OFFICE OF THE ATTORNEY GENERAL

Adam Paul Laxalt, *Attorney General*

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

MEETING MINUTES

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

Date and Time of Meeting: **July 26, 2017, 10:00 a.m.**

Place of Meeting: **Video Conferenced Between:**

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:

Las Vegas:	Carson City:
Members: Adam Laxalt, Chair Capt. Shawn Andersen (proxy for Mathew McCarthy) William Olsen, NV Energy Renato "Sonny" Vinuya Greg Weber, Valley Bank **Members Absent:** Jacob Cinco **Others:** Sgt. Troy Herring, City of Henderson Magann Jordan, CCDA Garrett Poiner, City of Henderson Adam Pranter, FBI **Staff:** Monica Moazez Rod Swanson	**Executive Director:** Patricia Cafferata **Members:** (Eric) Andrew Campbell Sgt. Dennis Carry (proxy for Jerry Baldridge) Washoe County Sheriff's Office Alan Cunningham, WCSD (proxy for Edward Grassia) James Earl (proxy for Sharon Rahming) Chris Lake **Members Absent:** Senator Moises Denis Assemblyman Edgar Flores **Others:** Lea Cartwright, PCIA Lea Tauchen, Retail Assn. of Nevada **Staff:** Catherine Krause Laura Tucker

1. Call to order and Roll Call.

Meeting called to order at 10:00 a.m., Marsha Landreth called roll and confirmed there was a quorum.

2. **Public Comment. Discussion only.**
None.

3. **Welcome and self-introduction of Technological Crime Advisory Board committee members.**
Attorney General Adam Laxalt welcomed everyone to the meeting, and members introduced themselves.

4. **Swearing in of new or reappointed Technological Crime Advisory Board committee members Chris Lake, William Olsen, and Renato "Sonny" Vinuya.**
AG Laxalt swore in Chris Lake, William Olsen, and Renato "Sonny" Vinuya.

5. **Discussion for possible action to approve minutes of April 5, 2017 meeting.**
AG Laxalt asked for approval of the April 5, 2017 meeting minutes. Greg Weber moved to approve the minutes. Andrew Campbell seconded the motion, and the motion passed unanimously.

6. **FBI Presentation on the Dark Web. Discussion only. Supervisory Special Agent Adam Pranter.**
SSA Adam Pranter of the Las Vegas Cyber Task Force gave a presentation explaining the three levels of the internet: the Web, the Deep Web, and the Dark Web.
    - The Web is Searchable and Indexed, accessed through search engines, i.e. Google, Bing.
    - The Deep Web contains content for which one needs authorization, i.e. a bank account number to access. There is an authentication process one must go through in order to access information, i.e. user names and passwords. The Deep Web comprises approximately 90% of the internet.
    - The Dark Web is a network that resides on the internet, but that can only be accessed using special tools. The most common browser is Tor (commonly referred to as an onion router accessed through TorProject.org [it is a modified form of Firefox]. Less commonly used are <Freenetproject.org and I2P>. The greater percentage of the Dark Web is purely illicit, sales of heroin, cocaine, illegal arms, pornography, and other illegal activities.

7. **Election of Chair and Vice Chair for one (1) year term from July 1, 2017 to June 30, 2018. Discussion and for possible action.**
Patty Cafferata noted that traditionally the Attorney General has been the Chair of the Advisory Board and a Legislator is elected Vice Chair; however, there has been no opportunity to discuss this with either legislator or with the AG. Senator Denis has a background in IT. William Olsen moved to elect AG Laxalt as Chair and Senator Mo Denis as Vice Chair. Greg Weber seconded this motion. Motion passed unanimously. Cafferata will follow up with Senator Denis to determine if he is willing to serve.

8. **Presentation on the EMV and PCI Security Standards for possible inclusion in the outreach plan. Discussion and for possible action. Greg Weber – Valley Bank.**
Greg Weber, IT Coordinator/Vice President for Valley Bank, touched on the high points of Attachment 2 - the PCI DSS Quick Reference Guide. In the late 1990s, VISA was the first

to try to come up with some consistent security standards for information exchanged across the internet and to try to combat fraud. They came to realize that VISA and MasterCard could not operate with different government standards and different policy standards, creating a need to centralize all these requirements throughout the globe. There was a combined effort of the major players (Discover, VISA, MasterCard, American Express, and JCV), who implemented the standards in December 2001.

Throughout the United States and Europe, there was lot of risky behavior occurring with merchant acceptance of payment cards: 81% of merchants store payment card numbers, 73% store payment card expiration dates, 71% store payment card verification codes, 57% store customer data, and 60% store other personal customer data. This is a major contributor to internet and bank fraud.

Weber reported that 95% of the fraud and identity theft occurs by an employee of the business, who has compromised the information. In other cases, it is a friend or family member, who has taken the information from the credit card or check.

In 2001, additional features were integrated for security, including the addition of an expiration date, a personal identification number (PIN), and a magnetic strip with two tracks of data - one accessible, the other not - to be retained by the point of sale software/merchant. More recently, there is the chip integrated into the card. The information is encrypted and therefore much harder to duplicate than the magnetic strip.

There are twelve (12) best security practices to take to secure the network so that information cannot be compromised:

1. Install and maintain a firewall configuration to protect cardholder data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;
3. Protect stored cardholder data;
4. Encrypt transmission of cardholder data across open, public networks;
5. Use and regularly update anti-virus software of programs;
6. Develop and maintain secure systems and applications;
7. Restrict access to cardholder data to only those who need to know;
8. Assign a unique ID to each person with computer access;
9. Restrict physical access to cardholder data;
10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes; and
12. Maintain a policy that addresses information security for all personnel.

A discussion ensued regarding whether to include this information with the cybersecurity information to be disseminated in October.

9. Presentation of Henderson Police Department's brochure on locating skimmers. Discussion only. Sergeant Troy Herring, Henderson Police Department (HPD). *(Attachment (3), photos of skimmers and "Protect Yourself from ATM and Gas Pump Skimming" brochure.)*

Sergeant Troy Herring noted that they have come across skimmers in several different ways: a customer will report that an ATM is not working correctly; a technician will be called out and will discover it; the device will come loose or falls off altogether; or oftentimes a victim will call the police when they realize that their card has been compromised, long after the skimmer has been removed. HPD created a pamphlet and poster for store employees. They then sent out detectives to show employees and managers pictures of actual skimming devices to show them what they look like. Sgt. Herring brought samples of the brochure. It defines what a skimmer is and outlines steps consumers can take to avoid becoming a victim of skimming. A large part is awareness of the appearance of the ATM machine itself; noticing loose parts, the presence of tape or glue; employees need to be aware of persons who spend long periods of time without conducting transactions, or who avoid depiction by covering their faces. HPD added their direct contact information to the brochure.

Since providing the posters and brochures in May, store employees located two active skimmers. They were not able to catch the suspects but did limit the exposure to residents. Sgt. Herring brought brochures for the board to review. AG Laxalt suggested that we approve something using HPD's brochure as a model. Sgt. Dennis Carry agrees; he would like to see a web-based video that one could click on to see how the skimmers work, how to check to see if it is loose to go along with it. Sgt. Herring stated that the brochure was part of a three-part program. The brochure was to get the store personnel to recognize what was going on; they did a YouTube video for the public; and they also have a skimmer warning on their Nextdoor app. Their final phase is that their analysis unit is constantly going through the reporting systems to see if fraud related reports could be traced back to skimming devices. AG Laxalt asked about the link to the YouTube video. Sgt. Herring said the link is (https://www.youtube.com/watch?v=cOanyy0Bf7c).

10. Presentation on agenda topics and participants in the outreach plan to small businesses and local communities. Discussion and for possible action. Laura Tucker, AGO.
(*Attachment Four (4), NRS 603A Compliance checklist and Attachment Five (5) PowerPoint – Cybersecurity for Individuals and Small Businesses in Nevada.)*
Laura Tucker created a Powerpoint presentation to be given during Cybersecurity month in October. It is broken down into three different parts. The first part covers trends that we see in tech scams against both small businesses and individuals, including what to look for and how to prevent them. The second part is on skimmers with some photos that were received from the Henderson Police Dept. It is similar to the presentation given by Sgt. Herring and the pamphlet has tips on what to look for both as a small business owner and as an individual. The third area is data breaches; that included tips for individuals and for small businesses and also has some instruction/explanation for business on what their duties are under NRS603A. Finally, there is a checklist for small businesses to help them figure out if they are in compliance with the statute.

Tucker presented the PowerPoint presentation briefly, as the full presentation runs for 40 minutes. She requested that the advisory board members review the presentation, which was sent out with the agenda. She would appreciate feedback or modifications. Dependent upon who is presenting, there may be additional topics to add; it can be presented by an individual or by a panel.

11. **Creating promotions for outreach to small business and local communities during National Cybersecurity Awareness month in October 2017. Discussion and for possible action. Monica Moazez, AGO.**

Monica Moazez reported that she and Laura Tucker had discussed targeting up to 10 Chambers of Commerce around the state for members of the board to present the PowerPoint. They would create a "toolkit:" a cybersecurity orientation, i.e., a physical folder or something bound together that would contain resources such as the PCI reference guide, plus five or seven pages of handouts which would, from our office's standpoint, broadly introduce why cybersecurity is important, along with relevant statistics.

Our office, for example, has a yearly training online (through the State of Nevada Online Professional Development Center eLearning Center); the AG IT department graciously circulates emails whenever there is a scam, virus or something to be aware of. A handout would also be included making readers aware of statutory standards and of the behavior of the business' employees. The last thing she suggested is to encourage businesses to develop a cybersecurity checklist, security risk assessment, and employee and network monitoring. She hopes to produce this toolkit, plans to email board members drafts for feedback and suggestions, and upon approval, send them to state printing for production as packets. They can also be uploaded to a website to download as needed.

Sonny Vinuya mentioned translations of the packets. Moazez has a Spanish translator available. Vinuya would be able to assist with obtaining Asian translation. He also suggested presentations of the panel/PowerPoint as part of the Lunch and Learn format already in place.

AG Laxalt asked whether these presentations could be put on in October. Per Moazez, this will depend on how many members of the group are willing to present. Laura Tucker is willing to train and willing to accompany; Moazez is also willing to accompany members. She suggests circulating an email for response to gauge interest to participate. AG Laxalt asked the members if they or their organizations would be willing to participate. His preference would be for a three-member panel: law enforcement, an IT person, and a member of the AG's staff. He asked for an indication of who would be willing to volunteer, not necessarily for all 10, but for at least a few. All persons in Las Vegas indicated willingness; in Carson, Patty Cafferata and Alan Cunningham volunteered. Carry stated that his department and partners do a lot of presentation already and is sure that they could transition to this from what they already do. Catherine Krause volunteered per the AG's request.

Cunningham stated that the National Institute of Standards and Technology (https://www.nist.gov/) has documents available that we may want to look at instead of creating a new tool guide. The other thing he would like to see included in the presentation is password strength; moving password strength to eight digits and above makes a huge difference; that 95% of the problems could be eliminated just by increasing password strength.

AG Laxalt suggested we prepare the cybersecurity presentations for October.

On the Distance Learning suggestion, that is a great idea, but AG Laxalt would like to see it done live, with a web portal like a town hall if we have that capability. Per Catherine Krause, the AGO does not, but others may; Cunningham stated that the capability to conduct that type of training exists through Skype.

Cunningham stated that there are also links already available for fee-based online training. Every Washoe County School district employee must go through online training through www.safeschools.com (NOTE: subset of ScenarioLearning.com which also has a safepersonnel.com sector customizable for municipalities, businesses, non-profits, and insurance providers; for example they offer fee based courses on cybersecurity and active shooters).

AG Laxalt noted the information is more than Moazez would be able to include for production by October, but we should definitely include in the list of things to look at. If we can aim for a Livestream, set up a panel, advertise so that people can just log in, and get 100 or 200 people from around the state, that would be good.

William Olsen stated that each type of presentation is going to attract a different audience. AG Laxalt suggested we look at doing both, a video for businesses as suggested by Carry as well as a Skype or Facebook presentation for individuals. Olsen also recommended more emphasis on phishing. He has noticed that more of the scams he sees are attributable to phishing.

Christopher Lake stated that it might be nice if after a business or an individual participates in this if we could send them a small document suitable for framing that said “Name has participated in Cybersecurity Training” as a matter of pride, but also as a deterrent so that when people walk in [to a business], if they do not know what this really means but maybe they’ll move on to the next gas station. Per AG Laxalt, we would have to investigate whether we have to authority to issue such a document.

Vinuya stated that he likes the idea of both the video and the broadcast. In the chamber of commerce, a lot of the business owners such as restaurant owners cannot get away from their restaurants to attend meetings or trainings.

It was suggested that included in the toolkit should be a resource page with a listing of websites and phone numbers of the various agencies and offices that can provide information and assistance. AG Laxalt stated that something similar had been produced for the Domestic Violence Board and it turned out very well.

It was stated that information goes out to the casinos and resorts through Infragard.com (FBI information service) and the Southern Nevada Cybersecurity Alliance www.snca.org. We can extend our reach by making them aware of our information.

12. **Accepting the $1,344.69 forfeiture funds into the Attorney General’s general operating budget to promote National Cybersecurity Awareness month in October 2017. Discussion and for possible actions. Patty Cafferata, AGO.**

Need official action by the board that we will use this forfeiture money for the printing and promotion of Cybersecurity month. Motion to approve $1,344.69 use this forfeiture money for the printing and promotion of Cybersecurity month by William Olsen. Second by Sonny Vinuya. The vote was unanimous to approve.

13. **Next meeting: November 27, 2017 at 10:00 a.m.**

14. **Public Comment. Discussion only.**
None.

15. **Adjournment.**
AG Laxalt called for a motion to adjourn the meeting. Weber moved to adjourn, Olsen seconded, and the motion passed unanimously. The meeting adjourned at approximately 11:35 a.m.

Minutes respectfully submitted by Marsha Landreth, Office of the Attorney General.