DAVID L. ANDERSON (CABN 149604)
United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

MICHELLE J. KANE (CABN 210579)
KATHERINE L. WAWRZYNIAK (CABN 252751)
Assistant United States Attorneys

1301 Clay Street, Suite 340S
Oakland, California 94612
Telephone: (510) 637-3680
FAX: (510) 637-3724
michelle.kane3@usdoj.gov
Katherine.Wawrzyniak@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. YEVGENIY ALEXANDROVICH NIKULIN, Defendant.	No. CR 16-00440 WHA **UNITED STATES' TRIAL BRIEF** Trial: March 9, 2020 Time: 1:30 p.m. Courtroom No. 12

TABLE OF CONTENTS

I. SUMMARY OF FACTS TO BE PRESENTED AT TRIAL 1

A. Overview 1

B. The Attack on LinkedIn and its Employees 1

C. The Continuing Investigation and Development of Chinabig01@gmail.com 2

D. Subscriber Records Identify Nikulin 3

E. Nikulin Controls Both Chinabig01@gmail.com and R00talka@gmail.com 3

F. Sale of Formspring Credentials 4

G. Further Evidence from Ieremenko's Computer 5

II. OFFENSES CHARGED 6

III. ANTICIPATED EVIDENCE 7

A. Evidence Obtained from Domestic Internet Service Providers 7

B. Subscriber Records from Russian National Cable Networks Obtained via MLAT 7

C. Defendant's Statements. 8

D. Electronic Evidence Obtained by MLAT 8

1. Defendant's Correspondence 9

2. Photos and Videos 10

E. Translated Documents and Transcripts 11

F. Victim Intrusion Logs 12

TABLE OF AUTHORITIES

Cases

Anderson v. United States, 417 U.S. 211 (1974) 9

United States v. Al-Imam, No. 17-cr-00213 (CRC), 2019 WL 2358365 (D.D.C. June 4, 2019) 8

United States v. Bonallo, 858 F.2d 1427 (9th Cir. 1998) 11

United States v. Burt, 495 F.3d 733 (7th Cir. 2007) 9

United States v. Dupre, 462 F.3d 131 (2d Cir. 2006) 10

United States v. Estrada-Eliverio, 583 F.3d 669 (9th Cir. 2009) 10, 11

United States v. Franco, 136 F.3d 622 (9th Cir. 1998) 12

United States v. Hamilton, 413 F.3d 1138 (10th Cir. 2005) 10, 12

United States v. Hock Chee Koo, 770 F.Supp.2d 1115 (D. Or. 2011) 11

United States v. Jaramillo Suarez, 950 F.2d 1378 (9th Cir. 1991) 9

United States v. Khorozian, 333 F.3d 498 (3d Cir. 2003) 12

United States v. Korchevsky, et al., CR 15-6076 (E.D.N.Y.) 5

United States v. Matlock, 415 U.S. 164 (1974) 8

United States v. Osorio, No. 88-5523, 1988 WL 83427 (4th Cir. July 26, 1988) 8

United States v. Radchenko, et al., CR 19-30 MCA (D. N.J.) 5

United States v. Safavian, 435 F.Supp.2d 36 (D.D.C. 2006) 10

United States v. Shaw, 2018 WL 9649495 (C.D. Cal. 2018) 11

United States v. Siddiqui, 235 F.3d 1318 (11th Cir. 2000) 10

United States v. Strickland, 935 F.2d 822 (7th Cir. 1991) 8

United States v. Tuchynov, et al., CR 15-390 MCA (D. N.J.) 5

United States v. Welton, No. CR 09-00153-MMM, 2009 WL 10680850 (C.D. Cal. July 17, 2009) 12

Statutes

18 U.S.C. § 371 6

18 U.S.C. § 1028A(a)(1) 6

18 U.S.C. § 1029(a)(2) 6

18 U.S.C. § 1030(a)(2)(C) 6

18 U.S.C. § 1030(a)(5)(A) 6

18 U.S.C. § 3505 ..... 7, 8

Rules

Fed. R. Evid. 401 11

Fed. R. Evid. 801(c) 9

Fed. R. Evid. 801(d)(2)(A) 8, 9, 10

Fed. R. Evid. 803(1) 11

Fed. R. of Evid. 803(6) 7-8

Fed. R. of Evid. 901 10

Fed. R. of Evid. 902(11) 7

Fed. R. of Evid. 902(13) 7

Other Authorities

Treaty With Russia On Mutual Legal Assistance In Criminal Matters, Treaty Doc. 106-22, 1999 U.S.T. LEXIS 163 8

Treaty With Ukraine On Mutual Legal Assistance In Criminal Matters, Treaty Doc. 106-16, 1998 U.S.T. LEXIS 203 8

The United States of America by and through undersigned counsel, respectfully submits this trial brief for purposes of summarizing the legal and factual issues it believes will be relevant to the upcoming trial, set to begin on March 9, 2020. At the pretrial conference on February 19, 2020, the Court also requested copies of the "top ten" trial exhibits. Those exhibits are being filed as exhibits to this brief, including two videos that were previously discussed with the Court.

I. SUMMARY OF FACTS TO BE PRESENTED AT TRIAL

A. Overview

During 2012 and 2013, defendant Yevgeniy Nikulin engaged in a sustained campaign to steal user account credentials from major U.S. companies. Defendant repeatedly targeted employees of the victim corporations that, based on their positions, he knew would have high level access to corporate data. Once he compromised those employees' corporate account credentials, he used their access to obtain millions of consumer user names and passwords, in addition to other information. Those credentials were extremely valuable on the underground market for their use in spamming and other illicit purposes.

B. The Attack on LinkedIn and its Employees

In March 2012, defendant Yevgeniy Nikulin, operating from Russia, gained access to the personal computer of LinkedIn engineer Nicholas Berry. LinkedIn is a networking site that includes technical and security professionals from major Silicon Valley companies as members. Through his position, Berry had access to core LinkedIn data. Berry owned an Apple iMac computer, which he sometimes used to work from home. He also ran a "virtual machine" on the iMac that acted as a personal web server. Defendant compromised the virtual machine and, through a security flaw, was able to gain access to the iMac itself. In doing so, he installed software on the computer. Because Berry used the iMac to access LinkedIn corporate computers through a Virtual Private Network ("VPN")[1], Nikulin was able to gain access to LinkedIn's servers through Berry's VPN credentials. Once he had access to LinkedIn's servers, Nikulin could obtain a copy of LinkedIn's user credential database. Although the

///

[1] A VPN is often used by businesses so employees can connect to their office network from another location.

passwords in that database were encrypted, the copy that Nikulin gained access to was not yet "salted," which was a stronger form of encryption that LinkedIn was in the process of instituting.

LinkedIn learned of the breach in June 2012 when a portion of the stolen data was posted on a Russian hacker forum with a request for help with decryption. Upon embarking on an internal investigation, LinkedIn security personnel observed suspicious logins from Berry's VPN account from IP addresses that resolved to Russia. After confirming that Berry had not traveled to Russia and was not responsible for those logins, LinkedIn investigated information captured by its VPN and other logs. LinkedIn identified several Russian IP addresses that accessed its computers, indicating that someone in Russia was responsible for the access. Exhibit A (Summary of LinkedIn VPN Logs for User NBerry). LinkedIn also identified other data captured by its logs, including the "user agent string" and "cookie," two pieces of information that help identify a particular computer. [2] This data indicated that the same computer was likely responsible for multiple accesses across different IP addresses. Furthermore, LinkedIn found evidence that the same computer had also accessed multiple LinkedIn consumer accounts. Finally, LinkedIn identified one account, with the username chinabig01@gmail.com that had been accessed from one of the same IP addresses used in the compromise of Nick Berry's VPN credentials. Exhibit B (LinkedIn, Dropbox, and Formspring Emails from chinabig01@gmail.com Account).

The FBI reviewed LinkedIn data and Berry's computer and came to the same conclusion. Due to the access to customer LinkedIn accounts, the FBI contacted the employers of those customers regarding possible attacks on their computer systems. The FBI also began following the leads generated from the LinkedIn investigation, including the chinabig01@gmail.com address.

C. The Continuing Investigation and Development of Chinabig01@gmail.com

Following the attack on LinkedIn, Dropbox found numerous unauthorized logins from Eastern European IP addresses on its own system between May and July 2012. Dropbox disclosed those IP

[2] A user agent string is information regarding a user's web browser and computer that is passed to a website in order to display content correctly. The general format for user agent strings is "Mozilla/[version] ([system and browser information]) [platform] ([platform details]) [extensions]." A cookie in this context is a small piece of unique data sent from a website and stored in a user's web browser while the user is browsing a website. When the user browses to the same website in the future, the data stored in the cookie is retrieved by the website to notify it of the user's previous activity.

addresses to the FBI. The FBI also obtained records regarding a Dropbox account that had been registered just before the attack on Dropbox's system with the username chinabig01@gmail.com. IP logs from that account showed that it was accessed from the same IP addresses that accessed Dropbox accounts without authorization.

The FBI thus began focusing on the person controlling chinabig01@gmail.com as the person responsible for the LinkedIn and Dropbox intrusions. A search warrant for that email account revealed an email message indicating that Dropbox employee Tom Wiegand had "invited" the owner of the chinabig01@gmail.com Dropbox account to a Dropbox shared account, when he had not done so. Wiegand's account had been compromised, and the invitation showed that the person controlling chinabig01@gmail.com was responsible. Other evidence from the chinabig01@gmail.com account linking the owner to the attacks included a search for information related to an "SSH key"[3] in February 2012, shortly before the compromise of Nick Berry's computer, which obtained the SSH key used to authenticate his VPN connection.

D. Subscriber Records Identify Nikulin

Subscriber records obtained through Russian authorities showed that Nikulin, at an address on Kantemirovskaya Street in Moscow, was the registered subscriber of one of the IP addresses used to access LinkedIn computers without authorization. Exhibit C (National Cable Networks Subscriber Information). That IP address also accessed multiple LinkedIn member accounts between February and April 2012, and was one of the IP addresses linked by cookies to other unauthorized access at LinkedIn.

E. Nikulin Controls Both Chinabig01@gmail.com and R00talka@gmail.com

The FBI identified an account with a gaming website, Kongregate that had been accessed by an IP addresses used in the LinkedIn attack, including one that was also used to access the chinabig01@gmail.com Dropbox account. The Kongregate account and the chinabig01@gmail.com Dropbox account both used the name "Jammis" in their subscriber information. The Kongregate account showed a user name of "Zopaqwe1" and was registered under r00talka@mail.ru, which is hosted by a Russian email provider generally unavailable to U.S. authorities. An account with the DNS provider

[3] SSH refers to the "secure shell" protocol that many businesses use to secure the connection between an individual computer or "client" and a server.

Afraid.org using the email address chinabig01@gmail.com also had the password Zopaqwe1. These links all showed that the same person was using the Kongregate, Dropbox, Gmail, and Afraid. org accounts.

The contents of the email account r00talka@gmail.com (similar to the r00talka@mail.ru account used with Kongregate) indicated that it was controlled by the same person controlling chinabig01@gmail.com. For example, multiple messages addressed to "china" or "china china" were found in both accounts and registration confirmations from Russian companies noted the same password, "qwe123!" for accounts registered under both email addresses. Moreover, the contents of the r00talka@gmail.com account pointed directly to Nikulin. These included multiple messages generated through the VK social media platform to the r00talka@gmail.com account, including links to messages from Nikulin's brother and girlfriend. Exhibit D (Translation of VK Email from r00talka@gmail.com Account). The messages from VK often included a photo of Nikulin and a photo of the person sending the message. The search history for the r00talka@gmail.com account showed Nikulin searching for terms including "LinkedIn hack" and "Wordpress vulnerabilities." Exhibit E (Translation of r00talka@gmail.com search history). These links established that Nikulin controlled both the r00talka@gmail.com and chinabig01@gmail.com accounts, and was responsible for the LinkedIn, Dropbox, and Formspring intrusions.

F. Sale of Formspring Credentials

Between June 13, 2012, and June 29, 2012, Nikulin stole approximately 30 million Formspring user credentials after compromising the account of a Formspring employee, John Sanders (identified in the Indictment as J.S.). The Formspring logs show that defendant used Sanders' credentials to login to Formspring's servers and execute the attack, including the installation of malicious software. In July 2012, Formspring discovered that a portion of its encrypted password database had been posted online. The IP address used in the Formspring attack was also used to access multiple LinkedIn member accounts.

Nikulin then conspired with several individuals to sell the stolen Formspring credentials. In July 2012, Alexsey Belan, encouraged Nikita Kislitsin to contact Nikulin about the Formspring database. After Kislitsin confirmed that he had contacted Nikulin, Kislitsin and Belan discussed how a brute-force

password cracker, and not Nikulin himself, had posted the encrypted Formspring passwords online. Kislitsin then negotiated the sale of the database in September 2012 to another individual, who paid through Western Union via another individual, Oleg Tolstikh. Kislitsin sent a sample of the data, which Formspring confirms was their user information. Exhibit F (Excerpt of Translation of Email Messages Between fyofyofyo@hotmail.com and "ibo ibo"). The Western Union records corroborate that the sale was consummated.

G. Further Evidence from Ieremenko's Computer

In November 2012, the U.S. Secret Service obtained the image of a hard drive belonging to a target in another criminal investigation, Oleksandr Ieremenko. Ieremenko is an Ukranian national who was charged in the District of New Jersey in connection with a separate hacking scheme, wherein a group of Ukranian and Russian hackers worked together to steal news releases from Business Wire, Marketwired, and PR Newswire between February 2010 and August 2015. The hackers then passed the stolen news releases to traders who traded based on the stolen content. *See United States v. Tuchynov, et* al, CR 15-390 MCA (D. N.J.); *see also United States v. Korchevsky, et al.*, CR 15-6076 (E.D.N.Y.).[4] The contents of Ieremenko's hard drive as a whole show that Ieremenko and Nikulin worked together on (1) the stolen news releases, (2) stolen LinkedIn information, and (3) other uncharged hacking activity. In general, the government views Ieremenko and Nikulin as co-conspirators. In 2012 specifically, they were both part of a small cohort of Ukranian and Russian hackers—a criminal clique—whose members consulted with one another and sometimes shared resources. While the government will not attempt to adduce all of this background information at trial, it is important context for two types of evidence recovered from the Ieremenko drive that the government will seek to introduce: Skype chats and certain photos and videos.

The Skype chats are from various dates between June and November 2012. In them, Ieremenko uses the Skype name vaiobro and the alias Sergey Shalyapin. Nikulin uses the Skype name dex.007 and

[4] Ieremenko was also later indicted again in the District of New Jersey for a similar scheme in which he and another individual hacked into the SEC's Electronic Data Gathering, Analysis and Retrieval (EDGAR) system and stole thousands of files, including annual and quarterly earnings reports containing confidential, non-public, financial information. The defendants and others then profited by selling access to the confidential information in these reports and trading on this stolen information prior to its distribution to the investing public. *United States v. Radchenko, et al.*, CR 19-30 MCA (D. N.J.)

the alias Yevgeniy Lomovich. The contents of those conversations demonstrate that Nikulin is dex.007. On November 10, 2012, dex.007 sent a link to Ieremenko that contained the password to chinabig01@gmail.com's Afraid.org account, "Zopaqwe1" and a unique cookie that was part of the Afraid.org subscriber information. Records obtained independently from Afraid.org contain that cookie, and show that the Zopaqwe1 Afraid.org account was searching Afraid.org's systems for vulnerabilities on November 10, 2012. Dex.007 also sent Ieremenko, in October 2012, nonpublic LinkedIn user data, including encrypted and unencrypted passwords. Exhibit G (Translation of Excerpt of Skype Chats).

Ieremenko's hard drive also had a folder on it titled "Moscow 2012." That folder's contents included eight short videos. The metadata and the content of the videos show they were made over the course of two days, March 18 and 19, 2012, in Moscow, Russia, during a meeting of the aforementioned criminal clique. The government seeks to introduce two of the eight videos at trial. In the first, Ieremenko is narrating a drive that he describes as the approach to a "summit of bad motherfuckers" at a Moscow hotel. At the end of the video, Ieremenko's friend, who is driving, calls the driver of a black vehicle that pulls in front of them at the hotel an "angry hacker." Ieremenko's hard drive also contained a photograph showing Nikulin at the wheel of the same black vehicle. Exhibit H (Photo of defendant from O. Ieremenko's computer). In the second video, Ieremenko pans the camera around a conference room. Nikulin is seen, as are coconspirators Nikita Kislitsin and Oleg Tolstikh and others. During the recording, the group is discussing plans for an Internet café business. Exhibit I (CD: Video Clips from Computer of Oleksander Ieremenko).

II. OFFENSES CHARGED

The Indictment charges the defendant with three counts of computer intrusion, in violation of 18 U.S.C. § 1030(a)(2)(C), for the attacks on LinkedIn, Dropbox, and Formspring; two counts of intentional transmission of information, code, or command causing damage to a protected computer, in violation of 18 U.S.C. § 1030(a)(5)(A), for the attacks on LinkedIn and Formspring; two counts of aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1), for the use of LinkedIn and Formspring employee access credentials in connections with the attacks on those companies; one count of trafficking in unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(2), for the trafficking of stolen Formspring credentials; and one count of conspiracy, in violation of 18 U.S.C. § 371, alleging

that the defendant conspired to traffic the stolen Formspring credentials.

III. ANTICIPATED EVIDENCE

The United States has filed motions in limine addressing specific evidentiary questions that are well-suited to pretrial evaluations. This brief addresses some of the other evidence that the government intends to introduce and issues raised at the pretrial hearing.

A. Evidence Obtained from Domestic Internet Service Providers

The government intends to offer records, including content and subscriber information, obtained from Google, Dropbox, Microsoft Hotmail, and others. In advance of trial, the government has provided the defense with the relevant certifications under Federal Rules of Evidence 902(11) and/or 902(13) and notified the defense of the government's intent to introduce those records pursuant to the certifications. Defendant has not objected to the government's notice. These records, which were obtained from legally valid search warrants or other process served on the providers, are admissible without further authentication.

Pursuant to Federal Rule of Evidence 902(11) and 902(13), certified domestic records of regularly conducted activities or electronic processes are self-certifying and admissible without the testimony of custodial witnesses under Federal Rule of Evidence 803(6)(A)-(C), if the custodian furnishes a written declaration that the records: (A) were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters; (B) were kept in the course of a regularly conducted activity; and (C) were made as a regular practice. Here, the records satisfy these requirements. Accordingly, while the government is prepared to provide additional bases for authentication of these materials at trial if necessary, including calling a custodian from the provider, the government believes the 902(11) or 902(13) certification satisfies the issue of authenticity, such that a custodial witness would cause unnecessary delay.

B. Subscriber Records from Russian National Cable Networks Obtained via MLAT

The United States requested and obtained subscriber records from Russia for some of the IP addresses used in the computer intrusions. The government has provided defendant a sworn declaration that the subscriber records were business records made and kept in the ordinary course of business.

Much like Federal Rule of Evidence 902(11) certifications for domestic business records, 18

U.S.C. § 3505 provides that foreign business records are admissible in criminal proceedings if they are "record[s] kept in the course of regularly conducted business activity" and records are made "at or near the time of the occurrence of the matters set forth, by (or from information transmitted by) a person with knowledge of those matters." 18 USCS § 3505(a)(1)(A); *see United States v. Osorio*, No. 88-5523, 1988 WL 83427, at *1 (4th Cir. July 26, 1988). Section 3505 requires that foreign records can be authenticated through a signed certification. See 18 U.S.C. § 3505(a). The declaration provided pursuant to the Russian response to the United States' request under the Treaty With Russia On Mutual Legal Assistance In Criminal Matters, Treaty Doc. 106-22, 1999 U.S.T. LEXIS 163, satisfies all of the requirements set forth. Accordingly, the subscriber records are admissible without any need for calling a custodian to provide live testimony to authenticate the documents. *See United States v. Strickland*, 935 F.2d 822, 831 (7th Cir. 1991) (admitting records and noting Congressional intent to "streamline" admission of foreign business records by substituting § 3505 certification for "the cumbersome and expensive procedures' of live-witness testimony under Rule 803(6)"); *United States v. Al-Imam*, No. 17-cr-00213 (CRC), 2019 WL 2358365, at *4 (D.D.C. June 4, 2019).

C. Defendant's Statements.

The United States will introduce defendant's own statements, including statements made in recorded telephone calls, email messages, and chat transcripts. For example, in one recorded telephone call, defendant talks about "hacking the prison" with his girlfriend. Exhibit J (Translation/excerpt of Defendant's Call 159.924 (Nov. 19, 2018)). Fed. R. Evid. 801(d)(2)(A) provides that a party's own statement is directly admissible against the party. *United States v. Matlock*, 415 U.S. 164, 172 (1974) (A party's "own out-of-court admissions . . . surmount all objections based on the hearsay rule . . . and [are] admissible for whatever inferences the trial judge [can] reasonably draw."). As noted below, the statements of others contained in the e-mail and chat conversations in reply to the defendant may be admitted for the non-hearsay purpose to supply context.

D. Electronic Evidence Obtained by MLAT

As described above, the government will offer records obtained from Ieremenko's laptop. The laptop was seized during a search executed by Ukrainian officials pursuant to the Treaty With Ukraine On Mutual Legal Assistance In Criminal Matters, Treaty Doc. 106-16, 1998 U.S.T. LEXIS 203. As part

of discovery, the government has produced records of the search and seizure provided by Ukranian officials in response to the Treaty request and the FBI's forensic report for the computer, as well as copies of the Skype chats, videos, and photos that it intends to introduce. A copy of the forensic image was made available for defense review.

Special Agent Richard LaTulip of the United States Secret Service will testify that he traveled to Ukraine to forensically image Ieremenko's computer, and will authenticate the evidence the United States' intends to introduce as obtained from that image. Other records obtained during the search, including a copy of Ieremenko's passport, will be authenticated by the form signed by the executing Ukrainian investigative officer pursuant to the relevant Treaty provision, Article 15, which provides for admissibility of items seized during the execution of searches performed pursuant to the Treaty.

1. Defendant's Correspondence

As with other evidence, the chat transcripts obtained via MLAT from the seized computer, and the correspondence contained in the email content obtained via search warrant are admissible where the requirements of the Federal Rules of Evidence are satisfied. The defendant's email and chat communications are admissible non-hearsay because the information is not offered to prove the truth of the matter asserted or does not meet the definition of hearsay under Fed. R. Evid. 801(c).

Statements introduced for a non-hearsay purpose do not violate the hearsay rule. See, e.g., *Anderson v. United States*, 417 U.S. 211, 219 (1974) ("Out of court statements constitute hearsay only when offered in evidence to prove the truth of the matter asserted."); *United States v. Jaramillo Suarez*, 950 F.2d 1378, 1383 (9th Cir. 1991) (noting that where the probative value of a document "was independent of the truth of its contents, the rule against hearsay was not implicated"; pay-owe sheets introduced for the non-hearsay purpose to show the character of the place not for the truth of the statements). As noted below, the statements of the defendant on emails and chat communications are directly admissible against the defendant under Fed. R. Evid. 801(d)(2)(A). The statements of others used in the e-mails and chat communications are admitted not for the truth of the matter but as non-hearsay to supply context. *See, e.g., United States v. Burt*, 495 F.3d 733, 738-39 (7th Cir.) (in prosecution for sexual exploitation of a minor, distributing child pornography, and possession of child pornography, in Yahoo! chat communication involving the defendant and a third party found on the

defendant's computer, the portion from the third party was admissible as non-hearsay and provided context to the conversation); *United States v. Dupre*, 462 F.3d 131, 136-37 (2d Cir. 2006) (in wire fraud prosecution, emails from investors demanding information about defendant's fraudulent scheme were not hearsay when offered not for truth of the assertion that the scheme was fraudulent, but to provide context for the defendant's message sent in response and to rebut defendant's argument that she did not know scheme was fraudulent; no Confrontation Clause issues arose since the statements were offered for a non-hearsay purpose); *United States v. Safavian*, 435 F.Supp.2d 36, 44 (D.D.C. 2006) (admitting some emails which "provide context for the defendant's statements and are not introduced for their truth").

The United States will also introduce automated account messages sent to defendant from victims such as LinkedIn and Dropbox for the non-hearsay purpose of demonstrating that the defendant opened accounts with those businesses in association with his intrusions as part of his method of operating. These automated messages are not hearsay. Courts have consistently held that machine-generated information is not hearsay as no "person" is making a statement. *See, e.g., United States v. Hamilton*, 413 F.3d 1138, 1142 43 (10th Cir. 2005) (computer generated "header" information (including the screen name, subject of the posting, the date the images were posted, and the individual's IP address) was not hearsay; no "person" acting as a declarant). Moreover, these communications show the relationship of the defendant with the victims and the fact of him receiving communications from those companies on relevant dates, and are not offered for the truth of the matters asserted in those communications. *See, e.g., United States v. Siddiqui*, 235 F.3d 1318, 1322 (11th Cir. 2000) ("Those [e-mails] sent by Siddiqui constitute admissions of a party pursuant to Fed. R. Evid. 801(d)(2)(A), and those between Siddiqui and Yamada unrelated to the NSF investigation are non hearsay admitted to show Siddiqui's and Yamada's relationship and custom of communicating by e mail.").

2. Photos and Videos

After Special Agent LaTulip has authenticated the image of Ieremenko's hard drive, Special Agent Miller will describe how he reviewed the image. Special Agent Miller is able to recognize at least one person in each video and photograph that the government will seek to admit. FBI Special Agent Emily Odom is able to identify Kislitsin in the second video because she personally interviewed Kislitsin in 2014. The combined testimony of the agents regarding the photos and videos is sufficient

authentication under Fed. R. Evid. 901. *See United States v. Estrada-Eliverio*, 583.F.3d 669, 672 (9th Cir. 2009) ("A party need only make a prima facie showing of authenticity so that a reasonable juror could find in favor of authenticity or identification.") (internal citations omitted). In other words, the exhibits are what they purport to be: videos and photos saved on Ieremenko's computer. *See United States v. Hock Chee Koo*, 770 F.Supp.2d 1115, 1122 (D. Or. 2011) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness. The mere possibility that the logs may have been altered goes only to the weight of the evidence not its admissibility.") *quoting United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1998).

As for the statements that are audible in the videos, the statements in the first video are admissible as present sense impressions. The person making the video says at the outset, "In short, we are reporting on the spot. Now, here at this Vega Izmailovo Hotel, there will be a fucking summit of bad motherfuckers." Later, the driver says in reference to the movement of the black sedan, "Look, what an angry person. Angry hacker." The present sense impression exception to the rule against hearsay applies to statements "describing or explaining an event or condition, made while or immediately after the declarant perceived it." Fed. R. Evid. 803(1). One of the key components of this exception is contemporaneousness, which is present. The statements in the video are being made without much reflection. Additionally, many of the statements are readily verified by the footage itself. As the speaker talks about the summit, a large hotel comes into view. Later, the camera pans to an older woman standing outside and the speaker says, "There's a granny over there. Picking her fucking nose." Indeed, the woman visibly removes something from her nose. The statements in the first videos should be admitted pursuant to Rule 803(1). *See, e.g. United States v. Shaw*, 2018 WL 9649495 (C.D. Cal. 2018) (admitting statements in 911 call as present sense impressions).

As for the audio in the second video, that conversation is not hearsay because the United States is not offering it to prove the truth of the matter asserted. The probative value of the video is that it puts three of the alleged co-conspirators in the same room approximately two months before the Formspring hack. Admission of Exhibit 74 is proper under Fed. R. Evid. 401.

E. Translated Documents and Transcripts

Among other evidence, the government intends to offer (1) foreign language correspondence that

has been translated into English and (2) audio and video recordings containing Russian that have been transcribed and translated into English. The government intends to offer as substantive evidence all English translations of foreign language documents, recordings, or videos (or any part thereof). This is necessary to allow the jury to properly evaluate foreign-language evidence.

In advance of trial, the government has provided the translations to the defendant. To date, the defense has not disputed the accuracy of any of these transcriptions or proposed revisions or alternative translations. The English transcripts of foreign language correspondence and conversations are admissible as substantive evidence. *See, e.g., United States v. Franco*, 136 F.3d 622, 626 (9th Cir. 1998) (recognizing procedure of admitting both foreign language evidence and translations).

F. Victim Intrusion Logs

Some of the evidence at trial will include machine-generated information contained in logs, including those obtained from computers operated by LinkedIn, Dropbox, Formspring, and Automattic[5]. For example, the information in the logs might the IP address of the outside computer connecting to the company, the date and time, account name, user agent string, and cookie. Courts have consistently held that machine-generated information is not hearsay as no "person" is making a statement. *See, e.g., Hamilton*, 413 F.3d at 1142 43 (computer generated "header" information not hearsay); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir.) (information automatically generated by fax machine is not hearsay since "nothing 'said' by a machine . . . is hearsay"); *United States v. Welton*, No. CR 09-00153-MMM, 2009 WL 10680850, at *3 (C.D. Cal. July 17, 2009) ("The header and footer information in question is generated by a computer independent of human observations or reporting, and thus does not

///

[5] Pending the Court's decision regarding the Automattic evidence.

contain assertions that amount to hearsay.") Because the original records are voluminous, the United States will introduce these records in summary format that can be read and understood by the jury.

DATED: March 3, 2020

Respectfully submitted,

DAVID L. ANDERSON
United States Attorney

/s/
MICHELLE J. KANE
KATHERINE L. WAWRZYNIAK
Assistant United States Attorneys