

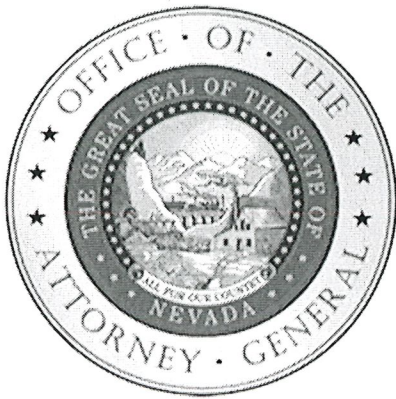
Attachment One (1)

to

Technological Crime Advisory Board Agenda

May 10, 2018

Minutes from February 28, 2018 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 Crimes Advisory Board
Date and Time of Meeting: February 28, 2018 at 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:

<p>Las Vegas:</p> <p><u>Members in Attendance:</u> Jacob Cinco, U.S. Secret Service Deputy Chief Christopher Darcy, LVMPD Senator Moises "Mo" Dennis Assemblywoman Sandra Jauregui Robert Kopacz, Proxy for Bill Olsen, NV Energy Renato "Sonny" Vinuya, Nevada State Bank Greg Weber, Valley Bank of Nevada</p> <p><u>Guests in Attendance:</u> Monica Moazez, AGO</p>	<p>Carson City:</p> <p><u>Members in Attendance:</u> Adam Laxalt, Attorney General, Chair Andrew Campbell, Churchill County School District Alan Cunningham, Washoe County School District Captain Greg Herrera, Washoe County Sheriff's Office Patricia Cafferata, Executive Director</p> <p><u>Members Absent:</u> Chris Lake, NV Hospital Association</p> <p><u>Guests in Attendance:</u> Catherine Krause, AGO Laura Tucker, AGO Greg Zunino, AGO Esmeralda Velazquez, AGO</p>
---	---

- Swearing in of new members.**
 AG Laxalt swore in Alan Cunningham, Christopher Darcy, Greg Herrera, and Sandra Jauregui.
- Call to Order and Roll Call.**
 Meeting called to order at 10:00 a.m. Roll call was taken by Marsha Landreth and a quorum was present.

3. **Public Comment. Discussion only.**

No public comment.

4. **Welcome and self-introduction of Technological Crime Advisory Board members.**

AG Laxalt welcomed everyone to the meeting, and members introduced themselves.

5. **Approval of minutes of November 27, 2017 meeting.** (*Attachment One (1) - Minutes from November 27, 2017 Meeting*). **Discussion and for possible action.**

AG Laxalt asked for approval of the November 27, 2017 meeting minutes. Alan Cunningham moved to approve the minutes. Greg Herrera seconded the motion, and the motion passed unanimously.

6. **Presentation on PSAs. Discussion and for possible action.** Monica Moazez, Communications Director; Laura Tucker, Deputy Attorney General; and Catherine Krause, IT Chief, AGO.

Monica Moazez reported on creating video presentations focused on cybersecurity and technology crime issues. Moazez stated that funding was available and the budget is \$10,000.00. A local public relations (PR) company, Brain Trust, have agreed to produce the videos. There will be three to four videos, each two-to-two and a-half-minutes-long. Moazez stated that they have reached out to several advisory board members to participate in making the videos. She will follow-up with them after this meeting. The focus of the videos will be on creating strong passwords, counterfeiting, skimmers and how they work; and on phishing.

Once the videos are produced, board members and participants can promote them to different organizations or schools. The videos will also be put on the AGO website and promoted through social media platforms, and sent to a list of local Nevada businesses. The idea is for some of the videos to be straightforward and some of them to be more of a documentary-style with focus on questions and answers. She plans to shoot the videos at one time, at one location, with the same individuals.

AG Laxalt asked for script input from the members for the next meeting. Assemblywoman Sandra Jauregui asked whether contact had been made with real victims, who would testify in some of the videos. Moazez expressed concern with obtaining cooperation of victims based on her past experience; Jauregui believes, however, that she may have some victims willing to participate.

Senator Moises Denis asked about shorter versions of the videos. His experience is that many media outlets will not run any public service announcement (PSA) longer than 30 seconds. Moazez explained that we were trying to keep the videos as short as possible and plans to cap them at two minutes. Denis has contacts at Nevada Broadcaster's Association who might be able to edit the videos at little or no cost. Cunningham suggested building the scripts in 30-second segments, so that the videos could be sent to TV stations and 30-second sections/excerpts could be easily broken out without additional costs. Moazez will look into it. We will submit scripts to the PR agency and learn what the productions will be. AG Laxalt asked that Moazez send a list to the group on the four topics, we intend to cover, so

that members can offer input on scripts or victims willing to participate. Scripts will be approved at the next meeting.

7. **Board proposed brochure on skimmers.** Laura Tucker, Deputy Attorney General and Monica Moazez, Communications Director, AGO. (*Attachment Two (2) – Skimmers Brochure*).

The information in the draft brochure was taken from a number of law enforcement sources, and the pictures are from the Henderson Police Department. This is a draft and comments are welcome. AG Laxalt commented that the pictures could use captions; Chris Darcy and Jacob Cinco both volunteered to match the photos and provide descriptions and incident response information.

Cunningham suggested that the blank space above the *Contact Us* section could be used to provide some short links. AG Laxalt asked who would be the appropriate contacts to have persons call to make a report regarding an incident. Darcy asked what our audience is for the brochure. Tucker stated that we intend to provide them at events and in our office lobbies. Darcy offered to place them in police stations in front lobbies. Moazez stated we would also make them downloadable on our website and offer them to banks, gas stations and other point-of-sale locations. Darcy asked whether they would be made available to business and licensing. Moazez stated that we will contact the Secretary of State's office and see if they are interested in carrying the brochure.

Andrew Campbell suggested a 3-point bullet of what to do for vendors, to check their credit report and list a few pointers, not just who to contact. AG Laxalt suggested taking our office contact information off the brochure so the brochure will contain a whole block for federal and/or local contact information. Cinco said that as far as Secret Service is concerned, he does not know what the FBI's policy is, but his agency does suggest contacting local law enforcement first. The standard procedure on skimmers is LVMPD's Financial Crimes Unit or local law enforcement to respond to a gas station or bank and get DNA and look for cameras. Darcy stated they conduct an initial investigation and depending on the level of magnitude and organization, sometimes they go with a federal scenario, and work with a federal prosecutor. They all work together, so they choose the best avenue to use for prosecution. Greg Herrera stated that in Washoe County they have the same setup in the north and handle things in the same fashion. AG Laxalt asked what percentage of gas station skimmers are one-off actors versus some larger multi-national criminal syndicate. Herrera stated they find with the gas station skimmers that there is a trail where they can typically track actors through northern California. They have been successful in prosecution because they have been able to get a couple of steps ahead of the perpetrators. They then identify them as they move along I-80 in northern Nevada on to Elko County. Usually the perpetrators are a unit – one family – not connected to a larger unit.

Robert Kopacz stated that when you look at the transfer (the buying of these devices), you can buy them on the dark web for a couple hundred dollars and then hand the information off to a larger group, but the larger group is not the people actually putting the skimmers in place. Darcy said it is a multi-level issue, and they are starting to see more and more organization in the enterprises in how they put these things together. Whether it is funding

gang or terrorism groups it is a big money maker for these groups. There are a lot of people involved, making it difficult to connect the dots, but they are connected. It is not one person setting up one skimmer in one place and keeping the money to themselves; it is usually part of a larger operation.

Cunningham said there are guys that put devices on the machines, guys that download the data, and guys that remake the cards and re-encode them onto pre-paid credit cards. So, there are multiple layers of actors. They can include Romanians, Cubans, and cross state lines. AG Laxalt asked if the law enforcement specialists can help us determine who the proper agencies and websites are to point businesses and victims to for information. The consensus was to proceed on the brochure and members were asked to submit their edits.

8. Meetings set for 2018 at 10 a.m. in the Attorney General's offices:

- May 10, 2018.
- August 15, 2018.
- November 14, 2018.

AG Laxalt requested that if anyone has any new topics to address at future meetings, please forward the information or topics to Patty Cafferata for coordination and addition to the agenda.

9. Public Comment. Discussion only.

No public comment.

10. Adjournment.

AG Laxalt moved to adjourn and Herrera seconded, and the motion passed unanimously. The meeting adjourned at approximately 10:45 a.m.

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

Attachment Two (2)

to

Technological Crime Advisory Board Agenda

May 10, 2018

Video Scripts

PHISHING—Laura Tucker (AGO BCP)

Every day, there are people trying to find their way into your accounts—PHISHING for your personal information.

These criminals don't even have to try hard to get this information. All they have to do is ask YOU.

Phishing occurs when a fraudster pretends to be a legitimate business and attempts to contact you by email, phone or text message.

They ask you to provide personal and financial information: like your credit card number, account login information, and even your social security number.

You might think keeping this information to yourself is easy. But fraudsters make it difficult to know you're being scammed.


[On-Screen Graphic]

It is estimated that 156 MILLION PHISHING EMAILS are sent out every day

8 MILLION of these emails are opened

On average, 80 THOUSAND people fall victim to a scam every day and share their personal information

Avoid falling victim to phishing scams by:

- Creating strong passwords, and never using your banking or account password for other websites or logins.
- Making sure you always communicate your personal information through a secure website.
 - Secure websites should have a secure icon 
- Double checking that the web address is the same as the site you want to visit.
- Avoid clicking on links you receive by email—visit the source instead or pick up the phone.
- Always using the phone number or website address on the back of your credit or debit card to contact your bank.

Forward phishing emails to the organization impersonating the email and to spam@uce.gov (on-screen)

And file a report with the Federal Trade Commission at [FTC.gov/complaint](https://www.ftc.gov/complaint) (on-screen)

[Last Screen]

PHISHING—Don't Get Hooked

This message is brought to you by the Nevada Attorney General's Technological Crimes Board
(AG Seal)

PASSWORDS & WIFI—Alan Cunningham (Washoe County School District)

Sometimes there's only one thing standing between your personal information and fraudsters: YOUR PASSWORD.

And you're probably using your password every day to log in to your computer, go onto your emails, check your bank account and access your private files.

If fraudsters guess your password, they will have all of this personal information at their fingertips.

And what's worse—they're very good at guessing passwords, and can even use software that allows them to input millions of guesses until one of them is right.

Your job as a consumer is to make your password very hard to guess.

[On-Screen] Remember, Your Username + Your Password = I AM YOU

Your password should not include information about YOU that is easily accessible to fraudsters—like your birthday, phone number, family members or pets.

Instead, try creating a passphrase from a news headline, title of a book or even a song. Something that is memorable ONLY to you.

Let's try turning a nursery rhyme that's easy to remember and tough to guess into a personal password.

[On-screen] For example: **Birds of a Feather Flock Together**

Take the first letter of each word:

[On-screen] boafft

You should add uppercase letters, numbers and special characters to make your password even stronger like:



[On-screen] BoaFft3!

Be aware that only YOU should know your password. Writing it on a sticky note or sharing it with others is risky. If you're having trouble remembering your password, there are password manager mobile apps you can use to safely store multiple passwords.

Be cautious while entering a username, password or other sensitive information on a public computer or public Wi-Fi.

Setting up a wireless network or mobile hotspot is easy, and if you use a fraudster's network, they can watch and record anything you send through it. Remember, just because it's accessible doesn't mean it's safe.

[On-Screen] Keep Your Information Safe By:

- Avoiding transactions on public Wi-Fi
- Only using websites with an https and a  symbol
- Making sure the  symbol stays there as you use the site

- Never giving out your personal information by phone, email or mail

If you believe someone has stolen your identity, contact your local police department to file a report and obtain more information.

[Last Screen]

Your Username + Your Password = I AM YOU

This message is brought to you by the Nevada Attorney General's Technological Crimes Board

(AG Seal)

GAS PUMP SKIMMING—Jefferson Grace (LVMPD Detective)

What if I told you there's a device that can collect your money and your identity with one swipe?

And what if I shared that in 2017, the Las Vegas Metropolitan Police Department recovered 195 of these devices in the Las Vegas valley.

[On-Screen] IT'S CALLED SKIMMING

AND IT CAN VICTIMIZE ANYONE

Q: What is skimming?

A: Skimming is a type of fraud that can happen when a skimmer device is used to copy payment card numbers and PINs.

Q: Where can you get skimmed?

A: Skimmers can be installed by fraudsters at gas pumps and ATMs. These devices are placed over card readers or internally at gas pumps and ATMs to steal your information.

Q: How can you spot a skimmer?

A: When paying at a gas pump with a credit or debit card, look at the security sticker and lock that's placed on the pump. If the tape has been damaged or the lock has been broken, try using a different pump.

How can you avoid falling victim to skimming?

- **[On-Screen]** *Tug the card slot.*

(Audio) Skimmers are often installed using double-sided tape for easy installation & removal.

- **[On-Screen]** *Cover the pin pad while using a gas pump or ATM to avoid any hidden cameras.*

- **[On-Screen]** *Avoid standalone cash machines.*

(Audio) These are usually easier for fraudsters to target. Instead, use ATMS that are physically installed in a bank.

- **[On-Screen]** *Use a credit card rather than a debit card whenever possible.*

(Audio) Credit cards are not linked to physical funds and offer more protections against fraud.

- **[On-Screen]** *Monitor your accounts to spot unauthorized purchases.*

If you find a skimming device, report it to the store manager or to local law enforcement.

[Last Screen]

CARD SKIMMING: Stay Safe at the Pump

This message is brought to you by the Nevada Attorney General's Technological Crimes Board

(AG Seal)

CURRENCY COUNTERFEITING—Jacob Cinco

If you're doing business with cash flow, at some point you'll encounter counterfeit or imitation bills. Especially because of recent advancements in digital imaging and printing.

Q: How much currency is being counterfeited every year?

A: In 2017, over \$143 million in counterfeit US currency was passed and seized. The bill that we're seeing counterfeited the most is the \$20 bill.

Q: Are you seeing any trends in currency counterfeiting?

A: In the last 20 years, the US Secret Service has seen an increased number in currency counterfeiters because of advancements to technology. Using digital imaging and printing technology, counterfeiters can easily produce a small amount of passable counterfeit bills.

It's hard to tell what's real from what's not. The best way to detect counterfeit bills is to

[On-Screen] Know What Real Money Looks Like:

- **[On-Screen]** *Real US bills have a slight texture you can feel from the printing process.*
(DEMO—feel the texture of the bill)
 - **[On-Screen]** *Bills of \$10, \$20, \$50 and \$100 have color-shifting ink.*
(DEMO--the lower-right number showing the bill's amount should change from copper to green when tilted)
- **[On-Screen]** *There should be a security thread on each bill greater than \$1 that's only visible when held under UV light.*
(DEMO—each of these threads are on a different place depending on the type of bill, and glow different colors under UV light)
- **[On-Screen]** *The first letter of the serial number on US bills of a series year 1996 or later corresponds to the series year.*
(DEMO—illustrate this by circling this correspondence on two sample bills)

Q: If you think you've received a counterfeited bill, what should you do?

[On-Screen] If you encounter a counterfeit bill:

- Do not put yourself in danger.
- Do not return the bill to the passer.
- Observe the passer's description and their companions' descriptions, and write down their vehicle license plate numbers if you can.

- Write your initials and date in the white border area of the suspected counterfeit note.
 - DO NOT handle the counterfeit note. Place it inside an envelope or plastic bag.
- Contact your local police department or call your local U.S. Secret Service Office to report the suspected counterfeit bill.
- Surrender the note or coin ONLY to a properly identified police officer or a Secret Service Special Agent, or mail it to your nearest U.S. Secret Service field office.

[Last Screen]

Know Your Money: KEEP YOUR MONEY

For more information on currency security features, visit UScurrency.gov or SecretService.gov

This message is brought to you by the Nevada Attorney General's Technological Crimes Board
(AG Seal)

Attachment Three (3)

to

Technological Crime Advisory Board Agenda

May 10, 2018

Skimmers Brochure

Skimmers and Identity Theft

A skimmer is a device used to copy payment card numbers and personal identification numbers (PINs), by capturing both the magnetic strip data and the PIN entered. Skimmers are installed at merchant locations, point-of-sale (POS) devices, automated teller machines (ATMs), and stand-alone kiosks.

Insert skimmers are installed inside of the card reader and are more difficult to identify. Some are used to copy the chip, and others block the chip, forcing the inserted card to read the magnetic strip.

Thieves may steal credit and debit card information for multiple reasons. Generally, a person's information is resold online or used for withdrawals from ATMs. The people stealing this information may be local criminals, international organized crime syndicates, or terrorist groups.

Skimmers are difficult to spot, even for trained law enforcement officers. Devices vary in shape, size, and design, and may be paired with small cameras designed to capture personal identification numbers (PINs). Skimmers tend to be unobtrusive and may look legitimate.

Contacts

Please do NOT remove the device if it is still in place, and if it has already been removed, do NOT handle. Initial notification involving fraud to a cardholder's account should be made to the cardholder's bank.

Clark County

Please contact the Las Vegas Metropolitan Police Department non-emergency number at 311 or (702) 828-3111.

Washoe County

Please contact the Washoe County Sheriff's Office non-emergency number at (775) 785-9276.

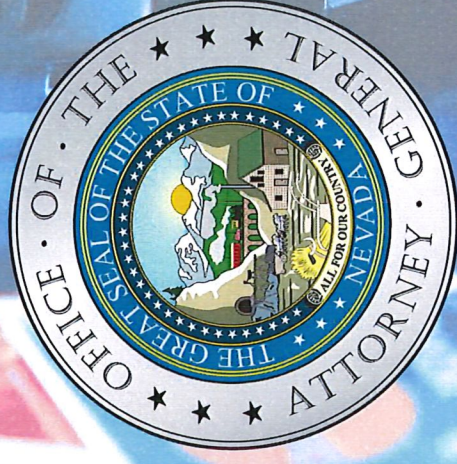
Other Nevada Counties

If you are in another jurisdiction, contact your local non-emergency number for your sheriff or police department.

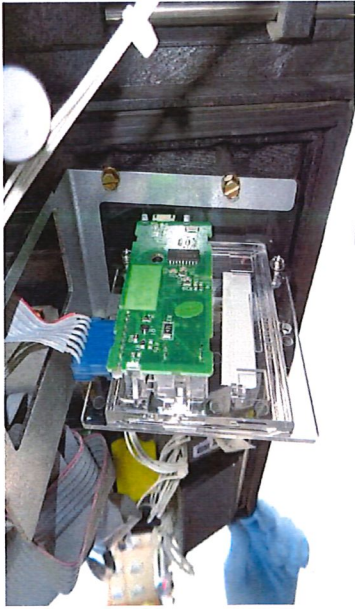
CREDIT CARD

SKIMMING:

Stay Safe at the Pump



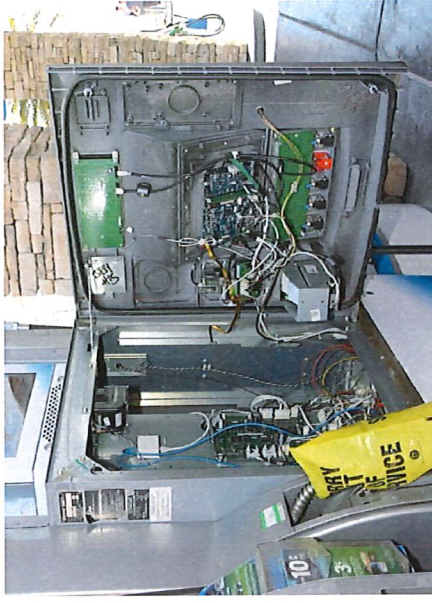
Office of the Nevada
Attorney General



A skimmer installed inside an ATM. Photo courtesy of the Henderson Police Department.

ATM Skimmers

- * Keep your wits about you when you're at an ATM. Avoid standalone cash machines, as these are usually easier for thieves to target. Instead, try to use ATMs that are physically installed in a bank.
- * Tug the area of the card slot. Many overlays use double-sided tape for quick installation and removal.
- * Examine above and around the PIN pad for a small pinhole camera. Cameras used for capturing PINs will blend into the ATM and look like a part of the machine. They usually are installed with double-sided tape in hard to see areas.
- * Be on the alert for individuals who appear to be tampering with the terminal, using the ATM repeatedly with different cards, showing up multiple times at the machine over a short period, or those who are using the ATM and intentionally covering their faces with sunglasses, scarves, or hats.



A skimmer behind a gas station pump. Photo courtesy of U.S. Secret Service Las Vegas Field Office.

Gas Pump Skimmers

- ⇒ The most common type of gas pump skimmer is located inside the pump and is not readily visible.
- ⇒ Inspect that the security label is not broken on the pump. If it is torn, this is a sign of tampering. Use another pump.
- ⇒ Look for excessive or out-of-the-ordinary electrical tape.
- ⇒ The gas pumps that are farthest away from the store and out of view of security cameras are most commonly targeted.
- ⇒ Tug on the area of the card slot. Many overlays use double-sided tape for quick installation or removal.
- ⇒ Pay attention to individuals who look to be tampering with parts of the gas pump, or who are at the gas pump for long periods of time.



Not all security tape is the same, and colors vary. However, the general principle is the same. This is an unsecured security label. Note the word "void" across the face of the tape. Photo courtesy of Las

Vegas Metropolitan Police Department.

More Tips

- If you locate a skimming device, do not remove it; contact the store manager and law enforcement instead.
- ◇ Cover the PIN pad while you enter your PIN. This will help block the view of a camera that may have been installed around the pad.
- ◇ Consider using a credit card rather than a debit card. Credit cards offer more protections than debit cards and are not linked to physical funds.
- ◇ Be especially vigilant when withdrawing money on weekends, as thieves tend to strike when they know the bank won't be open again for more than 24 hours.
- ◇ Keep a close eye on your bank statements, and dispute any unauthorized charges immediately.