ATTACHMENT 1

TO

Technological Crime Advisory Board

September 2020

Draft Minutes to June 22, 2020 Meeting

OFFICE OF THE ATTORNEY GENERAL

Aaron D. Ford, *Attorney General*

100 North Carson Street
Carson City, NV 89701
Telephone - (775) 684-1100
Fax - (775) 684-1108
Web - http://ag.nv.gov

MEETING MINUTES

Name of Organization: **Technological Crimes Advisory Board**

Date and Time of Meeting: **June 22, 2020 at 2:00 p.m.**

Place of Meeting: Telephonic Conference Call
Number: 605-313-5111
Access code: 468822

Attorney General's Office
Mock Courtroom
100 N. Carson Street
Carson City Nevada

Attorney General's Office
Sawyer Building, Room 4500
555 E. Washington Avenue
Las Vegas, Nevada

Attendees:

Teleconference:

Members in Attendance:
Attorney General Aaron Ford
Theresa M. Haar
Renato "Sonny" Vinuya
Alan Cunningham
Jacob Cinco
E. Andrew Campbell
Steve Yeager
Nicole Cannizzaro

Members Absent:
David Haws
Bill Olson
Chris Lake
Chris Darcy

Guests in Attendance:
Laura Tucker

1. Call to Order and Roll Call.

Meeting called to order at 2:00 p.m., Theresa Haar called roll and confirmed there was a quorum present.

2. Public Comment.

None.

3. Approval of Minutes.

AG Ford asked for approval of the March 25, 2020 meeting minutes.

AG Ford moves to approve the minutes. Steve Yaeger motions for the approval of minutes Nichole Cannizzaro seconded the motion, and the motion passed unanimously.

4. Security in video conferencing.

Introduction of Bob Dehnhardt, EITS Chief Information Security Officer by Theresa Haar. Mr. Dehnhardt reviews with the Board the four (4) types of online meetings that are occurring through video conferencing. Internal collaboration – the one on one or a small team of up to 50 participants; Learning and training – interactive presentation tools that allows the presenter to share content and ask/answer questions and assist thru a remote control desktop; External meetings – enables people to connect into it with a simply quick and easy start up to join, like Zoom; and, Webinars – primarily a one way communication to a very large group like WebEx.

The security considerations across all of them are fairly common. Information is what is being secured and not platforms or server or a desktop or anything like that, you're trying to secure information and you secure that by securing the platform or desktop something like that. Information dictates what kind of security you're looking for. Considerations for external meetings would be access controls like limiting who is invited, pre-registration, and meeting passwords. How well you can control the users once they are in the meeting, are you able to mute the user who is being disruptive or is trying to speak out of turn, are you able to remove an uninvited user without restarting the whole meeting.

Another area of concern is encryption. Look for acronyms like TLS, transport layer security, which used to be SSL, secured socket layer. TLS replaced SSL because it was hacked and is no longer used. Most website have moved onto TLS.

You should be aware if the vendor system storage used to store information from meetings or if files are exchanged or if the presentation is made available for download. You should ask if that information will be encrypted on the vendor system, how long will they be stored, and if the meeting organizer asks for the information to be deleted are there backups that are maintained that those be deleted as well.

Some of these questions you will not be able to find out using a free service. You need to look at whether it's worthwhile depending on the information you are sharing and the type of meeting that you're putting on and the frequency. Is it worthwhile to get a paid service? Most of the services have a free service which may have caps on attendance, access, shorter time, etc. These services also have a paid subscription to many of the services that you cannot get on the free service which provide better features, longer times, larger audience, etc.

AG Ford asks if there are any comments or questions. Mr. Haws asks if there is a concern for the state using a product like Zoom externally. Mr. Dehnhardt states that his preference is to use a vendor who is contracted with the state because if there is a problem or an issue it gives the state more leverage to getting it fixed.

5. Technology and Covid-related scams.

Jacob Cinco is on the line from Homeland Security. He is on the COVID taskforce which is coordinated with the Attorney General's office. Also, on the line is Laura Tucker in the event that she would like to offer any additional comments.

Mr. Cinco relates some of the scams they are seeing from the law enforcement side. Criminals like to take advantage of the fear that people were feeling at the onset of everything at the beginning of the COVID pandemic. When people are afraid, they become more susceptible to social engineering scams, phishing scams, and non-delivery scams. Criminals would send out via text or emails mass messages posing as legitimate agencies ie IRS, Center for Disease Control or the World Health Organization. They would send a link or attachment that people would click on and that would open up the malware on their computer.

Specifically, for the COVID-19 criminals were looking for personal identifying information (PII). With that information they would be able to submit claims to the IRS or unemployment platforms to get money sent their way. They also used this information to open up bank accounts or to take over your bank account. The biggest guidance or suggestion that they can give the public is that the bank, the IRS, the CDC etc. would not send a text message with a link to provide them with your information.

Another social engineering tactic was over the phone. People calling seeking charitable donations in relation to COVID. Criminals saw this as an opportunity to prey on people who were empathetic to the issues revolving around COVID.

The third scheme involved non-delivery scams. Criminal actors would advertise in demand medical supplies, PPE to be used to prevent the virus. Criminals would demand up front payment/deposits and then obviously not sending those items to the victim.

In mid-March the CARES Act was developed. Criminals would attempt phishing scams to get individuals PII to access the IRS site to change the banking/routing information so that the stimulus check went to them instead. Criminals also would state that if you did not file an IRS income tax form over the last few years, they would file a false income tax return for you thus getting the stimulus check sent to them.

The CARES Act also opened up fraud with the small business association were criminals were acting as business owners. This is a much larger amount of loan fraud that was made. This allowed criminals the same opportunity for phishing scams. Spoof domains and websites were used that actually did not exist and the information was being given to the criminals via that platform.

The process for submitting claims through the COVID-19 taskforce here in Nevada, the main flow was through the national center for disaster fraud thru phone numbers and online submittals. It was vetted through the Nevada Attorney Generals Office and the US Attorney's office. Law enforcement agencies here in Southern Nevada were given particular areas to be investigated. Secret Service communicated with the Banks and helped with the unemployment fraud and pandemic unemployment system thru DETR. Specifically, here in Nevada money mules were used to move money thru Credit Unions. Credit Unions would call the Secret Service to report potential fraud where a person would go in and set up an account and a week later the account would start getting unemployment checks from Massachusetts, Texas or Arizona all with different pay names. After some digging, contact and interview with the account holder, it was found that they were operating under the guidance of a romance scam or some type of a business scam. People are very gullible with what they are being told and instructed to do either through on-line dating site or text or emails. Millions of dollars are being exchanged through the hands of these money mules. Secret Service is continuing to work with DETR and the banks to provide information to the secret service initially to identify the mules. Investigations will progress to individuals who accessed the DETR website platforms and submitting claims using the PII of Nevada citizens and following where that leads.

They are working with the FBI, the Dept. of Labor, and OIG, together they can at least get the money back to the states where they came from and work on the prosecution of the money mules when more is established.

AG Ford opens up for comments or questions.

Mr. Vinuya asks if there are pamphlets and/or flyers regarding the different scams that they can pass out. Mr. Cinco states that there are flyers and alerts, advisories that the Secret Service has and he will get together with Theresa Haar to have these available for anyone who would like them.

Ms. Tucker states that BCP has been putting out a number of press releases about the various scams that they have been seeing.

6. Public Comment.

AG Ford asks for any public comment. None.

7. Adjournment (For possible action).

AG Ford moved to entertain motion to adjourn. Dave Haws moved to adjourn. Andrew Campbell second. Meeting adjourned approximately 2:36 pm.

Minutes respectfully submitted by Anela Kaheaku, Office of the Attorney General.