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

TECHNOLOGICAL CRIME ADVISORY BOARD

April 5, 2017 – 10:00 a.m.
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

AGENDA

Please Note: The Technological Crime Advisory Board may: 1) take agenda items out of order; 2) combine two or more items for consideration; or 3) remove an item from the agenda or delay discussion related to an item at any time. Reasonable efforts will be made to assist and accommodate physically handicapped persons, who wish to attend this meeting. Please contact Patricia D. Cafferata, Technological Crime Advisory Board Executive Director, at (775) 684-1136 or pcafferata@ag.nv.gov in advance, so that arrangements can be made.

1. **Call to Order and Roll Call**.

2. **Public Comment**. **Discussion only.**
   Action may not be taken on any matter brought up under this agenda item, until scheduled on the agenda of a future meeting for possible action.

3. **Welcome and self-introduction of Technological Crime Advisory Board committee members.** Adam Laxalt, Attorney General.

4. **Swearing in of new or reappointed Technological Crime Advisory Board committee members, Senator Moises Dennis, (Eric) Andrew Campbell, Jacob Cinco and Matthew McCarthy.**

5. **Discussion and possible action to approve minutes of January 11, 2017 meeting.**
   (Attachment One (1), Minutes from January 11, 2017 Meeting.).

6. **Report on the survey of the Technological Crime Advisory Board committee members on various issues**. Patricia D. Cafferata, Executive Director.
   (Attachment Two (2) Survey results).

7. **Discussion and possible action on Technological Crime Advisory Board members' survey results and how to achieve the Board's goals of Hispanic and small business outreach for 2017**.

8. **Report on outreach to broadcasting entities and the development of a Public Service Announcement (PSAO) for the Board.** Moises Denis, Senator.

9. **Presentation on the PSA process.** Mary Beth Seward and Judy Reich. Nevada Broadcasters Association

10. **Presentation regarding information on ways to communicate without digital technology.** (Eric) Andrew Campbell, Educator Churchill County School District.

11. **Report on forfeiture funds received.** Patricia D. Cafferata, Executive Director. (Attachment Three (3) Letter from LVMPD).

12. **Discussion and possible action on expenditure of forfeiture funds pursuant to NRS 205A.090.**

13. **Report from the Attorney General' Fraud Unit on skimmer device legislation in other states.** Daniel Westmeyer, Senior Deputy Attorney General. (Attachment Four (4) Memo on Research).

14. **Future meeting times are set for on July 19, 2017 and November 6, 2017 at 10 a.m. in Attorney General's offices.**

15. **Public Comment. Discussion only.** Action may not be taken on any matter brought up under this agenda item, until scheduled on the agenda of a future meeting for possible action.

16. **Adjournment**.

In accordance with NRS 241.020, this agenda was posted on or before March 31, 2017 online at: http://ag.nv.gov/About/Administration/Tech_Crime/2015_Mtgs/Tech_Crime_Meetings_2015/ and at the following locations:

- Office of the Attorney General, 100 N. Carson Street, Carson City, NV 89701
- Office of the Attorney General, 5450 Kietzke Lane, Suite 202, Reno, NV 89511
- Office of the Attorney General, Grant Sawyer Building, 555 E. Washington Ave., Las Vegas, NV 89101
- Legislative Building, 401 N. Carson Street, Carson City, NV 89701
- Capitol Building, 101 N. Carson Street, Carson City, NV 89701

Meeting materials may be requested from Patricia D. Cafferata, Technological Crime Advisory Board Executive Director, at (775) 684-1136 or pcafferata@ag.nv.gov, and obtained from the Office of the Attorney General at any of the first three (3) locations listed above.

Attachment One (1)

to

Technological Crime Advisory Board Agenda

April 5, 2017

Contents: Minutes of January 11, 2017 Meeting

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

MEETING MINUTES

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

Date and Time of Meeting: **January 11, 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 in Attendance:	**Members in Attendance:**
Assemblyman Edgar Flores, Vice Chair	Adam Laxalt, Chair
Jacob Cinco	Jerry Baldridge
Senator Moises Denis	Patricia Cafferata, Executive Director
Mathew McCarthy	(Eric) Andrew Campbell
Patrick Moers	Edward Grassia
Greg Weber	Shannon Rahming
Guests in Attendance:	**Guests in Attendance:**
Rod Swanson	Jim Estes
Daniel Westmeyer	Laura Tucker

1. **Call to order and Roll Call.**
   Meeting called to order at 10:00 a.m., Patricia Cafferata called roll and confirmed there was a quorum present.

2. **Attorney General Adam Laxalt's welcome and self-introduction of members.**
   Attorney General Adam Laxalt welcomed everyone to the meeting, and members introduced themselves.

3. **Swearing in of new committee members.**
   None

4. **Public Comment. Discussion only. Action may not be taken on any matter brought up under this agenda item, until scheduled on the agenda of a future meeting for possible action.**
   No Public Comment.

5. Discussion for possible action to approve minutes of November 8, 2016 meeting.
Laxalt asked for approval of the November 8, 2016 meeting minutes. Mathew McCarthy moved to approve the minutes. Shannon Rahming seconded the motion, and the motion passed unanimously.

6. EITS Division Administrator Shannon Rahming report on the December 1, 2016 Cyber Clinic and future plans for additional clinics.

a. Cyber Clinic

On December 1, 2016 a Cyber Clinic was held at the Governor's Mansion in Carson City. This Cyber Clinic was modeled after a Cyber Clinic held at the University of Nevada, Reno (UNR) and was coordinated by Rahming. Eighteen students from the Cyber Club at UNR, including a member, ranked 28th out of 1,050 collegiate students in a national Black Hat competition assisted in this event. For fun, giveaways at the door for those who attended included gift cards. One-Hundred-Eighty state employees attended from 23 different agencies, including a few family members.

The primary focus of the Cyber Clinic was mobile device basics, including back up, passwords, duo password, and having more than one access option. The Cyber Club did skills assessments of the participants, with rankings of either beginning, intermediate, or advanced levels. A skills sheet was given to each of the participants with recommendations and questions. Round tables were set up as stations for participants to talk to Cyber Club members. Rahming shared the positive feedback received at the event as well as a few pictures.

b. Future plans for additional clinics

There are requests for a similar clinic in Las Vegas. To that end, Rahming is in touch with James Elste, Co-Director of the Cyber Security Center at UNR, as well as contacting UNLV to see if there is a similar club. Rahming will also be contacting the College of Southern Nevada (CSN) as they have started a new cyber curriculum, to see if they would be interested in putting on a similar Cyber Clinic. If not, she will be looking into the possibility of bringing the UNR Cyber Club to Las Vegas for a Cyber Clinic. Senator Moises Denis volunteered to check with UNLV regarding whether or not an organization similar to the Cyber Club at UNR exists. When asked if a Las Vegas clinic could be run with fewer Cyber Club members, Rahming indicated that it could be done with approximately 12 members. A possible venue has been offered by Switch Company in its Innovation Center as a possible venue for a Las Vegas Cyber Clinic. This is preferable as the state buildings and local colleges have parking availability issues.

Additional clinics have been requested in Carson City for the city personnel and law enforcement agencies. Cyber Club at UNR is more than willing to participate in these clinics.

7. Member Andrew Campbell to present information on the possibility of communication without digital means.

No presentation available at this time. He noted that his research so far has shown that the publicly available information on infrastructure is out-of-date. As an educator, he is concerned about students being over dependent upon technology. In the event of a catastrophic change or disaster, education on what resources are available to students and how would they access them without a significant gap in their education. He hopes to have the presentation available for the next meeting.

8. Possible action on 2017 goals

a. Methods for Hispanic outreach to educate the community of identity theft - Agenda Item 8(a) and educating small businesses on how to protect them from cybersecurity – Agenda Item 8(b).

Assemblyman Edgar Flores has been working with the board on specific Hispanic outreach education regarding identity theft and other cybercrimes that are prevalent to that community. However, as agenda items 8(a) Hispanic outreach education regarding identity theft and 8(b) Small business cybersecurity education are directly connected, he suggested the Board's outreach and education plans could be combined. Reno/Sparks Chambers, Clark County Chamber of Commerce, and the Hispanic Chamber of Commerce are all interested in being a part of these outreach programs. Laxalt proposed bringing these chambers together on these outreach programs.

Metro Deputy Chief Mathew McCarthy agreed that it would be beneficial to combine these items, as the needs of these communities are similar. Washoe County School District Edward Grassia noted that overreach in this area was not possible—that the compartmentalization of the training is not necessary.

Flores noted that there are some different issues in the Hispanic community than in the business community. Specifically he mentioned, phone schemes by predatory businesses using legal retaliation threats against Spanish-speaking only community.

Denis suggested that we remain flexible in the program in order to be inclusionary. The integration of the Cyber Clinic mobile device training would also be beneficial to add to these outreach plans. Laxalt agreed that it would be beneficial to add the Cyber Clinic education but that the logistics of bringing a Cyber Clinic to all of these communities might not be feasible. Instead, he suggested that if it is not feasible to have Cyber Clinic, the board create a self-contained program.

Campbell offered a suggestion regarding education of businesses to contact their insurance companies regarding coverage for their personal computers. In his experience, there are extension policies to include computers. These policies are a new feature that is worth adding to small businesses' policies.

Laxalt asked if there was a motion for approval of moving forward with agenda items 8(a) and 8(b) together as one program. Flores so moved. Henderson Chief of Police Patrick Moers seconded the motion.

Discussion:
Denis asked for clarification if the board was moving to vote on agenda items 8(a) and 8(b) only or if there was going to discuss the other agenda items under #8. He wanted to discuss Public Service Announcements (PSAs). He further noted that he has worked with PSAs in the Hispanic Media and as well as the Nevada Broadcasters Association in the past.

Laxalt clarified that the vote would only pertain to the two agenda items 8(a) and 8(b) and the rest of the agenda items under 8 would be discussed after the vote. He sees PSAs as a subset of agenda items 8(a) and 8(b). However, he does not want to lock the board into PSAs yet due to budgetary considerations. He held that 8(a) and 8(b) as the general goal for 2017 and added that hopefully PSAs will be a part of that goal. He asked Denis if he is willing to work with the Board to reach out to broadcasting entities for possible PSA. He agreed.

Laxalt asked if there was any further discussion. No further discussion. The motion unanimously passed.

Laxalt asked the board members to e-mail Cafferata the bullet point input on these goals before the next meeting in April.

b. <u>Member suggestions for discussion - Agenda Item 8(e).</u>

Flores discussed ATM and credit card skimmers issue and the difficulties of small businesses to defend against ATM and credit card skimmers. Flores is authoring a bill to standardize the issuance and use of a sticker that show whether or not an ATM or credit card reader has been tampered with. The stickers work in three ways:

1) If part of the sticker is covered, it shows that a skimming device has been put on top of the ATM or credit card reader;
2) If the sticker has been cut, it can show that there has been tampering with the back of the credit card reader or ATM; and
3) Employees for the businesses that employ the stickers can do a quick visual inspection to see if the credit card reader or ATM has been tampered with.

Stickers are in use now, however, there is no universal standard. Without a universal standard for a sticker, anyone can purchase a sticker. Flores offered this as the most effective and economical solution for small businesses. There would be a bidding process, and one company would be chosen to print these stickers for the State.

McCarthy inquired if the State were to employ this system as a guarantee of safety, would the State be liable if the sticker was circumvented. Laxalt noted that there could be some possible liability issues depending on who would be making the sticker and setting the regulations.

Jacob Cinco of the United States Secret Service informed the Board that hot steaming and replacing these stickers is already taking place. The devices of the skimmers have become more sophisticated with Bluetooth technology which does not require any tampering of the reader, only one-time access. One key style is used for gas pump machines, only one key is needed to get access to the gas pump.

Instead of the State setting the standard, Cinco proposed that the credit card companies as well as gas companies would have to set the standards, since they are the ones who are charged with holding people's financial data. The small businesses are not necessarily liable for the circumventing of the credit card readers once swiped. With the stickers, there are issues regarding who is liable, if there is a breach.

Denis noted that if there is going to be legislation to fight this issue that the credit card companies should participate in the creation in that legislation. The public reliance on the sticker as a guarantee of safety and security is problematic, when there is a lack of education regarding the issue. If there is no incentive for the business to address this issue, perhaps publishing the names of the businesses that have been targeted might become incentive enough to force them to take action to curtail skimming.

Valley Bank's Greg Webber added that the sticker is a simple solution to a complex problem and not effective. Rather, education is needed on the part of the small businesses on how to monitor their own equipment and creating standard to protect customer information. Public education on these issues through PSAs on the issue to alert businesses when they see something suspicious. Larger businesses have access to technological professionals that are actively monitoring these problems. However, small businesses do not necessarily have that kind of support. Credit card companies already have aggressive programs for PCI compliance for Point of Sale transactions.

Flores thanked the Board members for their input, and he looks forward to discussing this further. If standards could be created with collaboration with law enforcement, it could ease the burden for law enforcement. Moving forward, the inclusion of credit card companies in any legislation would be for the best.

Moers stated the stickers are not a bad idea, as a tool for education. Education signage regarding skimming near card readers like the signage for gambling addiction in casinos could be a part of that education as well. This would inform the consumer of the dangers. Businesses should be required to notify their customers, when a breach has taken place. Customers are not finding out from the businesses that there has been a breach. Implementing a 30-day period after a breach for the business to advise their customers that there has been a breach might be a solution.

Laxalt asked the committee to bring information regarding this issue and possible remedies to the next meeting for a vote.

Denis inquired as to whether any cybercrime legislation has been proposed from the committee or state agency? Laxalt did not recall seeing any such legislation but offered to send any proposed bills he comes across.

Flores noted that there had been discussion about possession of a skimming device would be evidence of unlawful intent. McCarthy noted that the language could mirror enhancement for tools in a burglary—shows intent. However, this proposal was abandoned as devices, such as, credit card squares used for small businesses

would fall under that definition. Several committee members commented that skimming devices are so different in appearance that no one would mistake them for the legitimate devices used by businesses. Weber also noted that it is evident that the skimming devices serve no other purpose than to steal information. The average person might not see the sleeve skimming device but anyone in the industry would. He further added that skimming devices are not similar to legitimate business devices being used. Senior Deputy Attorney General Daniel Westmeyer noted that from the legislative perspective the difficulty is in drafting a piece of legislation that differentiates between legitimate business machines and skimmers. Laxalt asked and Westmeyer agreed to research for legislation in other states addressing this issue.

Grassia noted that education rather than legislation might be more effective to protect and inform people on how to take care of themselves. The technology is moving on quickly with card-less POS systems and ATMs. Anything that might be proposed this or next session could be obsolete before implementation. The Committee agreed.

Laxalt opened the floor for more suggestions. There were none.

9. Announcement. Next meeting is set for April 5, 2017 at 10 a.m.

10. Public Comment. Discussion only. Action may not be taken on any matter brought up under this agenda item, until scheduled on the agenda of a future meeting for possible action.
No Public Comment.

11. Adjournment.
The meeting was adjourned at approximately 11:03 a.m.

Minutes respectfully submitted by Nicole E. Fairfield.

In accordance with NRS 241.020, this agenda was posted on or before January 6, 2017 online at:
http://ag.nv.gov/About/Administration/Tech_Crime/2015_Mtgs/Tech_Crime_Meetings_2015/
and at the following locations:

- Office of the Attorney General, 100 N. Carson Street, Carson City, NV 89701
- Office of the Attorney General, 5450 Kietzke Lane, Suite 202, Reno, NV 89511
- Office of the Attorney General, Grant Sawyer Building, 555 E. Washington Ave., Las Vegas, NV 89101
- Legislative Building, 401 N. Carson Street, Carson City, NV 89701
- Capitol Building, 101 N. Carson Street, Carson City, NV 89701

Meeting materials may be requested from Patricia D. Cafferata, Advisory Board Executive Director, at (775) 684-1136 or pcafferata@ag.nv.gov, and obtained from the Office of the Attorney General at any of the first three (3) locations listed above.

Attachment Two (2)

to

Technological Crime Advisory Board Agenda

April 5, 2017

Contents: Survey Results

Goals for 2017 Tech Crime Board

Responder	Willing to Participate in Chamber Briefings	Willing to Participate in Cybersecurity Clinics	Public Service Announcement Participation	Proposed Legislative Suggestions	Expand Beyond Goals	Cyber-security Awareness Month Suggestion	Additional Comments
Responder 1	Yes, limited to Las Vegas and Reno	Yes, re guidance reporting incidents to law enforcement.	Yes, but do not have any contacts to produce a PSA	Review of Payment Card Industry Data Security Standards	Law Enforcement conducting briefings and documents re financial crimes & Cybersecurity	October	Community outreach should include UNLV & UNR sm. Bus. Development Cntr.
Responder 2	Yes, has 30+ years IT Experience	Yes, and with help from her staff re IT and cyber knowledge.	Could be helpful, but do not have any contacts to produce PSAs	Propose assistance in molding Cyber Defense Center	To complete goals, keep focus on current goals	October	n/a
Responder 3	Yes, has a security team and personal IT security experience	Yes, has a security team and personal IT security experience	Possibly, if brief and specific, although could work against effectiveness, no contacts	Educational programs for businesses and individual citizens.	n/a	Ready by Sept.- roll out conjunction w/ Cybersecurity Awareness Month	n/a
Responder 4	Yes, discuss consumer protection issues	Yes, discus protection against scams and cyberattacks, and steps to take after an attack	Yes, but do not have any contacts to produce a PSA	Update the notice requirement after a data breach	n/a	October	n/a
Responder 5	Yes, although would be logistically and financially difficult to support	No, unfortunately outside the scope of investigative duties	Yes, but do not have any contacts to produce a PSA	n/a	Sticking to stated goals may be more effective.	October	n/a
Responder 6	Yes, offering basic measures business should take re cybersecurity tied to avoiding ID theft	Yes, clinics based on UNR Cyber Club concepts	Yes, but do not have any contacts to produce a PSA	n/a	Recommend not discussing medical and other records, not included in statute	October	n/a
Responder 7	No, Short on personnel at this time.	Yes, to answer question and give support re law enforcement prospective and protecting ID and steps if ID is stolen.	Have done PSAs in the past. Only helpful for short periods of time. PIO Bob Harmon may be able to assist.	n/a	n/a	October	n/a
Responder 8	Yes	Yes, would try and replicate similar offering in coorporation with UNLV	No, do not have any contacts.	None	n/a	September or October especially if looking to engage UNLV	n/a

Prepared by Jan Riherd
Updated March 22, 2017

Attachment Three (3)

to

Technological Crime Advisory Board Agenda

April 5, 2017

Contents: Letter from LVMPD

LAS VEGAS METROPOLITAN
POLICE DEPARTMENT
JOSEPH LOMBARDO, Sheriff

Partners with the Community

February 17, 2017

Brett Kandt, Director
Nevada Technological Crime Advisory Board
5420 Kietzke Lane, Ste 202
Reno, NV 89511

In Response, Please Reply To:
Tracy Krylo, Analyst
702-828-3043

Re: EV# 140305-0508

Mr. Kandt:

As provided by NRS 179.1233,1, we are forwarding a check in the amount of $1,344.69. This is the result of a Guilty Plea Agreement under our event # 140305-0508.

NRS 179.1233 Sale of forfeited property; use of proceeds; deposit of balance of proceeds in Account for the Technological Crime Advisory Board; payment of certain encumbrances.

1. The State, county or city shall sell any property forfeited pursuant to NRS 179.1219 or 179.1229 as soon as commercially feasible. Except as otherwise provided in subsection 2, the proceeds from such a sale must be used first for payment of all proper expenses of any proceedings for the forfeiture and sale, including, without limitation, any expenses for the seizure and maintenance of the property, advertising and court costs. The balance of the proceeds, if any, must be deposited in the Account for the Technological Crime Advisory Board created pursuant to NRS 205A.090.

The gross forfeiture was $5,378.75. We did not have any costs associated with this Guilty Plea Agreement and no other agencies were involved. Per NRS 205A.090, 3(b) we have retained 75% of this forfeiture. The balance of $1,344.69 to be deposited into the account for the "Technological Crime Advisory Board".

NRS 205A.090 Account for the Technological Crime Advisory Board: Creation; use; distribution of money in Account as result of certain criminal or civil forfeitures.

3. For each criminal or civil forfeiture carried out pursuant to NRS 179.1211 to 179.1235, inclusive, the Board shall distribute the money deposited into the Account pursuant to NRS 179.1233 in the following manner:

(b) Not more than 75 percent to be distributed to the federal, state and local law enforcement agencies that participated in the investigation of the unlawful act giving rise to the criminal or civil forfeiture in accordance with the level of participation of each law enforcement agency as determined by the Board. If the participating law enforcement agencies have entered into an agreement to share any such money, the Board shall distribute the money to the law enforcement agencies in accordance with the provisions of the agreement.

Sincerely,
LAS VEGAS METROPOLITAN POLICE DEPARTMENT

Judy Bleak

Judy Bleak, Accounting Director
Office of Finance

Attachment Four (4)

to

Technological Crime Advisory Board Agenda

April 5, 2017

Contents: Memo on Research

ADAM PAUL LAXALT
Attorney General

WESLEY K. DUNCAN
First Assistant Attorney General

NICHOLAS A. TRUTANICH
Chief of Staff

KETAN D. BHIRUD
General Counsel

STATE OF NEVADA

OFFICE OF THE ATTORNEY GENERAL

555 East Washington Avenue, Suite 3900
Las Vegas, Nevada 89101

MEMORANDUM

To: All Members of the Technological Crimes Advisory Board

From: Daniel Westmeyer, Senior Deputy Attorney General
702-486-3191; dwestmeyer@ag.nv.gov

Subject: State Criminal Laws Pertaining to Skimming Devices

Date: March 22, 2017

At the January meeting of the Technological Crimes Advisory Board, I was asked by the Attorney General to provide a review of state criminal laws pertaining to ATM skimmers and similar devices, as well as any legal challenges to such laws. I was able to review several states' anti-skimming laws and legal challenges thereto.

A. Nevada:

Nevada already has an anti-skimming law. Since 2003, NRS §§ 205.605 and 205.608 have criminalized the use and possession of reencoders and card skimming devices. NRS § 205.603 defines "reencoder" as "an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different payment card." NRS 205.604 defines "scanning device" as "a scanner, reader or any other electronic device that is used to access, read, scan, obtain, memorize or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card."

Possession of a reencoder or scanning device is criminal when done with the intent to defraud. Possession is classified as a Category C felony under NRS § 205.606, carrying a maximum prison term of five (5) years. Use of a scanning device or reencoder is classified as a Category B felony under NRS § 205.605, carrying a maximum penalty of twenty (20) years. The law includes exemptions for using card scanners in the ordinary course of business and for authorized financial transactions (NRS § 205.607). There is only one case in Nevada appealing a conviction for a card-skimming device, *Andrjasov v. State*, 2016 WL 1615686. This unpublished case obviously has little precedential weight, and in any event, the appellant did not challenge the legality of the statute.

B. Other Western States:

California's skimming device statute was passed in 2002 (California Penal Code § 502.6). The language is similar to Nevada's statute, but the punishment is much less severe. Whereas use and possession in Nevada amount to felonies, in California they amount to misdemeanors. Instead of including exemptions, criminal possession and use must be shown to be "knowingly, willfully, and with the intent to defraud." The California statute defines "reencoder" identically with the Nevada statute. *See* California Penal Code § 502.6(e)(2).

Like Nevada, California courts have not confronted the issue of the legality of these statutes. Several unpublished decisions in California reference the statute, but no appellant has challenged its legality. *See People v. Hamilton*, 2016 WL 6651385; *see also People v. Torres*, 2014 WL 6634816.

Arizona enacted an anti-skimming statute in 2002, criminalizing the creation, possession, and use of a scanning device or reencoder without the permission of the cardholder (A.R.S. § 13-2110). "Reencoder" is defined as "an electronic device that places encoded information from the magnetic strip or stripe of a credit card onto the magnetic strip or stripe of a different credit card." "Scanning device" is defined as "a scanner, reader or other electronic device that is used to access, read, scan, obtain, memorize or store, temporarily or permanently, information that is encoded on a magnetic strip or stripe of a credit card." A.R.S. § 13-2101.

In Arizona, creation and possession are criminal when done with intent to commit fraud; use is criminal when done without the permission of the cardholder and with intent to defraud. The only exemption listed is for peace officers or prosecutors who possess such devices in the "performance of their duties." There is no appellate case law citing to this statute. The original classification of this crime in Arizona was a Class 6 Felony (6-18 months), but in 2016, it was increased to a Class 4 Felony (18-36 months)[1].

The biggest difference in language among Western states is the Oregon statute (O.R.S. § 165.074). That statute was originally passed in 1991, dealing with unlawful factoring of payments by merchants, and skimming or reencoding was added in 2003. Because the relevant parts were added on to an existing statute, the language deals with only with using scanning devices or reencoders, and not with possession or creation. Use of either a scanning device or a reencoder is criminal if done without the permission of the cardholder or with intent to defraud. Violation of this statute is a Class C felony, and repeat offenders are guilty of Class B felonies. The only appellate case regarding this statute was in regards to the sentencing for other offenses, and did not challenge this statute directly. *See State v. Mallory*, 213 Ore. App. 392 (2007).

[1] According to A.R.S. § 13-702(D), felony sentences for first time offenders in Arizona fit into one of five categories: Mitigated, Minimum, Presumptive, Maximum, and Aggravated. For purposes of this memo, I have not included the Mitigated or Aggravated sentences as part of the sentencing range.

C. Conclusions

Thirty-one (31) states have statutes that provide criminal penalties for using a card skimming device and/or reencoder. Of these, twelve (12) punish the crime as a misdemeanor (if a first offense). Some states increase penalties for subsequent convictions.

Nevada's statute appears to be in accord with similar statutes in other states, both in terms of defining language and penalties. If the Board so requests, I can dig deeper into the other twenty-seven (27) states' statutes, but my cursory review of these suggests that the language is the same or similar to our own.

If there is any additional follow-up requested by the Board, I would be happy to do so.

By: /s/
DANIEL WESTMEYER
Senior Deputy Attorney General

APPENDIX TO MEMO—STATE STATUTES

Nevada Revised Statutes

NRS 205.603 "Reencoder" defined. "Reencoder" means an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different payment card.

(Added to NRS by 2003, 1354)

NRS 205.604 "Scanning device" defined. "Scanning device" means a scanner, reader or any other electronic device that is used to access, read, scan, obtain, memorize or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card.

(Added to NRS by 2003, 1354)

NRS 205.605 Using scanning device or reencoder to defraud.

1. A person shall not:

(a) Use a scanning device to access, read, obtain, memorize or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card:

(1) Without the permission of the authorized user of the payment card; and

(2) With the intent to defraud the authorized user, the issuer of the payment card or any other person.

(b) Use a reencoder to place information encoded on the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card:

(1) Without the permission of the authorized user of the card from which the information is being reencoded; and

(2) With the intent to defraud the authorized user, the issuer of the payment card or any other person.

2. A person who violates any provision of this section is guilty of a category B felony and shall be punished by imprisonment in the state prison for a minimum term of not less than 1 year and a maximum term of not more than 20 years, and may be further punished by a fine of not more than $100,000.

3. In addition to any other penalty, the court shall order a person who violates any provision of this section to pay restitution, including, without limitation, any attorney's fees and costs incurred to:

(a) Repair the credit history or rating of each person who is a victim of the violation; and

(b) Satisfy a debt, lien or other obligation incurred by each person who is a victim of the violation.

(Added to NRS by 2003, 1354)

NRS 205.606 Possession of scanning device or reencoder for unlawful purpose.

1. A person shall not possess a scanning device or reencoder with the intent to use the scanning device or reencoder for an unlawful purpose.

2. A person who violates any provision of this section is guilty of a category C felony and shall be punished as provided in NRS 193.130.

(Added to NRS by 2003, 1355)

NRS 205.607 Exempt persons. The provisions of NRS 205.601 to 205.608, inclusive, do not apply to any person who, without the intent to defraud or commit an unlawful act, possesses or uses a scanning device or reencoder:

1. In the ordinary course of his or her business or employment; or

2. Pursuant to a financial transaction entered into with an authorized user of a payment card who has given permission for the financial transaction.

(Added to NRS by 2003, 1355)

California Penal Code Section 502.6

(a) Any person who knowingly, willfully, and with the intent to defraud, possesses a scanning device, or who knowingly, willfully, and with intent to defraud, uses a scanning device to access, read, obtain, memorize or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card without the permission of the authorized user of the payment card is guilty of a misdemeanor, punishable by a term in a county jail not to exceed one year, or a fine of one thousand dollars ($1,000), or both the imprisonment and fine.

(b) Any person who knowingly, willfully, and with the intent to defraud, possesses a reencoder, or who knowingly, willfully, and with intent to defraud, uses a reencoder to place encoded information on the magnetic strip or stripe of a payment card or any electronic medium that allows an authorized transaction to occur, without the permission of the authorized user of the payment card from which the information is being reencoded is guilty of a misdemeanor, punishable by a term in a county jail not to exceed one year, or a fine of one thousand dollars ($1,000), or both the imprisonment and fine.

…

(e) As used in this section, the following definitions apply:

(1) "Scanning device" means a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card.

(2) "Reencoder" means an electronic device that places encoded information from the magnetic strip or stripe of a payment card on to the magnetic strip or stripe of a different payment card.

Arizona Revised Statutes

13-2101. Definitions

In this chapter, unless the context otherwise requires:

…

10. "Reencoder" means an electronic device that places encoded information from the magnetic strip or stripe of a credit card onto the magnetic strip or stripe of a different credit card.

11. "Scanning device" means a scanner, reader or other electronic device that is used to access, read, scan, obtain, memorize, transmit or store, temporarily or permanently, information that is encoded on a magnetic strip or stripe of a credit card.

13-2110. Unlawful possession or use of scanning device or reencoder; classification

A. It is unlawful for a person to use a scanning device or reencoder without the permission of the cardholder of the credit card from which the information is being scanned or reencoded and with the intent to defraud the cardholder, the issuer or a merchant.

B. It is unlawful for a person to intentionally or knowingly make or possess with the intent to commit fraud any device, apparatus, equipment, software, article, material, good, property or supply that is specifically designed or adapted for use as or in a scanning device or a reencoder.

C. Subsection B of this section does not apply to peace officers or prosecutors in the performance of their duties.

D. A person who violates this section is guilty of a class 4 felony.

Oregon Revised Statutes
2015 ORS 165.074
Unlawful factoring of payment card transaction
(1) A person commits the crime of unlawful factoring of a payment card transaction if the person intentionally or knowingly:
…
(d) Uses a scanning device to access, read, scan, obtain, memorize or store information encoded on a payment card:
(A) Without the permission of the cardholder; or
(B) With the intent to defraud another person; or
(e) Uses a reencoder to place encoded information from one payment card onto another payment card:
(A) Without the permission of the cardholder of the payment card from which encoded information is being taken; or
(B) With the intention to defraud another person.
(2) Unlawful factoring of a payment card transaction is a Class C felony.
(3) Notwithstanding subsection (2) of this section, unlawful factoring of a payment card transaction is a Class B felony if the person has one or more previous convictions under this section. [1991 c.398 §2; 2003 c.383 §2]