# EXHIBIT A

**FEDERAL BUREAU OF INVESTIGATION**

Date of entry 04/23/2014

Nikita Igorevich KISLITSIN, date of birth (DOB) [redacted] was interviewed at the United States (U.S.) Embassy, Moscow, Russia. Present in the interview were Supervisory Special Agent (SSA) Emily A. Odom, Special Agent (SA) Anton Mlaker, and Federal Bureau of Investigation (FBI) Russian Linguist Marina Parsegova.

Prior to beginning the interview, at approximately 10:05 A.M., Linguist Parsegova explained her role as a Russian-English translator. KISLITSIN stated he was 95% confident in his English language abilities and agreed to conduct the interview in English. He further stated he may not be comfortable using English in some instances and in those instances he would utilize Linguist Parsegova's assistance. Interviewing agents requested that KISLITSIN be truthful and explained to KISLITSIN that formal charges were filed against him in the U.S. and he was entitled to specific rights.

At approximately 10:08 A.M., KISLITSIN was provided the FD-395 Advice of Rights in both the Russian and English languages. Agents explained to KISLITSIN he had the right to remain silent; however, should he choose to speak with agents, he could discontinue the interview at any time or refuse to answer any questions. KISLTSIN was also informed he had a right to have an attorney represent him, as well as have an attorney present during the interview. KISLITSIN stated, "I'm quite open for collaboration" and his "goal was to mitigate problems." He further stated he was seeking to "provide a way to have a win/win situation" as a result of the discussion with the agents. KISLITSIN stated he understood his rights as explained and at approximately 10:10 AM, KISLITSIN read and signed both the English and Russian translations of the FD-395 Advice of Rights form.

After KISLITSIN signed the FD-395, the agents asked about his familiarity with Aleksey Belan. KISLITSIN provided the following information:

Andrey Komarov allowed KISLITSIN to view papers regarding Belan's arrest and the charges filed against Belan. Komarov works for the Russian Ministry of Foreign Affairs and is a common acquaintance of KISLITSIN and Belan. Komarov was not involved in Belan's criminal activity, but KISLITSIN believes Komarov obtained the papers through Komarov's employment at the

Investigation on 04/02/2014 at Moscow, Russia (In Person)

File # 288A-LV-43343 Date drafted 04/07/2014

by Anton E Mlaker, Emily A. Odom

Russian Embassy. Komarov currently conducts business in the U.S. and is very "open". KISLITSIN further stated he has not spoken to Belan since Belan's arrest.

At approximately 10:15 A.M., KISLITSIN was provided a copy of the indictment outlining the charges against him. KISLITSIN was given several minutes to read the document and was not interrupted until he indicated that he had finished. He was then informed the Northern District of California also filed charges against him.

It was explained to KISLITSIN the FBI's role was to investigate the criminal activity and provide the information to a prosecutor who would determine how to proceed. The agents further explained they could not provide any promises or guidance as to the resulting punishment, regardless of his level of cooperation.

KISLITSIN was asked if the "Nikita Kislitsin" named in the indictment was someone other than himself, to which he replied, "I don't think so." KISLITSIN stated it was his decision to speak with the FBI at the U.S. Embassy and he was familiar with the matter described in the indictment; however, KISLITSIN stated the indictment contained many things regarding his involvement that were incorrect. Agents stated that during the interview they would be making a record of his statements which would be provided to prosecuting attorneys. SA Mlaker further explained to KISLITSIN he must decide for himself whether to cooperate and reiterated he was not required to answer any questions.

KISLITSIN stated Belan is not the most dangerous criminal. KISLITSIN again reiterated his goal was to mitigate his situation so he could travel without fear of being arrested. He also stated he traveled "now", which the agents understood to mean KISLITSIN had traveled recently. KISLITSIN inquired as to whether the U.S. had issued an international notice for his arrest and what type of punishment he might face for the stated charges. SA Mlaker explained the likelihood and amount of time served in prison depended on his level of cooperation, as well as the determination of the prosecuting attorneys and respective courts. KISLITSIN stated serving any "jail time was not an option".

KISLITSIN then stated he could provide a lot of information, as he knew people in the "community", which agents understood to mean KISLITSIN could provide information on numerous individuals engaged in criminal activity. KISLITSIN also stated he did "not feel guilty about it" and the interviewing agents were welcome to ask any questions they wished. Interviewing agents understood this to mean KISLITSIN did not feel guilty regarding his activity concerning the charges filed against him.

Interviewing agents asked KISLITSIN to describe his relationship with Belan to which KISLITSIN provided the following information:

KISLITSIN has known Belan since approximately 2006/2007 while KISLITSIN was working as the editor for the Russian hacker magazine Xakep (pronounced "hacker"). At the time, an advertisement was placed in the magazine in an attempt to identify individuals who could write articles about Internet security topics. Some other editors read a response from Belan and Belan was selected to write for the magazine. Belan wrote interesting articles related to vulnerabilities in web engines, exploitations, SQL injections, and cross-site scripting.

KISLITSIN met Rais, whom KISLITSIN knows to be Mehmet Sozen, in the summer 2011. Rais has both Belgian and Turkish citizenship, resides in Brussels and owns a magazine. Rais asked KISLITSIN for help promoting his e-commerce company and also asked KISLITSIN if he was capable of obtaining databases of other e-commerce websites. Rais provided KISLITSIN the Uniform Resource Locators (URL) of the websites he wanted KISLITSIN to obtain. KISLITSIN agreed and contacted Belan. KISLITSIN stated, "Belan was the guy to do the job for me".

KISLITSIN maintained a business relationship with Rais and Belan until spring 2013. When asked why he ended the business relationships, KISLITSIN stated the following three reasons:

One reason KISLITSIN ended the relationships with Rais and Belan was because in January 2013 KISLITSIN began working for the company Group-IB on a botnet-monitoring project. The goal of the project was to identify botnet command and control servers housing compromised data, gain access to the server, extract the data, and return it to the victim companies. The botnet command-and-control servers were identified through sensor monitors placed within Russian Internet Service Providers (ISP). As a result, approximately 15 victim banks, believed to be located in Russia, were identified.

KISLITSIN explained he also ended the relationships with Rais and Belan because the activity was not something he could envision himself doing for an extended period of time. When KISLITSIN has children, he would like to tell his children he has a legitimate job and is applying himself in a positive, meaningful manner. KISLITSIN would like to set a good example for his future children. KISLITSIN stated that on one hand, he would not be able to fight criminal activity through his employment, and on the other, conduct criminal activity.

Lastly, KISLITSIN stopped the activity with Rais and Belan because, "From a religious perspective, it is wrong."

KISLITSIN then asked the interviewing agents if they knew of an individual named Pavel Volkov, whom KISLITSIN met in an English language class in New York. KISLITSIN described Volkov's behavior as "unnatural" and "strange", partly because Volkov was enrolled in the same English class as KISLITSIN, yet he was able to speak English at a much higher level. KISLITSIN further stated Volkov was "frequently present" and KISLITSIN felt as if Volkov was sent to follow him. KISLITSIN grew more suspicious when Volkov, who did not have technical abilities, invited him to the Defcon Conference in Las Vegas, Nevada. Also, shortly after KISLITSIN returned to Russia, Volkov ceased contact with KISLITSIN and would not return e-mail messages. He also deleted his Facebook account. After Volkov disappeared, KISLITSIN had a strong feeling that Volkov was sent to obtain information from him. KISLITSIN speculated Volkov might be a spy for the National Security Agency (NSA).

KISLITSIN further stated Volkov purported to be from the country of Georgia, but obtained his U.S. citizenship in the fall 2012. KISLITSIN last saw Volkov in Los Angeles and believed he worked as a producer. KISLITSIN felt comfortable around Volkov and described him as a "smart guy" and good musician. KISLITSIN believed Volkov's e-mail address to be similar to pavel.volkov75@gmail.com.

At approximately 11:10 A.M., KISLITSIN asked for a restroom break and the interview was stopped for approximately ten minutes. Upon returning from the break, KISLITSIN provided the following information:

The compromise of the Zappos network was Belan's idea, and was also conducted by Belan. After Belan obtained the Zappos database, he asked KISLITSIN for ideas on how to sell the data. KISLITSIN contacted Rais the same day and attempted to negotiate a price for the Zappos data, which contained approximately 25 million customer records. KISLITSIN and Rais could not agree on an amount; therefore, KISLITSIN never sold the database to Rais nor acquired it from Belan.

Belan obtained e-commerce databases with a goal to sell them for financial gain or use them for spamming purposes. Belan specifically targeted American citizens by offering weight loss products or services pertaining to "Internet promotion business". Belan used the Zappos database as part of a spamming campaign and made approximately $200,000 USD. Belan conducted the spamming campaign with a partner, referred to as "Johnny Green" (phonetic). KISLITSIN has no further information on "Johnny Green."

KISLITSIN provided a printed copy of a Russian forum posting which he explained was an advertisement purportedly authored by Johnny Green which requested "new and used dumps". The posting offered 50/50 revenue sharing for the provider of "dumps" of 100,000 records or more containing primarily

U.S. customer information. The posting also offered the ability to crack password hashes. The dumps were presumably used as part of e-mail spamming efforts.

Belan and Johnny Green continue to work together and conceal cash payments between buyers and sellers by transporting money in shoeboxes via train attendants. Belan is very wealthy and owns multiple flats in Russia. Because Belan has very low self-esteem, he constantly brags about his wealth in an effort to compensate. KISLITSIN met Belan in person on one occasion in February 2013 at a party hosted by Dmitriy Dokuchayev, who is a close friend of Belan's and a captain within the Russian Federal Security Service (FSB). KISLITSIN met Dokuchayev when KISLITSIN was 16 or 17 years old. Kislitsin provided a photograph of Belan, Belan's wife, and Dokuchayev which he recently obtained from an Internet posting.

According to Komarov, Dokuchayev secretly records his conversations with other individuals, both in person and over the phone. Komarov told KISLITSIN Dokuchayev was involved in other criminal activity and was actively building profiles on various individuals using "compromising information". KISLITSIN provided no further information on Dokuchayev's other criminal activity. Belan assisted Dokuchayev with "assignments", which KISLITSIN believed involved the targeting of specific e-mail accounts and other data. Dokuchayev was recruited by the FSB after being caught stealing dial-up accounts and was given the ultimatum to join the FSB or go to jail.

KISLITSIN stated Belan was not involved in the Formspring intrusion. After learning of Johnny Green and Belan's successful spamming operation, KISLITSIN became interested in conducting the same activity and knew Yevgeniy LNU already possessed the Formspring database. After agreeing on a price, KISLITSIN acquired the database from Yevgeniy and provided it to Rais for spamming purposes; however, KISLITSIN stated, "Formspring users don't want to buy anything." As a result, KISLITSIN did not make enough to money to pay as much as he promised Yevgeniy and Yevgeniy became unhappy with KISLITSIN.

To make the payment to Yevgeniy for the Formspring data, KISLITSIN provided the money to Rais, who provided the money to Oleg Tolstyky. Tolstyky is a common acquaintance of KISLITSIN and Yevgeniy and on one occasion KISLITSIN met Yevgeniy in person through Tolstyky. Tolstyky acts as a money transfer agent for Yevgeniy and provided the money from Rais to Yevgeniy for the Formspring database.

Tolstykh has schizophrenia and once attempted to form a new Russian political party comprised of hackers. Tolstykh was described as a "famous person on the Internet" who uses the moniker "NSD". He is known to be

involved in serious crimes including theft from approximately 12 or more U.S. banks, such as E*Trade, and Scottrade. Tolstykh engaged in a criminal act (NFI) which he called Operation Blitzkrieg. He recorded the act and posted it to Youtube. The video showed his real face and plate numbers from his vehicle.

KISLITSIN described Yevgeniy as "way more interesting than Belan" and the "Putin" of the hacking world. Yevgeniy's nickname is "Zhenya", which translates to "Eugene" in English. Yevgeniy currently lives in Moscow, is very wealthy, and owns multiple Maserati cars. Yevgeniy has low self esteem and flaunts his wealth as a way to compensate.

Yevgeniy compromised LinkedIn and sold the data for hundreds of thousands of dollars. KISLITSIN believes Yevgeniy has the databases for Google and Facebook; however, KISLITSIN is unsure if Yevgeniy actually conducted the compromises.

Yevgeniy has numerous databases containing user names and passwords. After using the LinkedIn information to identify specific employees, such as network administrators of specific companies, Yevgeniy used known passwords to login to the employees e-mail accounts. He then analyzed the e-mail communications to identify other accounts and passwords such as Virtual Private Network (VPN) credentials. These credentials allowed Yevgeniy to further exploit the company's network. If Yevgeniy was unable to access a specific employee's email account, he would identify and target friends of the employee. For example, Yevgeniy would identify the employee's friends, login to the friend's email account using known credentials, and then send an email containing a malicious link from the friend to the employee. Kislitsin stated the LinkedIn information is very powerful and used to not only exploit the employee directly, but also the employees social network.

Yevgeniy claimed to have current access into the DropBox network and to have acquired numerous password containers stored in user's DropBox accounts. These containers allow Yevgeniy to further exploit other accounts owned by the user. Yevgeniy told KISLITSIN he struggled to brute force the passwords to the Dropbox containers, but he eventually found an individual who wrote software to break the encryption algorithm. Yevgeniy has a "farm" of GPUs (graphics processing unit) used to brute force passwords.

KISLITSIN believes Yevgeniy creates persistent access into the networks he exploits to allow him to continue to access the network. KISLITSIN suspected that Yevgeniy may still have access into the DropBox network.

Yevgeniy uses Skype and Jabber to communicate online, and further, he implements OTR (off-the-record) encryption when using Jabber. KISLITSIN

described Yevgeniy's data buyers as "big guys", serious people who pay with cash and likely were not from Russia. KISLITSIN did not specifically know any of the buyers.

KISLITSIN further stated Belan was responsible for the compromises of Evernote, Groupon and Yelp, as well as, likely responsible for the compromise of Last.FM. Belan may also be responsible for the compromise of Zoosk as Belan likes targeting dating websites.

Rais attempted to contact KISLITSIN several times since they last worked together and a few months ago, they had a conversation wherein Rais stated he was detained in Serbia while driving from Belgium to Turkey. Rais was subsequently extradited to Belgium where he was charged with related crimes. KISLITSIN presumed Rais was released from jail since he was able to contact him. Rais asked KISLITSIN to continue their business relationship, to which KISLITSIN declined. KISLITSIN stated he met Rais in person on two occasions, once in Russia and once in Brussels.

KISLITSIN indicated he could likely determine and provide the last name and address of Yevgeniy; however, he would probably not be able to obtain information on Johnny Green.

KISLITSIN could also likely arrange a meeting to speak with Belan, but stated he would prefer not to do so as he was apprehensive about potential repercussions related to Belan's association with Dokuchayev. Dokuchayev previously indicated to KISLITSIN he was "very much" concerned about the situation surrounding Belan's arrest. KISLITSIN supposed that Dokuchayev was concerned Belan may divulge information about his involvement with Dokuchayev. Dokuchayev informed KISLITSIN that Belan obtained a Bulgarian passport and glued his own photograph inside the passport. This passport allowed Belan to travel from Greece into Russia. Dokuchayev's wife also works for the FSB.

KISLITSIN stated Group-IB was investigating the carding shop "FETEAM". FETEAM operated successfully, in part because they were able to evade efforts to shut them down by changing the domain name used to access their carding web site. Group-IB works with the registrars and hosting providers to "sinkhole" the Internet traffic to the domain names. KISLITSIN described the sinkhole action as putting a passive proxy server inline with the server hosting the target forum. This method allows Group-IB to monitor the Internet traffic associated with users of the carding forum as well as related botnet activity. KISLITSIN offered the data being collected by Group-IB to the FBI. Group-IB CEO Ilya Sachkov was aware and supportive of KISLITSIN's offering of the data to the FBI.