IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA -v.- DIOGO SANTOS COELHO Defendant.	Case No. 1:21-cr-114

AFFIDAVIT IN SUPPORT OF REQUEST FOR EXTRADITION OF DIOGO SANTOS COELHO

I, Assistant United States Attorney Carina A. Cuellar, being duly sworn, state that:

1. I am a citizen of the United States of America and a resident of the State of Virginia. I make this affidavit in support of the request of the United States of America to the United Kingdom of Great Britain and Northern Ireland for the extradition of Diogo Santos Coelho.

2. I graduated from Harvard Law School. I am licensed to practice law in the State of California and the District of Columbia. From December 1, 2014 to the present, I have been employed by the U.S. Department of Justice as an Assistant U.S. Attorney for the Eastern District of Virginia. My duties are to prosecute persons charged with criminal violations of the laws of the United States. During my practice as an Assistant U.S. Attorney, I have become

knowledgeable about the criminal laws and procedures of the United States.

3. In the course of my duties, I have become familiar with the charges and evidence in the above-captioned case of Diogo Santos Coelho ("Coelho"), criminal case number 1:21-cr-114. The charges arose out of an investigation by the Federal Bureau of Investigation ("FBI") and the United States Secret Service ("USSS") (the "U.S. investigators"), as well as the U.S. Attorney's Office for the Eastern District of Virginia and the Computer Crime and Intellectual Property Section of the Department of Justice (together, the "U.S. Authorities"). The investigation revealed that between approximately June 2016 and on or about January 31, 2022, Coelho controlled and was the chief Administrator of a website www.Raidforums.com ("RaidForums"), which he operated with the help of other website Administrators. The RaidForums website was a platform where members could solicit for sale, sell, and purchase contraband, including stolen access devices, means of identification, hacking tools, breached databases, and other illegal services.

SUMMARY OF THE FACTS OF THE CASE

4. In or around 2016, RaidForums became a popular marketplace for individuals to purchase and download stolen databases containing access devices, including, but not limited to, bank routing and account numbers, and stolen payment card data, such as payment card account numbers, card verification values, card expiration dates, and hacked databases of login credentials, such as usernames and associated passwords, for access to online accounts issued by United States entities, and means of identification, including, but not limited to, names, email addresses, and social security numbers. The website also hosted sub-forums where members

could solicit the sale and purchase of stolen access devices and means of identification. Often the stolen access devices and means of identification belonged to United States companies and individuals. Additionally, and more recently, RaidForums members have also used the platform to solicit others to commit computer intrusions and sell means to commit computer intrusion.

A. Background on RaidForums Investigation

5. From at least June 2016 and continuing until the United States government seized the RaidForums domains, the U.S. authorities' investigation indicates that RaidForums trafficked in breached data by offering hundreds of databases for sale, consisting of over 10 billion unique records of individuals residing in the United States and internationally. The databases included information stolen from companies and other entities, such as customer and subscriber lists. Those customer and subscriber lists often included credit card information, bank account information, usernames and passwords for accessing customer accounts, and other personally identifiable information, such as name, addresses, dates of births, and social security numbers. To purchase compromised databases from RaidForums, a member purchased "credits." Members could purchase credits via cryptocurrency. Prior to November 2021, members could also purchase credits through PayPal, an online payment system headquartered in the United States.

6. Any individual could access the RaidForums website without a membership. However, the website required an individual to sign up for a membership to solicit items for sale or purchase items. The RaidForums website offered four tiers of membership options, including in order of cost: (1) free membership; (2) VIP membership; (3) MVP membership; and (4) God

membership. The more expensive the membership, the more access a user could get to the RaidForums website. The God membership, for example, offered almost unlimited access to the RaidForums website and features.

7. The "credits" RaidForums sold to members granted access to privileged areas of the website and enabled members to "unlock" and download stolen access devices, means of identification, and data from compromised databases, among other items. Members could also earn credits through other means including, but not limited to, by posting instructions on how to commit certain illegal acts.

8. RaidForums had different forums where members could post about different subjects and offer items for sale. The forums included "Cracking," "Leaks," and "Marketplace," among others. The "Leaks" forum had a sub-forum entitled the "Leaks Market." The "Leaks Market" description stated that it was "[a] place to buy/sell/trade databases and leaks." The "Leaks Market" included for-sale listings for stolen credit card account information, means of identification, and hacked online accounts and databases.

9. The chief administrator and self-described "owner" of RaidForums used the moniker "Omnipotent," and the evidence establishes that this is Coelho. Omnipotent and other administrators designed and administered the website's software and computer infrastructure; established and enforced website's rules; and created and managed sections of the website dedicated to promoting the buying and selling of contraband, including the "Leaks Market" sub-forum.

10. Omnipotent also offered an "Official Middleman Service" for a fee on the

RaidForums website. For instance, on or about July 24, 2018, Omnipotent posted an advertisement for an "Official Middleman Service" on the RaidForums website indicating that the service would enable both buyers and sellers to complete their transactions. More specifically, Omnipotent offered to accept cryptocurrency from the purchaser and files, including stolen access devices and means of identification, from the seller. Omnipotent then typically verified the contents of the files and conversed with the buyer and seller. Once the parties were satisfied, Omnipotent released the funds to the seller and the files, including stolen access devices and means of identification, to the purchaser. Omnipotent profited from the middleman service by charging a fee commensurate to pre-set percentages of the transaction.

11. As detailed below, the evidence proves that Diogo Santos Coelho controlled the Omnipotent moniker on RaidForums, as well as several other online monikers and personas that he has used to administer or otherwise further malicious activity on RaidForums, such as "Downloading," "Shiza," and "Kevin Maradona." Indeed, as noted below, Coelho admitted that he is Omnipotent to U.S. law enforcement.

B. Overview of Primary Sources of Evidence

12. FBI and USSS personnel, as well as other sources, have accessed, monitored, and memorialized criminal content on RaidForums, including through undercover activity and confidential human sources. As further explained below, the investigators have also memorialized screenshots of conversations through the messaging services Discord and Telegram in which Coelho facilitated transactions with other RaidForums members.

13. Further, as part of the investigation, the FBI obtained a copy of the back-end

database for RaidForums. The back-end database contained a substantial amount of information that is not generally accessible to the public or other RaidForums members, including account registration information, user Internet Protocol ("IP") addresses, login information, and private messages of members and administrators of RaidForums, including for Coelho's monikers "Omnipotent" and "Downloading."

14. In addition, warrants to search Discord and Twitter accounts associated with RaidForums activity, including for Coelho, revealed substantial evidence of Coelho providing middleman services to other RaidForums members who bought and sold illicit goods and services, such as hacked or "leaked" databases, access devices, and hacking tools. Coelho's activity on Discord and Twitter further confirmed that he aided and abetted these illicit transactions knowingly and intentionally.

C. Incidents Underlying Charged Counts

15. The above-described sources of evidence reveal that Coelho, along with others associated with administering and selling access devices on RaidForums, have knowingly and intentionally engaged in a multi-year scheme to profit from the largescale buying and selling of access devices through the administration of the RaidForums website and Coelho's middleman service, as alleged in Count 1 of the Second Superseding Indictment. Indeed, the RaidForums official database index, which is where the major database leaks are posted, claimed to have close to 10 billion Personal Identifiable Information ("PII") records available. Five exemplary transactions are specifically described and alleged in Counts 1-6. As detailed below, some of these transactions involved access devices that Coelho and other RaidForums members offered

on RaidForums, and that the FBI and USSS purchased in an undercover capacity using Coelho's middleman service. Another involved a RaidForums member's sale of data through Coelho's middleman service that was stolen by compromising the computer system of a major telecommunications company and wireless network operator that provides services in the United States.

i. Purchase of Usernames and Passwords Using Credits

16. RaidForums has several forums covering different topic areas. In one of these forums, an unknown member using the moniker "mariecurie" posted an offer to sell access to user accounts issued by an electronic commerce company in the United States ("Company 1") on or about October 18, 2018. On or about October 22, 2018, a law enforcement officer in the Eastern District of Virginia, acting in an undercover capacity, purchased eight credits from RaidForums and then used those credits to "unlock" the post. After paying the eight credits, a link was made available, and a law enforcement officer downloaded the accounts. Information provided by Company 1 confirmed that approximately 3,810 accounts were legitimate and approximately 75 of these accounts belonged to individuals in the Eastern District of Virginia.

17. This law enforcement purchase is set forth in the overt acts for Count 1 (Conspiracy to Commit Access Device Fraud) and Count 4 (Access Device Fraud – Unauthorized Solicitation).

ii. Purchase of Credit Card Numbers Using Omnipotent's Middleman Service

18. On or about December 16, 2018, Coelho, who was using the moniker "Downloading," posted an offer on RaidForums to sell approximately 2.3 million credit card

numbers, including the names, addresses, and phone numbers associated with the credit cards. The post stated that the credit cards were obtained from a breach of records belonging to "a bunch of USA hotels." He continued that "if anyone is interested in buying this leak[,] its [sic] around $25,000[,] the cards are still fresh"—*i.e.*, they can still be used. In a subsequent post in the thread, Downloading denied that he was reselling previously published credit cards by emphasizing that "I never said it was a known breach? This is private data what I am selling is card info and its fresh and hasn't been resold anywhere so its first come first serve."

19. In February 2019, law enforcement in the Eastern District of Virginia began engaging with Downloading. On or about February 5, 2019, Downloading informed law enforcement that the stolen credit card numbers were still available for sale. On or about March 4, 2019, law enforcement and Downloading then negotiated his sale of 1.1 million of the records for a Bitcoin amount that was then equivalent to approximately $4,000. Downloading also suggested that the parties use the middleman service offered on RaidForums.

20. Prior to agreeing to the sale, law enforcement asked for a sample so they could verify that the credit cards were actual "legitimate" cards. Downloading then sent three credit card numbers and card verification values to law enforcement. Once law enforcement received the credit card numbers and verification values, they contacted the credit card companies, who verified that the cards worked. Law enforcement also interviewed the owners of the cards, and each stated that they did not provide another individual permission to use or sell their credit card information.

21. On or about March 5, 2019, the purchase took place. During the purchase, law

enforcement and Coelho moved their communications to Discord, where Downloading (Coelho) and Omnipotent (Coelho) used the Shiza and Omnipotent accounts. During these communications, the parties discussed how payment was to be made and law enforcement transferred a Bitcoin amount that was then equivalent to approximately $4,000 to a Bitcoin wallet address that Omnipotent (Coelho) provided for the escrow exchange. Shortly after this transfer was made, Omnipotent and Shiza both blocked the law enforcement Discord account and all communications ceased. The law enforcement account was also blocked from using RaidForums.

22. After these actions, law enforcement, purporting to be the now blocked RaidForums member, emailed Omnipotent at unrivalled@pm.me and revealed that they knew his real identity was Coelho, and demanded the credit card information. Omnipotent denied that he was, in fact, Coelho and ignored law enforcement's subsequent email communications. As further explained below, Coelho would later email law enforcement from unrivalled@pm.me and represent that he was the same Coelho who attempted to enter the United States.

23. As will be discussed below, there is overwhelming evidence that Coelho used both the Omnipotent and Downloading accounts on RaidForums, as well as used those monikers on other platforms.

24. This law enforcement purchase is set forth in the overt acts for Count 1 (Conspiracy to Commit Access Device Fraud), Count 2 (Access Device Fraud – Using or Trafficking in an Unauthorized Access Device), Count 5 (Access Device Fraud – Unauthorized Solicitation), and Count 6 (Aggravated Identity Theft).

iii. Purchase of Broadcasting and Cable Database Using Credits

25. USSS made several undercover purchases of apparently breached data sold on RaidForums. Notably, on or about July 24, 2020, the USSS reviewed the following post initially made by Omnipotent on or about October 26, 2016, which stated, in relevant part:

> "In November 2015, the U.S. internet and TV provider [redacted company name] suffered a data breach that exposed 590k customer email addresses and plain text passwords. A further 27k accounts appeared with home addresses with the entire data set being sold on underground forums. Compromised data: Email addresses, passwords, and physical addresses."

USSS then used its credits on RaidForums to unlock this database. After using the credits, USSS was provided a link to use, which enabled USSS to download the database. USSS confirmed that the data contained usernames and passwords.

26. Subsequently, USSS interviewed representatives of a major broadcasting and cable company in the United States ("Company 2"), who confirmed that they were the victim of a data breach a few years ago and that they were aware that the data was shared on the dark web. Company 2 representatives reviewed a sample of the data provided by USSS and confirmed that the data was, in fact, Company 2 customer data. Company 2 also confirmed that some of the email accounts belonged to live accounts; however, Company 2 had reset the passwords and so the passwords would no longer work.

27. This law enforcement purchase is set forth in the overt acts for Count 1 (Conspiracy to Commit Access Device Fraud) and Count 3 (Access Device Fraud – Possession of Fifteen or More Unauthorized Access Devices).

iv. Purchase of Tax Account Information Using Coelho's Middleman Service

28. On or about April 5, 2020, a confidential source ("CHS") working with the FBI alerted the FBI that a member using the moniker "fairbanksfires" posted an offer on RaidForums to sell tax information, including approximately 39,000 social security numbers, 20,000 tax IDs, 58,000 emails and passwords, and over 20,000 bank accounts with routing numbers. The CHS obtained a sample data from fairbanksfires and identified the victim tax company in the Eastern District of Virginia, who were aware of the data leak and were in contact with the IRS.

29. On or about April 25, 2020, the CHS used Coelho's middleman service to purchase the data. A forum conversation with all three monikers established the rules for the transaction. During the transaction, it was made clear that "[t]here is a lot to [the data], but the most valuable elements [of the data] were in the header – US Tax efiling Co DB: 39,601 SSN+, 21, 975 EIN+, 58,083 Email/Pass." The CHS agreed to provide payment to a BTC address provided by Omnipotent in exchange for fairbanksfires providing a download link to a file share repository to Omnipotent. The CHS then transferred a Bitcoin amount that was then equivalent to approximately $4,000 to Coelho during the transaction, and Omnipotent then provided the CHS with a download link.

30. After the transaction, law enforcement analyzed the data and determined that it contained the information as advertised, including bank account numbers and routing numbers. Then, on or around April 27, 2020, the CHS notified Omnipotent that he could release the funds to fairbanksfires.

31. This law enforcement purchase is set forth in the overt acts for Count 1

(Conspiracy to Commit Access Device Fraud).

v. Purchase of Databases Using Omnipotent's Middleman Service

32. On or about August 11, 2021, an individual using the moniker "SubVirt" posted on the RaidForums website an offer to sell recently hacked data with the following title: "SELLING-124M-U-S-A-SSN-DOB-DL-database-freshly-breached." This post provided a small sample of data, which included names and dates of birth, and priced the information at six (6) Bitcoin. At the time, that was equivalent to approximately $273,672. Several days later, "SubVirt" revised this post with the following title: "SELLING 30M SSN + DL + DOB database." This post provided a small sample of data, which included names and dates of birth, and priced the information at six (6) Bitcoin. The post also provided a Telegram handle as contact information for interested buyers. A subsequent post confirmed that the hacked data belonged to a major telecommunications company and wireless network operator that provides services in the United States ("Company 3").

33. After this post, Company 3 hired a third-party to purchase exclusive access to the database to prevent it from being sold to criminals. A third-party employee then posed as a prospective buyer and used Omnipotent's middleman service to purchase a sample of the databases for a Bitcoin amount that was then equivalent to approximately $50,000. Subsequently, an employee of the third-party again used Omnipotent's middleman service to purchase the entire database for a Bitcoin amount that was then equivalent to approximately $150,000. The agreement was for "SubVirt" to then destroy their copy of the database; however, it appears the co-conspirators continued to attempt to sell the databases after the third-party's

purchase.

34. Information provided by Company 3 and also obtained by law enforcement indicates that the data sold by SubVirt included several sensitive databases containing the following types of information: customer names, social security numbers, dates of birth, driver's license numbers, phone numbers, billing account numbers, customer relationship manager information, Mobile Station Integrated Services Digital Network (MSISDN) information, International Mobile Subscriber Identity (IMSI) numbers, and International Mobile Equipment Identity (IMEI) numbers.

35. This purchase is set forth in the overt acts for Count 1 (Conspiracy to Commit Access Device Fraud).

vi. Coelho Falsely Registers "Raidforums.com" Domain in Furtherance of Conspiracy

36. The domain "Raidforums.com" was initially registered in or around 2014 when Coelho was a minor. However, Coelho has continued to use false information to modify and renew his registration after turning 18. For instance, records received from Namecheap, a U.S.-based domain registrar, reveal that a person with the username "Omnipotents," created a Namecheap Account on or around June 6, 2018, and transferred the registration of the Raidforums.com domain to Namecheap. To amend the registration, the name "Kevin Maradona" was provided. As further detailed below, there is strong evidence to believe that Coelho routinely used both the Omnipotent username and Maradona alias. The Raidforums.com domain, in turn, furthered the above-described scheme by hosting the RaidForums website

through which Coelho committed the above-specified crimes.

37. Coelho also registered the domains rf.ws and raid.lol to ensure that the RaidForums website could remain online if there was a disruption to the Raidforums.com domain. For instance, on or around April 20, 2020, Omnipotent posted on RaidForums that "[i]n case our domain is ever seized or terminated[,] here are some mirrors we will be using in the future; rf.ws and raid.lol."[1] Records received from Namecheap and Namesilo LLC ("Namesilo"), a U.S.-based domain registrar, used false identifying information to register the domains rf.ws and raid.lol, including to renew and transfer their registrations after Coelho turned 18. Notably, the above-identified Namecheap account also renewed the registration of the domain raid.lol on or around July 23, 2019. Records received from Namesilo in 2021 further indicated that an account was created on or around April 23, 2020, to maintain the registrations of the domain names rf.ws and raid.lol, which listed the username "Omnipotent" and email "unrivalled@pm.me."[2] As further detailed below, unrivalled@pm.me is an email address Coelho used to correspond with U.S. law enforcement.

D. Evidence that Coelho is Omnipotent and therefore Operates RaidForums

38. As detailed above, RaidForums is run by an actor using the moniker Omnipotent.

---

[1] A mirror website or mirror is a replica of an original website. Such sites have different uniform resource locators (URLs) than the original website, but host identical or near identical content.

[2] The account listed a registration name "Joshua Snow," which appears to be fictitious or false given the other information tying its account owner to Coelho.

Additionally, an actor using the moniker Downloading has advertised the sale of stolen access devices on RaidForums. There is extensive evidence proving that Coelho is both Omnipotent and Downloading on RaidForums, and the owner and chief Administrator of RaidForums. There is also extensive evidence that Coelho has also used the online moniker Shiza and online persona "Kevin Maradona," to register accounts on other platforms used in furtherance of the scheme. Because the attribution evidence is voluminous, we only detail some of this evidence below.

i. Evidence Obtained From Coelho's Electronic Devices

39. On or about June 25, 2018, Coelho attempted to enter the United States at the Hartsfield-Jackson Atlanta International Airport. Upon entry, Coelho told a U.S. law enforcement official certain biographical information, including his home address, cell phone number, and father's phone number. Coelho identified "Jose" as his father. Coelho stated that he worked online in "coding," and owned his own website, but did not identify the site. U.S. law enforcement also obtained a warrant to search the electronic devices that Coelho brought with him upon entry to the United States. The FBI's search of these devices confirmed both that they belonged to Coelho, and that Coelho used the moniker, "Omnipotent," to operate and administer RaidForums. For instance, Coelho's smart phone received numerous emails from the "mail system at host raidforums," as well as emails concerning a new RaidForums password and account activation. The phone also revealed a Discord account with the username "Omnipotent" and email address unrivalled@pm.me, an account with Snapchat, a multimedia instant messaging application and service, with the name "Diogo {Omnipotent}" and same email address, and text messages where he identifies himself as "Omni." The smart phone also

revealed that it was linked to the email address linkedbrew@gmail.com with the name "Kevin Maradona."

ii. Coelho's Statements to Law Enforcement and Use of unrivalled@pm.me

40. In an attempt to retrieve his items, Coelho called the lead FBI case agent on or around August 2, 2018, and used the email address unrivalled@pm.me to email the agent on or around August 29, 2018. Coelho stated that Omnipotent was his online alias and confirmed his address as 121B Rua São João Bairro Do Pereiro 3515-169 Viseu, in Portugal. He also provided a photo of his Citizen Card, number 152028676 ZY0, which matched the Citizen Card contained in know your customer (KYC) information received from Coinbase, Inc. pursuant to a subpoena issued on the account used to accept cryptocurrency for RaidForums "credits."

iii. Coelho's Use of the linkedbrew@gmail Account and Ties to RaidForums

41. In addition, pursuant to a search warrant issued by a court in the Eastern District of Virginia, investigators searched the Google account associated with linkedbrew@gmail.com that, as described above, was linked to Coelho's smart phone. Information contained in this account confirmed that it was under Coelho's control, including the following:

a. the user-configured display name for the account was "Diogo Coelho";

b. email conversations between Coelho and several prospective employers regarding scheduling of, and follow up to, employment interviews;

c. the linkedbrew@gmail.com account contained numerous emails sent to diogo.coelho@aldemarltd.co.uk. A combination of metadata in the headers of these messages and public information regarding the email service provider for the aldemarltd.co.uk domain

suggests this address has been configured to forward email messages to linkedbrew@gmail.com since in or around 2016;

d. metadata for 30 photographs created in or around June and July 2017 containing location data (Latitude and Longitude coordinates) clustered at Coelho's known address in Portugal.

e. metadata for 31 photographs created in or around June and July 2017 indicating they were taken with a Lenovo "Tab3 10 Business" Tablet. These photos all contain location data (Latitude and Longitude coordinates) clustered at Coelho's known address; and

f. email receipts for purchases that used the name and address of Coelho's father as the delivery address.

42. The linkedbrew@gmail.com account also revealed additional evidence tying Coelho to RaidForums. For instance, the account replied to requests to purchase RaidForums credits and account activation support requests and contained over 500 emails addressed to lol@raid.lol. Further, the recovery email address for the linkedbrew@gmail.com account was recovery@raidforums.com. Additionally, information provided by Google in response to a court order indicates that linkedbrew@gmail.com was the recovery email account for info@raidforums.com.

43. Moreover, according to PayPal records, Coelho's father is the account holder for the PayPal account associated with linkedbrew@gmail.com. The account is also linked to a credit card and a bank account in the name of Coelho's father. Transaction records for this account support that the account received thousands of transactions for RaidForums "credits."

44. Further, law enforcement in its review of the search warrant return for the linkedbrew@gmail.com account identified that Omnipotent's private messages and payment notifications on RaidForums were either sent directly to linkedbrew@gmail.com, or were forwarded to linkedbrew@gmail.com from another email account.[3] For instance, from on or around November 11, 2016 through July 8, 2017, linkedbrew@gmail.com received emails from Uptime Robot, a website monitoring service, which sent notifications about the operation of the database server db.raidforums.com or the RaidForums website.

iv. Steam Profile in Omnipotent's Name Tied to Coelho's Billing Information

45. The Omnipotent user profile on raidforums.com further contained a link to a Steam profile. Steam is a digital distribution platform, which offers digital rights management, multiplayer gaming, video streaming, and social networking services. Law enforcement received subscriber information for the Steam player name "Omnipotent." The Omnipotent account used the linkedbrew@gmail.com and billing information for Coelho.

v. Coelho Admits to using the "Downloading" Moniker in a Private Chat

46. Records received pursuant to a warrant to search Coelho's above-identified Discord account with the "Omnipotent" username further revealed that he admitted to another Discord user that he used the "Downloading" moniker on RaidForums in or around August 2018, and explained how he convinced buyers to conduct transactions through Omnipotent's

---

[3] Accounts include but are not limited to contact@raidforums.com and log@raidforums.com.

middleman service. The chats further revealed correspondence in which he often purported to closely collaborate with the "Downloading" moniker.

vi. IP Address Records

47. During the investigation, law enforcement obtained IP address records, which link accounts in the name of Omnipotent, Downloading, and Shiza to Coelho's suspected address in Portugal. In several instances, the Omnipotent, Downloading, and Shiza are using the same IP addresses at, or near the, same time.

vii. Namecheap Records for RaidForums.com

48. According to NameCheap records, the domains raidforums.com and raid.lol were as of September 4, 2018, registered to username Omnipotents, name: Kevin Maradona, and emails xlux@pm.me and unrivalled@pm.me. As stated above, Coelho has communicated with law enforcement on multiple occasions using unrivalled@pm.me. Further, he also left a review of the case agent on Google using the name Kevin Maradona. Moreover, a search of Coelho's phone revealed that Kevin Maradona is one of his personas.

49. Moreover, according to PayPal records, Diogo Santos with DOB: February 23, 2000, a URL of https://webhost.raid.lol and an address of Rua Sau Joan, Visu, Abraveses, PT 2515, is the holder of the PayPal account associated with xlux@pm.me. As discussed below, the Shiza account with Discord is also registered with xlux@pm.me.

viii. Cryptocurrency

50. Coelho's middleman service uses the bitcoin address 16hMesD4n3hMoRBAZ9t9Xi933nH4d6ZC9S. Blockchain analysis conducted on this wallet

address revealed numerous transactions to US-based cryptocurrency exchanges, such as Coinbase and Kraken. On March 17, 2018, funds were sent from Coelho's middleman bitcoin address to the wallet address 33VGGE9SwGKanQUYhnqZpJSXGFB2K5YmK1, which is held by Coinbase. According to Coinbase records, this wallet address is registered in the name of Diogo Santos Coelho, DOB: February 23, 2020, and the email address unrivalled@pm.me. Further, on June 19, 2019, funds were sent from Coelho's middleman wallet to the wallet address 33mmCm3s1YPs8rzWpQzuJ3qRRBvfehhBsp, which is held by Kraken. According to Kraken records, this wallet address is associated with the name Diogo Santos Coelho, 121B BR Pereiro Viseu, Portugal, 3515-169, DOB: February 23, 2020.

51. Taken together, the evidence conclusively proves that Diogo Santos Coelho is "Omnipotent," "Kevin Maradona," "Shiza" and the operator of RaidForums.

E. Coelho's Knowledge and Intent

52. The U.S. authorities' investigation indicates that Coelho and other RaidForums administrators knowingly and intentionally committed and aided the abetted the commission of the offenses charged in the Second Superseding Indictment, including by providing RaidForums members with a platform and tools needed to offer, buy, and sell access devices and means of identification. As explained above, Coelho's knowledge and intent is demonstrated by his years of administering and developing RaidForums, including portions of the platform dedicated to the buying and selling of stolen or hacked data containing access devices and other PII, his operation of a middleman service to support these deals, and his sale of illicit material of his own on RaidForums through the "Downloading" moniker. Moreover, Coelho has stated as much and

more in private communications with RaidForums members and others, as further highlighted below.

53. As an initial matter, there is substantial evidence that Coelho personally reviewed and verified many of the illicit materials and services that RaidForums members trafficked through his platform and middleman service. For instance, as noted above, Omnipotent's pinned post on RaidForums describing the "Official Middleman Policy" emphasized that "I will verify the contents of said files and make sure you are getting what you pay for," and even offered to provide servers through which sellers could transfer data to buyers. Records received from Discord likewise reveal that the Omnipotent Discord account described the procedure in a similar manner on or around December 10, 2018, and routinely sent messages on Discord to buyers and sellers confirming his verification of files. For example, on or around July 22, 2018, Omnipotent served as the middleman for a transaction that involved the sale of emails and passwords for accessing 580k users with a Bitcoin advertising company for a price of $1,000. In response to a series of inquiries from parties to the transaction, Omnipotent explained:

Omnipotent	Ok I downloaded the file
Trester	Just email: pass, I wrote about it
Omnipotent	Its emails and passwords
aaaax	ok
aaaax	580k lines?
Omnipotent	587983

54. Other messages show Coelho and other administrator(s) discussing difficulties associated with RaidForums maintaining substantial volume of breached databases on servers and infrastructure accounts that they controlled. For instance, in one Discord thread from on or

around September 4, 2019, an unidentified Discord user reported to Coelho, using Omnipotent, that certain "big files" had been omitted from the most recent upload. The omitted files were databases named after a range of companies around the world, including three major U.S. social media companies, an international credit reporting agency, and a major U.S. file hosting service.

55. Further, Coelho's correspondence and posts often confirmed that RaidForums was purposely and strategically designed to generate profits from the illicit trade of access devices and stolen data on his marketplace. For instance, a USSS agent observed on or about December 4, 2020, that the "RaidForums" account on Facebook, which listed the website's official contact information, described the platform as "a database sharing and marketplace forum. We have exclusive database breaches and leaks plus an active marketplace." Coelho's private correspondence was even clearer. For example, in or around February 2018, Coelho, using the Omnipotent Discord account, described his wealth as coming from having "a site where database breaches are shared and sold . . . like when myspace was hacked for example we will sell download to the full database." He further underscored how he profited from his members' hacking activities by stating, in relevant part, "[t]he more money I make the more customers I can drag in and the more money i make again and more customers e.t.c."

56. Coelho's private correspondence also reveals that he not only knowingly and intentionally aided and abetted the crimes of his members but also leveraged RaidForums and his position to participate in the same illicit activity. For instance, in a Discord thread from on or around July 10, 2018, Omnipotent boasted to another Discord user that he had hacked an "asian loan agent website and now have everyone's IDs and passports . . . ." He then continued, "lol

[expletive] i ***only hack stuff that will give me loads of monies . . . I am gonna sell this data now on my site*** and get around 30k EUR for it . . . ." (Emphasis added). In yet another Discord thread from on or around February 27, 2018, Omnipotent insisted to a different Discord user that they "never will" run out of databases to transfer on RaidForums. He continued that "we will switch over to another thing close to databases[,] or ***we will hack sites ourselves***." (Emphasis added). After the user expressed surprise, Omnipotent admitted that he was not engaging in legal activity and then attempted to recruit the user to hack for him. He said, in relevant part:

back thought u went legal
Omnipotent ye not me
Omnipotent we buy someone to hack them
Omnipotent thats where u come in
Omnipotent u hack everyone
back like who lul
Omnipotent u

57. Coelho's private correspondence on Discord and Twitter further reveal that he often helped arrange or even orchestrate transactions amongst RaidForums members, including by steering buyers to his "Downloading" persona. For example, records received from Twitter, Inc., a U.S. social media platform, revealed that Coelho's "Omnipotent" account on that platform helped a RaidForums member buy data that was apparently hacked from a U.S. flight distribution company. As part of that discussion in or around January 2019, Coelho directed the prospective buyer to "Downloading" on RaidForums, and then agreed to serve as the middleman for the transaction between the buyer and "Downloading"—*i.e.*, himself—for an additional fee. In other words, Coelho arranged with the buyer to profit from both the sale and facilitation of the stolen data.

58. In private correspondence, Coelho also evinced a clear understanding of how buyers on marketplaces, like RaidForums, use access devices they purchase to generate illicit proceeds. Indeed, Coelho often spoke favorably about the benefits of "carding"; a term that is generally understood to refer to the unlawful acquisition and use of data associated with debit and credit cards for the purposes of conducting fraudulent transactions and withdrawals. For instance, in a Discord thread from in or around December 2018, Omnipotent attempted to encourage another user to begin re-selling stolen credit cards in marketplaces. In relevant part, he explained that "carding is high risk kinda[,] but its super high reward fam." He further clarified that it was "dumb" to directly use the cards yourself, and instead encouraged the user to "just gather ccs and sell them" on markets and assured him that "gathering CCs is easy . . . ." As part of the discussion, he described how one of his friends—the once prominent carder known by the moniker "Joker's Stash"—had grown rich from reselling credit cards. When the user then questioned whether he could get cards from "my local mafia," Omnipotent further clarified how credit cards could be stolen through hacking. In relevant part, he stated "mafia don't collect ccs lol . . . so basically 2 ways of collecting ccs 1. u own a big site or hack a big site injecting code to save full cc info . . . ."

PROCEDURAL HISTORY OF THE CASE

The Charging Process

59. Under the federal law of the United States, a criminal prosecution is commenced when a grand jury files an Indictment. Institutionally, a grand jury, though an arm of the court, is

an independent body composed of private citizens—not less than 16 and not more than 23 people—whom the U.S. District Court selects at random from the residents of the judicial district in which the court resides. The purpose of the grand jury is to review the evidence of crimes presented to it by U.S. law enforcement authorities. After independently reviewing this evidence, each member of the grand jury must determine whether there is sufficient evidence to believe that a crime has been committed and that a particular person committed that crime. If at least 12 grand jurors find that the evidence they have reviewed is sufficient to believe that a particular person committed the crime, the grand jury may return an Indictment. An Indictment is a formal written accusation that charges the particular person, now a defendant, with a crime, and identifies the specific laws that the defendant is accused of violating.

60. If, after the return of the Indictment, U.S. authorities develop evidence demonstrating that additional charges are appropriate or that the existing charges should be modified, prosecutors may return to the grand jury, present any additional evidence, and ask the grand jury to return what is called a "Superseding Indictment." If, after the return of the Superseding Indictment, the grand jury is asked to make any further additions or modifications to the charges pursuant to the same process, the grand jury may return what is called a "Second Superseding Indictment." A Second Superseding Indictment is a new charging document that includes the additional or modified charges and supersedes or supplants the earlier indictments.

61. After a grand jury returns the Second Superseding Indictment, a warrant for the defendant's arrest may be issued at the direction of a United States District Judge or Magistrate Judge. Under United States law, the arrest warrant is simply a document authorizing a law

enforcement officer to take physical custody of a defendant and bring him to court to answer the charges contained in the Second Superseding Indictment. The type of detail on the face of an arrest warrant regarding the charges against a defendant can vary by district. The fact that an arrest warrant summarizes the outstanding charges in words, provides only some of the relevant statutory citations, or merely references the Second Superseding Indictment does not alter the validity of the arrest warrant to authorize a defendant's arrest on all of the charges contained in the corresponding Second Superseding Indictment. Under United States law, it is the Second Superseding Indictment, and not an arrest warrant, that controls the specific number and type of offenses with which the defendant is charged.

The Charges and Pertinent U.S. Law

62. On March 15, 2022, a grand jury sitting in the Eastern District of Virginia returned a Second Superseding Indictment charging Coelho with the following federal criminal offenses in violation of the laws of the United States:

Count One:	Conspiracy to Commit Access Device Fraud, in violation of Title 18, U.S. Code, Sections 1029(b)(2), and 3559(g)(l), which carries a maximum penalty of 10 years in prison.
Count Two:	Access Device Fraud – Using or Trafficking in an Unauthorized Access Device, in violation of Title 18, U.S. Code, Sections 1029(a)(2) and 2, which carries a maximum penalty of 10 years in prison.
Count Three:	Access Device Fraud — Possession of Fifteen or More Unauthorized Access Devices, in violation of Title 18, U.S. Code, Sections 1029(a)(3) and 2, which carries a maximum penalty of 10 years in prison.

Counts Four and Five:	Access Device Fraud – Unauthorized Solicitation, in violation of Title 18, U.S. Code, Sections 1029(a)(6) and 2, which carries a maximum penalty of 10 years in prison.
Count Six:	Aggravated Identity Theft, in violation of Title 18, U.S. Code, Sections 1028A(a)(1) and 2, which carries a mandatory two years of imprisonment consecutive to any other term of imprisonment imposed.

63. This Second Superseding Indictment was filed with the U.S. District Court for the Eastern District of Virginia. It is the practice of the U.S. District Court for the Eastern District of Virginia to retain the original Second Superseding Indictment and file it with the records of the court. Therefore, I have obtained a copy of the Second Superseding Indictment from the clerk of the court and have redacted the foreperson's signature. I have attached the Second Superseding Indictment to this affidavit as **Exhibit 1**.

64. On March 16, 2022, based on the filing of the Second Superseding Indictment, the United States District Court for the Eastern District of Virginia issued a warrant for Coelho's arrest. The arrest warrant remains valid and executable to apprehend Coelho on the charges set forth in the Second Superseding Indictment. It is the practice of the U.S. District Court for the Eastern District of Virginia to retain the original arrest warrant and file it with the records of the court. Therefore, I have obtained from the clerk of the court a copy of the arrest warrant for Coelho and have attached it to this affidavit as **Exhibit 2**.

65. Each count of the Second Superseding Indictment charges a separate offense. Each offense is punishable under a statute that: was the duly enacted law of the United States at the time the offense was committed; was the duly enacted law of the United States at the time the

Second Superseding Indictment was filed; and is currently in effect.

66. Each offense is a felony offense punishable under U.S. law by more than one year of imprisonment. I have attached copies of the pertinent sections of these statutes and the applicable penalty provisions to this affidavit as **Exhibit 3**.

Elements for Counts One through Five (Access Device Fraud and Related Counts)

Count One (Conspiracy – 18 U.S.C. § 1029(b)(2))

67. Count One charges Coelho with conspiracy to commit, and conspiracy to aid and abet, access device fraud. To satisfy its burden of proof and convict Coelho on this Count, the United States must establish that:

a. The defendant agreed with at least one other person;

b. The agreement was to violate, and/or aid abet violations of, 18 U.S.C. § 1029(a)(2) and/or 1029(a)(3) and/or 1029(a)(6); and

c. A conspirator committed at least one overt act in furtherance of the conspiracy.

68. There are several features regarding the crime of conspiracy that bear mentioning.

a. First, under U.S. law, a conspiracy is an agreement between two or more people to commit one or more criminal offenses.

b. Second, the agreement on which the conspiracy is based need not be expressed in writing or in words but may be simply a tacit understanding by two or more persons to do something illegal.

c. Third, each member of the conspiracy becomes a partner or agent of every

other member. A person may become a member of a conspiracy without full knowledge of all of the details of the unlawful scheme or the identities of all the other members of the conspiracy. If a person has an understanding of the unlawful nature of a plan and knowingly and willfully agrees to it, joining in the plan, he is guilty of conspiracy even though he did not participate before and may play only a minor part. A conspirator can be held criminally responsible for all reasonably foreseeable actions undertaken by other conspirators in furtherance of the criminal partnership. Moreover, because of this partnership, statements made by a conspirator during and in furtherance of the criminal conspiracy are admissible in evidence not only against that conspirator, but also against all other members of the conspiracy.

d. Fourth, the crime of conspiracy is an independent offense, separate and distinct from the commission of any specific "substantive crimes." Consequently, a conspirator can be found guilty of the crime of conspiracy to commit an offense even where the substantive crime that was the purpose of the conspiracy is not committed.[4]

e. Fifth, a conspirator can be found guilty of the crime of conspiracy upon evidence that the object of the conspiracy was to aid and abet the commission of a substantive crime. Aiding and abetting, under Title 18, U.S. Code, Section 2, provides that whoever commands, procures, assists in, or causes the commission of a crime shall be held accountable

---

[4] The Congress of the United States has deemed it appropriate to make conspiracy, standing alone, a separate crime, even if the conspiracy is not successful, because collective criminal planning poses a greater threat to the public safety and welfare than individual conduct and increases the likelihood of success of a particular criminal venture.

and punished in the same manner as the principal, or the person who actually carried out the task. Accordingly, under an aiding and abetting theory, a conspirator who agrees with another to knowingly and intentionally command, procure, assist in, or cause the commission of a crime shall be held accountable and punished in the same manner as the principal, or the person who actually carried out the task. Based on this theory of liability, Coelho may be found guilty of Count One as long as he conspired with at least one other person with the objective of intentionally and knowingly helping, encouraging, or willfully causing others to commit at least one of the substantive crimes identified in Count One —*i.e.*, 18 U.S.C. § 1029(a)(2), 1029(a)(3) or 1029(a)(6).

69. Regarding the maximum penalty for Count One, 18 U.S.C. §1029(b)(2) provides for imprisonment "not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section." In turn, 18 U.S.C §1029(c) provides for a maximum penalty of ten years' imprisonment for the objects of the conspiracy – violations of 18 U.S.C. § 1029(a)(2) (Count 2) and/or 1029(a)(3) (Count 3) and/or 1029(a)(6) (Counts 4 and 5), or aiding and abetting such violations under 18 U.S.C. § 2 – that are charged in the Second Superseding Indictment. Accordingly, the maximum penalty for Count One would otherwise be five years. However, Count One pleads a sentencing enhancement under 18 U.S.C. Section 3559(g)(l) that doubles the maximum term of imprisonment that may be imposed for a conviction on this count. To satisfy its burden of proof on this sentencing enhancement, the

United States must additionally establish that the defendant (a) falsely registered[5] a domain name; and (b) knowingly used that domain name in the course of the offense. Thus, by pleading this sentencing enhancement, the maximum penalty for Count One is doubled from five years to ten years.

Count Two (Access Device Fraud - 18 U.S.C. § 1029(a)(2))

70. Count Two charges Coelho with using or trafficking in an unauthorized access device.[6] To satisfy its burden of proof and convict Coelho on this Count, the United States must establish that:

a. The defendant trafficked in or used one or more unauthorized access devices;

b. By such conduct, the defendant obtained anything of value aggregating $1,000 or more during a one-year period;

c. The conduct affected interstate or foreign commerce; and

d. The defendant did so knowingly with the intent to defraud.

71. Count Two (as well as Counts Three through Six) charge Coelho with aiding and abetting the unknown sellers with the commission of the crimes charged in these counts. As noted above, aiding and abetting, under Title 18, U.S. Code, Section 2, provides that whoever

---

[5] "Falsely registers" means "register in a manner that prevents the effective identification of or contact with the person who registers."

[6] An "unauthorized access device" is defined in 18 U.S.C.§1029(e)(2), and (e)(3), and includes email addresses and associated passwords.

commands, procures, assists in, or causes the commission of a crime shall be held accountable and punished in the same manner as the principal, or the person who actually carried out the task. Additionally, whoever willfully causes an act to be done that would be a federal crime if directly performed by him is punishable as a principal.

72. Based on this theory of liability, Coelho may be found guilty of Counts Two though Six even if he did not personally perform every act involved in the commission of the crimes charged, as long as he intentionally helped, encouraged, or willfully caused the sellers to commit the crimes.

Count Three (Access Device Fraud – 18 U.S.C. § 1029(a)(3))

73. Count Three charges Coelho with possession of fifteen or more unauthorized access devices. To satisfy its burden of proof and convict Coelho on this Count, the United States must establish that:

a. The defendant knowingly possessed fifteen or more access devices;

b. Those devices were counterfeit or unauthorized;

c. The defendant possessed those devices with the intent to defraud; and

d. The defendant's conduct affected interstate or foreign commerce.

Counts Four and Five (Access Device Fraud – 18 U.S.C. § 1029(a)(6))

74. Counts Four and Five charge Coelho with unauthorized solicitation. To satisfy its burden of proof and convict Coelho on these Counts, the United States must establish that:

a. The defendant knowingly solicited a person for the purpose of offering an access device;

b. The defendant solicited that person without authorization of the issuer of the access device;

c. The defendant acted with the intent to defraud; and

d. Interstate commerce was affected.

Summary of the Evidence for Counts One Through Five

75. The government will meet the elements of Counts One through Five by proving that: (1) Coelho knowingly operated RaidForums and the middleman service advertised on RaidForums; (2) Coelho through his middleman service conspired and aided and abetted others in purchasing and selling a myriad of data that qualifies as access devices and means of identification including, but not limited to, bank routing and account numbers, and stolen payment card data, such as payment card account numbers, card verification values or card verification codes, card expiration dates, or personal identification numbers, and the personal identifying information of individuals, such as names, email addresses, and social security numbers, and hacked databases of login credentials, such as usernames and associated passwords, for access to online accounts issued by United States entities; (3) Coelho was aware that the data was being sold without the authorization of the owner of the data; (4) Coelho charged the purchaser and seller a percentage of the agreed purchase price for his middleman service; (5) Coelho's middleman service was used for each of the substantive overt acts and Counts Two through Five; (6) Coelho was well aware that his website was used for this illicit activity and that each of the transactions was done with the intent to defraud the rightful owner of the data; and (7) the transactions affected interstate or foreign commerce.

76. At trial, the United States anticipates relying on the following evidence, among other evidence, to establish the elements required for Counts One through Five:

a. Coelho's private communications on RaidForums, Discord, and Twitter, which reflect that Coelho understood RaidForums was being used by others to illegally sell access devices, means of identification, hacking tools, databases of hacked data, and other illegal services. Coelho's private communications also show his own involvement in selling access devices, means of identification, and other illegally obtained data, and his understanding that the selling of such information would be used to defraud others.

b. Testimony of the victims, including individual credit card holders and representatives from the victim companies, who will all state that they did not authorize Coelho or others to use, possess, or traffic in their data.

c. Law enforcement witnesses who will testify to the four individual transactions for credit card data, banking and routing information, and usernames and associated passwords, as previously described in paragraphs 16, 18-23, 25-26, and 28-30.

d. A law enforcement witness who will testify to the contents extracted from Coelho's electronics, which were lawfully seized and searched when Coelho attempted to enter the United States. The contents of the devices clearly establish that Coelho is Omnipotent, Downloading, Kevin Maradona, and the owner and operator of RaidForums.

e. A law enforcement witness who will introduce into evidence relevant communications, registration records, and login activity obtained from a back-end copy of the RaidForums server.

f. Bank records for Coelho's PayPal account and other cryptocurrency accounts, which reflect that Coelho had access to, and was the owner of, accounts that received payment from RaidForums transactions and Coelho's middleman service.

g. IP records establishing that the Omnipotent, Downloading, and Shiza accounts all use the same IP address, and sometimes simultaneously use the same IP address, which shows that the user of the monikers is accessing the internet, including the RaidForums website, from his known home in Portugal.

77. The United States anticipates relying on the following evidence, among other evidence, to prove the elements of the sentencing enhancement pled in Count One:

a. Namecheap and Namesilo records that show Coelho registered, transferred, and renewed the registration of the domain names raidforums.com, raid.lol, and rf.ws, using false or fictitious information designed to prevent his identification, including by using the username "Omnipotents" or "Omnipotent," and aliases such as "Kevin Maradona."

b. Posts from RaidForums that show the domain names raidforums.com, raid.lol, and rf.ws were used to host the RaidForums website that facilitated Count 1; and

c. Testimony of law enforcement agents who accessed the RaidForums website through the domain names raidforums.com, raid.lol, and rf.ws.

Elements for Count Six (Aggravated Identity Theft — 18 U.S.C. § 1028A(a)(1))

78. Count Six charges Coelho with aggravated identity theft. To satisfy its burden of proof and convict Coelho on Count Six, the United States must establish that:

a. The defendant knowingly transferred, possessed, or used;

b. Without lawful authority;

c. A means of identification[7] of another person, who may be living or dead, knowing that the identifiers belonged to another individual; and

d. The defendant did so during and in relation to [one of the felonies enumerated in 1028A(c), which here is access device fraud].

79. At trial, the United States anticipates relying on the following evidence, among other evidence, to establish the elements required for Count Six:

a. As further detailed above, RaidForums posts where Coelho, who was using the moniker "Downloading," advertised the sale of approximately 2.3 million records of credit card data, including names, addresses and phone numbers. For instance, in one post, Coelho stated that the credit card numbers were "fresh" and that he was "able to test 100 cards with random charges and 93 out of the 100 were working."

b. Communications between an undercover law enforcement officer and Coelho, who was using the monikers Omnipotent, Downloading, and Shiza.

c. Bitcoin records tracing the payment made by law enforcement to Coelho's bank account.

d. Communications and other information obtained from Coelho's electronic devices, which were lawfully seized and searched in the United States establishing that Coelho is

---

[7] A "means of identification" is defined in Title 18, United States Code, Section 1028(d)(7).

Omnipotent, Downloading, and Kevin Maradona.

e. Private communications where Coelho states that he is Downloading;

f. IP records establishing that the Omnipotent, Downloading, and Shiza accounts all use the same IP address, and sometimes simultaneously use the same IP address, which shows that the user of the monikers is accessing the internet from the same location in Portugal.

DIOGO SANTOS COELHO'S LOCATION

80. According to information received from UK authorities, Coelho was arrested on January 31, 2022, based on an Interpol diffusion notice submitted by the United States. He is in the custody of United Kingdom authorities.

IDENTIFICATION INFORMATION FOR DIOGO SANTOS COELHO

81. Diogo Santos Coelho is a citizen of Portugal born on February 23, 2000 in Viseu, Portugal. He is white male with brown or black hair.

82. As stated above, Coelho confirmed to the lead FBI case agent that Omnipotent was his online alias and provided the FBI case agent with a photo of his Citizen Card, which is attached as **Exhibit 4**.

SURRENDER OF PROPERTY

83. Pursuant to Article 16 of the Annex to the U.S.—UK Extradition Instrument, it is requested that any items relevant to the charged offenses and found in Coelho's possession at the time of his arrest be delivered to the United States if he is found to be extraditable.

CONCLUSION

84. The following attachments support this request for the extradition of Coelho:

a. Exhibit 1 is a copy of the redacted Second Superseding Indictment.

b. Exhibit 2 is a copy of the arrest warrant against Coelho.

c. Exhibit 3 is a copy of the pertinent sections of the following statutes and their penalties:

(1) Title 18, U.S. Code, Section 1028(d)(7);

(2) Title 18, U.S. Code, Section 1029(e)(1), (2), and (3);

(3) Title 18, U.S. Code, Section 1029(b)(2);

(4) Title 18, U.S. Code, Section 1029(a)(2);

(5) Title 18, U.S. Code, Section 1029(a)(3);

(6) Title 18, U.S. Code, Section 1029(a)(6);

(7) Title 18, U.S. Code, Section 1029(c);

(8) Title 18, U.S. Code, Section 3559(g)(l));

(9) Title 18, U.S. Code, Sections 1028A(a)(1) and 1028A(c)(4); and

(10) Title 18, U.S. Code, Section 2

d. Exhibit 4 is a copy of a photograph of Coelho.

85. I have thoroughly reviewed the government's evidence against Coelho and attest that this evidence indicates that Coelho is guilty of the offenses charged in the Second Superseding Indictment.

Executed this 17th day of March 2022, at Alexandria, Virginia, United States of America.

BY: _____
Carina A. Cuellar
Assistant U.S. Attorney

Signed and sworn to before me this ____ day of March 2022, at Alexandria, Virginia, United States of America.

Digitally signed by Ivan Davis
Date: 2022.03.17 14:47:19 -04'00'

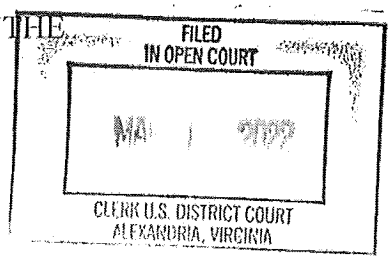
_____
The Honorable Ivan D. Davis
United States Magistrate Judge

EXHIBIT 1

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

DIOGO SANTOS COELHO,
a/k/a "Omnipotent"
a/k/a "Downloading"
a/k/a "Shiza"
a/k/a "Kevin Maradona"

Defendant.

FILED UNDER SEAL

Case No. 1:21-cr-114

Count 1: Conspiracy to Commit Access Device Fraud
(18 U.S.C. §§ 1029(b)(2) and 3559(g)(1))

Count 2: Access Device Fraud — Using or Trafficking in an Unauthorized Access Device
(18 U.S.C. §§ 1029(a)(2) and 2)

Count 3: Access Device Fraud — Possession of Fifteen or More Unauthorized Access Devices
(18 U.S.C. §§ 1029(a)(3) and 2)

Counts 4-5: Access Device Fraud — Unauthorized Solicitation
(18 U.S.C. §§ 1029(a)(6) and 2)

Count 6: Aggravated Identity Theft
(18 U.S.C. §§ 1028A(a)(1) and 2)

Forfeiture Notice

SECOND SUPERSEDING INDICTMENT

March 2022 Term—at Alexandria, Virginia

THE GRAND JURY CHARGES THAT:

General Allegations

At all times material to this Indictment:

1. Defendant DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), was a Portuguese national who resided in Portugal.

2. From at least in or around January 1, 2015 to on or about January 31, 2022, COELHO controlled and was the chief Administrator of a website www.Raidforums.com (the "RaidForums website"), which he operated with the help of other website Administrators. COELHO used the monikers "Omnipotent" and "Downloading" on the RaidForums website.

3. The RaidForums website was hosted on a server located outside the United States.

4. The RaidForums website served as a platform where members could solicit for sale, sell, and purchase contraband including, but not limited to, stolen access devices as defined in Title 18, United States Code, Section 1029(e)(1), means of identification as defined in Title 18, United States Code, Section 1028(d)(7), hacking tools, databases of hacked data, and other illegal services, such as hacking-for-hire.

5. An individual could access the RaidForums website without a membership. However, the website required an individual to sign up for a membership to solicit items for sale or purchase items. The RaidForums website offered four tiers of membership options, including in order of cost: (1) free membership; (2) VIP membership; (3) MVP membership; and (4) God membership. The more expensive the membership, the more access a user could get to the RaidForums website. The God membership, for example, offered almost unlimited access to the RaidForums website and features.

6. The RaidForums website sold "credits" to members, which granted members access to privileged areas of the website and enabled members to "unlock" and download stolen access devices, means of identification, and data from compromised databases, among other

items. Members could also earn credits through other means including, but not limited to, by posting instructions on how to commit certain illegal acts.

7. The RaidForums website had different forums where members could post about different subjects and offer items for sale. The forums included "Cracking," "Leaks," and "Marketplace," among others. The "Leaks" forum had a sub-forum entitled the "Leaks Market." The "Leaks Market" description stated that it was "[a] place to buy/sell/trade databases and leaks." The "Leaks Market" included for-sale listings for bank routing and account numbers, and stolen payment card data, such as payment card account numbers, card verification values ("CVV") or card verification codes ("CVC"), card expiration dates, or personal identification numbers. The "Leaks Market" sub-forum also displayed posts listing offers to sell the personal identifying information of individuals, such as names, email addresses, and social security numbers, and hacked databases of login credentials, such as usernames and associated passwords, for access to online accounts issued by United States entities.

8. COELHO offered an "Official Middleman Service" for a fee on the RaidForums website. More specifically, COELHO offered to accept cryptocurrency from the purchaser and files, including stolen access devices and means of identification, from the seller. COELHO then verified the contents of the files and conversed with the buyer and seller. Once the parties were satisfied, COELHO released the funds to the seller and the files, including stolen access devices and means of identification, to the purchaser.

COUNT 1

(Conspiracy to Commit Access Device Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

9. The Grand Jury re-alleges and incorporates by reference the General Allegations of this Indictment.

10. Beginning from at least in or around June 2016 and continuing to on or about January 31, 2022, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendant, DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), did knowingly and with the intent to defraud, combine, conspire, confederate, and agree with other persons both known and unknown to the Grand Jury, to commit and aid and abet the following offenses:

a. To knowingly and with the intent to defraud, traffic in and use one and more unauthorized access devices during a one-year period, to wit payment card data, bank routing and account numbers, social security numbers, and login credentials, including usernames and associated passwords, for access to online accounts provided by United States entities, and by such conduct obtain things of value aggregating $1,000 and more during that period, in violation of 18, United States Code, Sections 1029(a)(2) and 2;

b. To knowingly and with the intent to defraud, possess fifteen and more unauthorized access devices, to wit payment card data, bank routing and account numbers, social security numbers, and login credentials, including usernames and associated passwords, for access to online accounts issued by United States

entities, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 1029(a)(3) and 2; and

c. Without the authorization of the issuers of access devices, knowingly and with the intent to defraud, solicit individuals with the purpose of selling unauthorized access devices, to wit payment card data, bank routing and account numbers, social security numbers, and login credentials, including usernames and associated passwords, for access to online accounts issued by United States entities, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 1029(a)(6) and 2.

11. COELHO will be first brought to and arrested in the Eastern District of Virginia.

WAYS, MANNERS, AND MEANS

The primary purpose of the conspiracy was to make money through the trafficking in stolen access devices. The ways, manners, and means by which the defendant, DIOGO SANTOS COELHO, and his co-conspirators carried out the primary purpose of the conspiracy included, but were not limited to, the following:

12. It was part of the conspiracy that the defendant controlled and operated the RaidForums website.

13. It was further part of the conspiracy that the defendant operated the RaidForums website with the help of co-conspirators, who operated as Administrators of the RaidForums website. The defendant and other Administrators designed and administered the website's software and computer infrastructure; established and enforced website's rules; and created and managed sections of the website dedicated to promoting the buying and selling of contraband, including the "Leaks Market" sub-forum.

14. It was further part of the conspiracy that the defendant and his co-conspirators posted offers to sell stolen access devices on the RaidForums website, including, but not limited to, payment card data, bank routing and account numbers, social security numbers, and login credentials, including usernames and associated passwords, for access to online accounts issued by United States entities.

15. It was further part of the conspiracy that the defendant offered to sell "credits" to users, who could then use these "credits" to purchase stolen access devices on the RaidForums website, among other items.

16. It was further part of the conspiracy that the defendant offered a fee-based service, described as an "Official Middleman Service" on the RaidForums website, which enabled purchasers and sellers to verify the means of payment and contraband files being sold prior to executing the purchase and sale.

17. It was further part of the conspiracy that the defendant and his co-conspirators accepted payment in cryptocurrency in return for the sale of stolen access devices.

18. It was further part of the conspiracy that the defendant and his co-conspirators knowingly falsely registered a domain name, including RaidForums.com, and knowingly used that domain name in the course of committing the offense charged in Count 1, in violation 18 U.S.C. § 3559(g)(l).

OVERT ACTS

In furtherance of the conspiracy, and to effect the objects thereof, the defendant, DIOGO SANTOS COELHO, and his co-conspirators committed overt acts in the Eastern District of Virginia and elsewhere, including, but not limited to, the following:

19. On or about June 6, 2018, COELHO, using the moniker "Omnipotent," transferred the false registration of the domain "Raidforums.com" to a U.S.-based domain registrar based in Phoenix, Arizona using the alias "Kevin Maradona." COELHO falsely registered the domain name knowing that it was used to support the RaidForums website in furtherance of the conspiracy.

20. On or about July 24, 2018, COELHO, using the moniker "Omnipotent," made a posting on the RaidForums website, in which he advertised an "Official Middleman Service." The posting indicated that the service would enable both buyers and sellers to complete their transactions, and that COELHO would verify the contents of files to ensure buyers received the data that they expected to purchase.

21. On or about October 18, 2018, an unknown co-conspirator using the moniker "mariecurie" made a posting on the RaidForums website, which offered for sale stolen access devices, to wit, usernames and associated passwords for access to user accounts issued by an electronic commerce company in the United States ("Company 1").

22. On or about October 22, 2018, in the Eastern District of Virginia and elsewhere, an undercover law enforcement officer used eight credits, which the officer purchased on the RaidForums website, to "unlock" and download the Company 1 usernames and associated passwords that user "mariecurie" offered for purchase.

23. On or about December 16, 2018, COELHO, who was using the moniker "Downloading," made a posting on the RaidForums website, which offered for sale 2.3 million payment card account numbers, including the names, addresses, and phone numbers associated with the payment card account numbers, which were purportedly obtained from a breach of records belonging to United States hotels.

24. On or about February 5, 2019, in the Eastern District of Virginia and elsewhere, COELHO, who was using the moniker "Downloading," informed an undercover law enforcement officer that the stolen payment card data described in paragraph 23 were still available for sale.

25. On or about March 4, 2019, in the Eastern District of Virginia and elsewhere, COELHO, who was using the moniker "Downloading," provided an undercover law enforcement officer with three stolen access devices, to wit, payment card account numbers, card verification values, expiration dates, and the names associated with the payment cards. COELHO agreed to this exchange to convince the undercover law enforcement officer that "Downloading" could be trusted to sell approximately 1.1 million stolen access devices in exchange for a Bitcoin amount that was equivalent to approximately $4,000 at the time.

26. On or about March 5, 2019, in the Eastern District of Virginia and elsewhere, COELHO, who was using the monikers "Downloading," "Omnipotent," and "Shiza," arranged to both sell and serve as the middleman in the transaction to sell approximately 1.1 million stolen access devices to the undercover law enforcement officer. COELHO received a Bitcoin amount that was then equivalent to approximately $4,000; however, he did not provide the stolen access devices.

27. On or about April 5, 2020, an unknown co-conspirator using the moniker "fairbanksfires" made a posting on the RaidForums website, which offered for sale stolen access devices associated with an online tax filing company in the United States. The stolen access devices included, but were not limited to, social security numbers, email addresses, passwords, and bank routing and account numbers.

28. On or about April 25, 2020, COELHO, who was using the moniker "Omnipotent," executed his middleman service and aided and abetted "fairbanksfires" in selling stolen access devices to a confidential human source ("CHS"), who was working with the Federal Bureau of Investigation. The CHS transferred a Bitcoin amount that was then equivalent to approximately $4,000 to COELHO in furtherance of this transaction. COELHO then provided the CHS with a link, which enabled the CHS to download the stolen access devices.

29. On or about April 27, 2020, the CHS communicated to COELHO that the funds could be released to "fairbanksfires."

30. From on or about October 26, 2016 until at least on or about July 24, 2020, the RaidForums website offered for sale in its Official Database Index a 2015 database, which included stolen access devices, namely associated email addresses, passwords, names, and addresses for gaining access to online customer accounts issued by a major broadcasting and cable company in the United States ("Company 2").

31. On or about July 24, 2020, in the Northern District of Illinois and elsewhere, an undercover law enforcement officer used eight credits, which the officer purchased on the RaidForums website, to "unlock" and download the Company 2 database, as described in paragraph 30.

32. On or about August 11, 2021, a known individual using the moniker "SubVirt" posted on the RaidForums website an offer to sell recently hacked data with the following title: "SELLING-124M-U-S-A-SSN-DOB-DL-database-freshly-breached." This post provided a small sample of data, which included names and dates of birth, and priced the information at six (6) Bitcoin.

33. On or about August 14, 2021, a known individual using the moniker "SubVirt" created a revised post on the RaidForums website offering to sell recently hacked data with the following title: "SELLING 30M SSN + DL + DOB database." This post provided a small sample of data, which included names and dates of birth, and priced the information at six (6) Bitcoin. The post also provided a Telegram handle as contact information for interested buyers. A subsequent post confirmed that the hacked data belonged to a major telecommunications company and wireless network operator that provides services in the United States ("Company 3").

34. On or about August 17, 2021, COELHO, who was using the moniker "Omnipotent," executed his middleman service and aided and abetted "SubVirt" in selling a sample of confidential and sensitive information and other data of value obtained during an unlawful computer intrusion, including, but not limited to, customer names, social security numbers, dates of birth, driver's license numbers, phone numbers, billing account numbers, customer relationship manager information, Mobile Station Integrated Services Digital Network (MSISDN) information, International Mobile Subscriber Identity (IMSI) numbers, and International Mobile Equipment Identity (IMEI) numbers to a third-party then operating on behalf of Company 3. The third-party used COELHO's middleman service to transfer a Bitcoin amount that was then equivalent to approximately $50,000 to "SubVirt."

35. On or about August 22, 2021, COELHO, who was using the moniker "Omnipotent," executed his middleman service and aided and abetted "SubVirt" in selling complete database sets containing confidential and sensitive information and other data of value obtained during an unlawful computer intrusion, including, but not limited to, customer names, social security numbers, dates of birth, driver's license numbers, phone numbers, billing account

numbers, customer relationship manager information, MSISDN information, IMSI numbers, and IMEI numbers to a third-party then operating on behalf of Company 3. The third-party used COELHO's middleman service to transfer a Bitcoin amount that was then equivalent to approximately $150,000 to "SubVirt."

(All in violation of Title 18, United States Code, Sections 1029(b)(2) and 3559(g)(1))

COUNT 2

(*Access Device Fraud — Using or Trafficking in an Unauthorized Access Device*)

THE GRAND JURY FURTHER CHARGES THAT:

36. The factual allegations in paragraphs 1 through 8 and 23 to 26 are re-alleged and incorporated as if fully set forth below.

37. From on or about February 5, 2019 until on or about March 5, 2019, in the Eastern District of Virginia and elsewhere, the defendant, DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), knowingly and with the intent to defraud, did traffic in and use one and more unauthorized access devices, to wit, payment card account numbers, card verification values, expiration dates, and other associated information, during a one-year period, to wit, from January 1, 2019, through December 31, 2019, and by such conduct did obtain things of value aggregating $1,000 and more during that period, to wit, the Bitcoin worth approximately $4,000 on or about March 5, 2019, said trafficking affecting interstate and foreign commerce, in that the trafficking occurred via the Internet, and between computers located inside the Commonwealth of Virginia, and computers located outside of the Commonwealth of Virginia.

(In violation of Title 18, United States Code, Sections 1029(a)(2) and 2)

COUNT 3

(*Access Device Fraud — Possession of Fifteen or More Unauthorized Access Devices*)

THE GRAND JURY FURTHER CHARGES THAT:

38. The factual allegations in paragraphs 1 through 8 and 30 to 31, are re-alleged and incorporated as if fully set forth below.

39. From on or about October 26, 2016 until on or about July 24, 2020, within the jurisdiction of the United States and in an offense begun and committed outside the jurisdiction of a particular State or district, including in Portugal, Germany, and elsewhere, the defendant, DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), did knowingly and with intent to defraud, possess fifteen or more unauthorized access devices as defined by 18 U.S.C. § 1029(e)(2), and (e)(3), to wit, email addresses, associated passwords, and other related information to access the customer accounts of subscribers to a major broadcasting and cable company in the United States, said possession affecting interstate and foreign commerce.

40. COELHO will be first brought to and arrested in the Eastern District of Virginia.

(In violation of Title 18, United States Code, Sections 1029(a)(3) and 2)

COUNTS 4-5

(Access Device Fraud —Unauthorized Solicitation)

THE GRAND JURY FURTHER CHARGES THAT:

41. The factual allegations in paragraphs 1 through 8 and 21 through 26 are re-alleged and incorporated as if fully set forth below.

42. On or about the dates identified below, in the Eastern District of Virginia and elsewhere, the defendant, DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), did knowingly and with intent to defraud solicit other persons for the purpose of offering unauthorized access devices as defined by 18 U.S.C. § 1029(e)(2), and (e)(3), to wit, the access devices as set forth below in each count, without the authorization of the issuer of the access devices, said solicitation affecting interstate and foreign commerce, in that the solicitation occurred via the Internet, and between computers located inside the Commonwealth of Virginia, and computers located outside of the Commonwealth of Virginia.

Count	Date	Description of Access Device
4	October 18 to 22, 2018	Usernames and passwords for access to online accounts issued by an electronic commerce company in the United States
5	December 16, 2018 to March 5, 2019	Payment card account numbers, card verification values, and expiration dates

(In violation of Title 18, United States Code, Sections 1029(a)(6) and 2)

COUNT 6

(*Aggravated Identity Theft*)

THE GRAND JURY FURTHER CHARGES THAT:

43. The factual allegations in paragraphs 1 through 8 and 23 through 26 are re-alleged and incorporated as if fully set forth below.

44. From on or about December 16, 2018 until on or about March 5, 2019, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendant, DIOGO SANTOS COELHO (a/k/a "Omnipotent," "Downloading," "Shiza," and "Kevin Maradona"), did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, access device fraud, in violation of 18 U.S.C. §§ 1029(a)(2) and (a)(6) as alleged in Counts 2 and 5 of this Indictment, knowing that the means of identification belonged to another actual person.

45. COELHO will be first brought to and arrested in the Eastern District of Virginia.

(In violation of Title 18, United States Code, Sections 1028A(a)(1) and 2)

FORFEITURE NOTICE

THE GRAND JURY HEREBY FINDS THAT:

46. There is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

47. The defendant is hereby notified, pursuant to Fed.R.Crim.P. 32(a), that upon conviction of the offenses set forth in Counts 1-5 of this Indictment, the defendant, DIOGO SANTOS COELHO, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(B) any property constituting, or derived from, proceeds the defendant obtained directly or indirectly, as the result of such violation; and pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property used or intended to be used to commit the offenses. The assets subject to forfeiture include, but are not limited to, the following:

a. The domain name RaidForums.com;

b. The domain name raid.lol;

c. The domain name rf.ws;

d. One Samsung smartphone model SM-G950F;

e. One Lenovo tablet with serial number HGER85N8;

f. One Acer laptop with serial number NXGNLEB00272108E6B7200;

g. One Yubico authentication device;

h. One Sony Digital Camera with serial number 4098514; and

i. A money judgment in the amount of not less than $215,571, representing the proceeds the defendant obtained as a result of the violations described in this Indictment.

48. Pursuant to 21 U.S.C. § 853(p), the defendant shall forfeit substitute property, if, by any act or omission of the defendant, the property referenced above cannot be located upon the exercise of due diligence; has been transferred, sold to, or deposited with a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty.

(All in accordance with Title 18, United States Code, Section 982(a)(2)(B), Title 18, United States Code, Section 1029(c)(1)(C), and Federal Rule of Criminal Procedure 32.2).

A TRUE BILL

FOREPERSON

Jessica D. Aber
United States Attorney

By: _____
Carina A. Cuellar
Assistant United States Attorney

Aarash A. Haghighat
Senior Counsel
Computer Crime and Intellectual Property Section
United States Department of Justice

EXHIBIT 2

AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

United States of America
v.
DIOGO SANTOS COELHO
a/k/a "Omnipotent"
a/k/a "Downloading"
a/k/a "Shiza"
a/k/a "Kevin Maradona"

Defendant

Case No. 1:21-cr-114

UNDER SEAL

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) Diogo Santos Coelho, a/k/a "Omnipotent", "Downloading", "Shiza", "Kevin Maradona" ,

who is accused of an offense or violation based on the following document filed with the court:

☐ Indictment ☑ Superseding Indictment ☐ Information ☐ Superseding Information ☐ Complaint

☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

Conspiracy to Commit Access Device Fraud, in violation of Title 18, United States Code, Sections 1029(b)(2) and 3559(g)(l)
Access Device Fraud — Using or Trafficking in an Unauthorized Access Device, in violation of Title 18, United States Code, Sections 1029(a)(2) and 2);
Access Device Fraud — Possession of Fifteen or More Unauthorized Access Devices, in violation of Title 18, United States Code, Sections 1029(a)(3) and 2);
Access Device Fraud — Unauthorized Solicitation, in violation of Title 18, United States Code, Sections 1029(a)(6) and 2); and
Aggravated Identity Theft, in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2)

Date: 3/16/22

Issuing officer's signature

City and state: Alexandria, Virginia

Judith Lanham, D. Clerk

Printed name and title

INFORMATION COPY ONLY

NOTICE: BEFORE ARREST, VALIDATE THROUGH NCIC. ORIGINAL HELD BY U.S. MARSHAL.

Return

This warrant was received on *(date)* _____, and the person was arrested on *(date)* _____

at *(city and state)* _____.

Date: _____

Arresting officer's signature

Printed name and title

EXHIBIT 3

1. **Title 18, United States Code, Section 1028(d)(7)**

the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029(e)).

2. **Title 18, United States Code, Sections 1029(e)(1), (2), and (3);**

(e) As used in this section—

(1) the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

(2) the term "counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(3) the term "unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.

3. **Title 18, United States Code, Section 1029(b)(2)** provides in relevant part:

Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

4. **Title 18, United States Code, Section 1029(a)(2)** provides, in relevant part:

Whoever knowingly and with the intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period… shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

5. **Title 18, United States Code, Section 1029(a)(3)** provides, in relevant part:

Whoever knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices… shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

6. **Title 18, United States Code, Section 1029(a)(6)** provides, in relevant part:

Whoever, without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of (A) offering an access device . . . shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

7. **Title 18, United States Code, Section 1029(c)**

(c) Penalties.—

(1) Generally.—The punishment for an offense under subsection (a) of this section is—
(A)in the case of an offense that does not occur after a conviction for another offense under this section—

(i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

(ii) if the offense is under paragraph (4), (5), (8), or (9) of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

(B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

(C) in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

(2) Forfeiture procedure.—

The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be

governed by section 413 of the Controlled Substances Act, except for subsection (d) of that section.

8. **Title 18, U.S. Code, Section 3559(g)(l)** provides, in relevant part:

> if a defendant who is convicted of a felony offense (other than offense of which an element is the false registration of a domain name) knowingly falsely registered a domain name and knowingly used that domain name in the course of that offense, the maximum imprisonment otherwise provided by law for that offense shall be doubled or increased by 7 years, whichever is less.

9. **Title 18, United States Code, Sections 1028A(a)(1) and 1028A(c)(4)** provide, in relevant part:

> Section 1028A(a)(1):
>
> Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.
>
> Section 1028A(c)(4):
>
> (c) DEFINITION.—For purposes of this section, the term "felony violation enumerated in subsection (c)" means any offense that is a felony violation of—
>
> (4) any provision contained in this chapter (relating to fraud and false statements), other than this section or section 1028(a)(7) . . . .

10. **Title 18, U.S. Code, Section 2** provides:

> (a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.
>
> (b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.

EXHIBIT 4

CARTÃO DE CIDADÃO
CITIZEN CARD

PORTUGAL
REPÚBLICA PORTUGUESA | PORTUGUESE REPUBLIC

APELIDO(S) / SURNAME
SANTOS COELHO

NOME(S) / GIVEN NAME
DIOGO

SEXO / SEX	ALTURA / HEIGHT	NACIONALIDADE / NATIONALITY	DATA DE NASCIMENTO / DATE OF BIRTH
M	1,76	PRT	23 02 2000

Nº DOCUMENTO / DOCUMENT No.	DATA DE VALIDADE / EXPIRY DATE
Nº ID CIVIL / CIVIL ID No.	
15202867 6 ZY0	03 11 2022

ASSINATURA DO TITULAR / HOLDER'S SIGNATURE

Diogo Coelho

PORTUGAL
CARTÃO DE CIDADÃO
CITIZEN CARD

FILIAÇÃO / PARENTS
JOSÉ CARLOS DA SILVA COELHO * MARIA DE LURDES DE JESUS SANTOS COELHO

006.005.23

Nº IDENTIFICAÇÃO FISCAL / TAX No.	Nº SEGURANÇA SOCIAL / SOCIAL SECURITY No.	Nº UTENTE DE SAÚDE / HEALTH No.
244575053	11924653274	278483644

I<PRT152028676<ZY06<<<<<<<<<<<
0002233M2211031PRT<<<<<<<<<<<2
SANTOS<COELHO<<DIOGO<<<<<<<<<<