2 account. Scanlon instructed further that, once the funds arrived in the Bank-2 account, the employees were to wire approximately $2.5 million from the Bank-2 account into a bank account provided by Customer-3. Through the above transactions, Customer-3 was able, through his Aurae Lifestyle account, to convert more than $2.5 million in bitcoin into U.S. dollars.

32. In or around August 2019, Customer-3 messaged Scanlon via a chat application and requested that Scanlon send money to Lawyer-1's Aurae Lifestyle account because Customer-3 had not properly completed know your customer documentation purportedly required by Nvayo before Customer-3 could send the money directly through his account.

33. Thereafter, as a separate transaction, Customer-3 asked Scanlon if he could convert approximately 22,000 Litecoin, a type of cryptocurrency, worth approximately $1.7 million, into bitcoin for Customer-3. Scanlon agreed to convert the cryptocurrency for Customer-3 and did in fact do so.

34. Customer-3 then asked Scanlon if Scanlon could keep the cryptocurrency transaction off of the ledger of Customer-3's Aurae Lifestyle account because Customer-3 wanted the transaction to appear "nowhere." Scanlon agreed to keep the transaction off of the books. Customer-3 confirmed: "So for sure? Ghost!" "If not I have to treat differently. So need to know for sure" "You will need to attach this to [Customer-4's] account if anything." Scanlon replied: "No attachment at all" "Doesn't hit fiat." Scanlon and Customer-3 then exchanged wallet addresses.

35. A review of the cryptocurrency transaction using blockchain analysis software, along with records from Cryptocompany-1, confirmed that Customer-3's cryptocurrency exchange described in Paragraph 33, above, was conducted through AU Card, LLC's account at Cryptocompany-1.

36. After the transaction was completed, Customer-3 confirmed: "Boom! Received!" Customer-3 asked Scanlon to confirm that the transaction was not posted on the ledger of his Aurae Lifestyle account, asking Scanlon: "Ghost, right?," to which Scanlon confirmed: "Boo."

37. In or around November 2019, Scanlon sent an email to Customer-3 and Customer-3's accountant (the "November Email"). The November Email attached a letter on Aurae company letterhead that bore Scanlon's signature. The letter described a wire transfer of approximately $205,973 that AU Card, LLC had made on behalf of a property owned by Customer-3 and Lawyer-1, both of which Scanlon identified as AU Card clients. The letter represented that the wire transfer was being sent as a part of AU Card, LLC's concierge service. The letter bore a stamp

with Nvayo's license number from the United Kingdom's Financial Conduct Authority ("FCA") and stated that AU Card, LLC was authorized by the FCA to issue electronic money payments. The Financial Services Record is an online registry of entities that are registered or authorized by the FCA. The online registry does not reflect that AU Card, LLC has been registered or authorized by the FCA to issue electronic money payments.

Customer-4

38. Customer-4 maintained an Aurae Lifestyle account during the time he was perpetuating Fraud Scheme-2.

39. In or around November 2018, Scanlon instructed employees of the AU Entities to conduct a wire transfer of approximately $30,000 on behalf of Customer-4 using the AU Bank-1 Account.

40. In or around 2019, Customer-4 requested to wire approximately $400,000 from his Aurae Lifestyle account to an account in Cambodia. The transaction was flagged by Nvayo's compliance department.

41. In or around July 2019, Nvayo filed a report with a regulator in the United Kingdom in which Nvayo relayed issues flagged with Customer-4's accounts. The report represented: "We have not closed the account, yet we are restricting the funds of USD 400,000 to be transferred out and we are restricting the customer ability to transact further."

42. During this time, Scanlon continued to assist Customer-4 with financial transactions as Customer-4 relayed to Scanlon that he wanted his financial transactions to run through other Aurae Lifestyle customers' accounts.

43. Specifically, Scanlon exchanged several chat and audio messages with Customer-4 about Customer-4 providing source of funds documentation regarding the $400,000 wire transaction. In or around July 2019, Customer-4 sent audio message files to Scanlon informing Scanlon that he did not have an invoice for the transfer to his Cambodian account and asked whether they should instead conduct a series of small transactions.

44. In or around July 2019, Customer-4 instructed Scanlon to move money from his account to Customer-3's account and to then send that money to Customer-4's Cambodian bank account.

45. Thereafter, Customer-4 sent audio files to Scanlon informing Scanlon that Customer-4 asked Customer-3 to use his account again because he needed to wire additional money and Customer-4 understood that his Aurae Lifestyle account was "no good" for the time being for transferring money.

46. Customer-4 then sent Scanlon another instruction to transfer money for Customer-4 through another member's Aurae Lifestyle account.

47. In or around August 2019, Customer-4 sent Scanlon another audio message telling Scanlon that his accountant was a "million percent by the book, won't do anything" so Customer-4 would try to find someone else (presumably, to provide false source-of-funds documentation for Customer-4). Customer-4 told Scanlon further that he wouldn't be doing any more transfers from his account, but that he "has some friends."

48. In or around September 2019, Customer-4 sent Scanlon several audio messages explaining to Scanlon how wire transfers and cryptocurrency sales should be conducted outside of his account. Customer-4 asked Scanlon if using other people's accounts to effectuate his transfers could be done long term if Customer-4 did not "have a letter" explaining his source of funds.

49. Customer-4 sent Scanlon an audio message in which Customer-4 told Scanlon that Customer-4 was going to modify a source of funds letter that Lawyer-1 had provided to him, which Customer-4 would then get notarized.

50. On or about October 21, 2019, Customer-4 provided an attestation claiming that he was a practicing attorney licensed in Utah who served as legal counsel and as a trustee for various clients, and he entered into a speaking engagement with a company, in which he received approximately $3 million for participating in three speaking engagements. The attestation at the bottom of the document still included the name of Lawyer-1 instead of Customer-4. The document appeared to be notarized in Japan.

51. Customer-4 was not a lawyer. In fact, an Internet search revealed that Customer-4 was a noncompliant, Tier II sex offender. He had previously been convicted of coercion using sexually motivated force and possession of child pornography.

52. Customer-4 remained a customer of Aurae Lifestyle and continued to conduct financial transactions through his account through in or around February 2020, notwithstanding that the AU Entities were aware of pending criminal charges pertaining to Fraud Scheme-2 against Customer-4 in December 2019.

Customer-5

53. In or around June 2018, Customer-4 purchased an Aurae Lifestyle membership for Customer-5.

54. In or around September 2018, Scanlon emailed an AU Entities employee and directed him to send a wire transfer of approximately $325,040 on

behalf of Customer-5 using the AU Bank-1 Account. The invoice provided in the body of Scanlon's email reflected that the wire transfer was to pay "tax credits."

55. In or around May 2019, Scanlon emailed employees of the AU Entities and directed them to send a wire on behalf of Customer-5. Attached to the email with the directions was a barebones invoice addressed to Customer-5 for approximately $36,500 for "BTC Conversion." In response to Scanlon's instructions, an individual with a PMA email address observed, "[i]f we share this invoice to [one of the AU Entities' money processing company] they may hold the payment and raise question [sic] around the description of payment as it is mentioned as 'BTC conversion.'" The individual asked Scanlon permission to instead process the wire transfer through Bank-2, to which Scanlon agreed.

56. Records received from AU Card, LLC reflect that on or about December 2, 2019, the AU Entities wired approximately $58,000 from AU Card, LLC's Bank-2 account on behalf of Customer-5. The wire transfer record reflects an IMAD number, which I know, generally speaking, means the wire transfer was accomplished through the Fedwire system. The AU Entities charged Customer-5 approximately 1% of the wire amount as a wire transfer fee.