



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: May 4, 2016, 10:00 a.m.

Place of Meeting: Video Conferenced Between:

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

Sawyer Building, Room 4500
 555 E. Washington Avenue
 Las Vegas, Nevada

Attendees:

Las Vegas:	Carson City:
<p><u>Members in Attendance:</u> Edgar Flores Greg Weber Todd Peters (Sitting Proxy for Patrick Moers) Jim Owens</p> <p><u>Members Absent:</u> Mark Lipparelli Brian Spellacy</p> <p><u>Guests in Attendance:</u> Rod Swanson Jonathan Cooper</p>	<p><u>Members in Attendance:</u> Adam Laxalt Patricia Cafferata Jim Earl (Sitting Proxy for Shannon Rahmig) Lea Tauchen (Sitting Proxy for "Tray" Abney) (Eric) Andrew Campbell</p> <p><u>Members Absent:</u> Frank Schumann Kyle Burns</p> <p><u>Guests in Attendance:</u> Laura Tucker Catherine Krause Ernest Figueroa</p>

- 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.
- 3. 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.

4. **Discussion for possible action to approve minutes of March 31, 2016 meeting.**
Laxalt asked for approval of the March 31, 2016 meeting minutes with corrections to Jim Owens and Greg Weber's names. Greg Weber moved to approve the minutes as amended. Jim Earl seconded the motion. All in favor, and an approval of meeting minutes motion passed.
5. **Report of Executive Director Patricia Cafferata.**
 - a. **Governor appointed Eric Campbell from the Churchill County School District to the board.**
Executive Director Patricia Cafferata reported (Eric) Andrew Campbell was appointed to the board.
6. **Discussion and election of new chair and vice chair for one year term beginning on July 1, 2016. In the past, the Board elected the Attorney General as the chair and one of the legislators as the vice chair.**
Laxalt requested a motion to elect a chair and vice chair for the committee beginning July 1, 2016. Jim Owens moved that Attorney General Adam Laxalt be elected chair and Assemblyman Edgar Flores be elected the vice chair. Jim Earl seconded the motion. The motion passed unanimously.
7. **Presentation and discussion for possible action on outreach programs, in particular to the Latino community. Assemblyman Edgar Flores.**
Flores spoke about outreach programs to inform the Latino community of legal issues. He reported most Latinos go to notary public for legal advice, or use word of mouth. Flores suggested utilizing churches, law enforcement, radio, TV, internet and various other people and programs to get information to the Latino community. He and Laxalt discussed the possibility of bringing Latino community members to the next meeting.
8. **Presentation on the prosecution of technological crimes. Clark County Deputy District Attorney Jonathan Cooper.**
Jonathan Cooper of the Clark County District Attorney's Office gave a PowerPoint presentation on using evidence for criminal prosecution. This presentation included how to use and get internet IP addresses, cell phones, metadata, emails, Facebook and Twitter posts, and deleted computer files. Search warrants may be needed to get cell phone data.
9. **Presentation and discussion for possible action on one of the committee's legislative duties, per NRS 205A.060.3. (Attachment Two (2) - NRS 205A).**
 - a. **Presentation on Modern Trends in Identity Theft and Consumer Education. Deputy Attorney General Laura Tucker.**
Deputy Attorney General Laura Tucker gave a presentation about identity theft. She reported there were 781 incidents of data breaches in the U.S. in 2015. Most information stolen is social security numbers and debit and credit card information. Verizon produces a data breach report that has good information and tips of how to protect yourself. There was also discussion on a 2005 law that requires consumers to be notified of data breaches by businesses. NRS 603A.220(4). Laxalt and Flores will

work together to change the language in the statute for businesses to better inform consumers. It was also agreed to add ID theft to the community outreach programs. (See Attachment One (1), Report by Laura M. Tucker, Modern Trends in Identity Theft, and Consumer Education and Legislation.)

10. Presentation and recommendations by former Privacy Subcommittee member. Lecturer, Information Systems. UNR James Elste.

James Elste could not attend and the topic will be discussed at a later date.

11. Discussion and possible action on proposed legislation:

- a. To increase penalties for commission of technological crimes, redefine the meaning of “intent” and**
- b. Other related legislation on technological crimes for the 2017 Legislative Session.**

Discussion conducted about broadening and/or redefining the meaning of “intent” with regards to credit card skimmer cases. Flores will look into the legislative reason for making the credit card skimmer law so broad. He will carry a bill to make the change to the law. NRS 603A.

12. Discussion and possible action on applying for grants for education and prevention of ID theft. Management Analyst for Grants Liz Greb.

This topic will be in the next agenda.

13. Discussion for possible action setting quarterly meetings on July 14, 2016 and November 9, 2016.

Future meetings were set for July 14, 2016, and November 9, 2016.

14. 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.

15. Adjournment.

Jim Earl moved to adjourn the meeting; Andrew Campbell and Greg Weber both seconded the motion. Approved unanimously, the meeting adjourned at about 11:25 a.m.

Minutes respectfully submitted by Lacey J. Austin.

In accordance with NRS 241.020, this agenda was posted on or before April 29, 2016 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 One (1)

to

Technological Crime Advisory Board Minutes

May 4, 2016

Contents: Modern Trends in Identity Theft, and
Consumer Education and Legislation; a report by

Laura M. Tucker, Deputy Attorney General

Modern Trends in Identity Theft, and Consumer Education and Legislation
Prepared by Laura M. Tucker, Deputy Attorney General, and Lucas J. Tucker,
Senior Deputy Attorney General

- I. How Identity Theft Occurs
 - a. Trend – Data Breaches
 - i. A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.
 - ii. According to the Identity Theft Resource Center, the number of U.S. data breaches tracked in 2015 was 781. 40 percent of these occurred in the business sector, 35.5 in the health/medical sector; 9.1 percent in the banking/financial sector; 8.1 percent in government/military, and 7.4 percent in education.
 - iii. Hacking incidents accounted for almost 40 percent of these breaches, with employee error/negligence at about 15 percent.
 - iv. In 2015, only 12.4 percent were “paper” breaches
 - v. Most of the information obtained included SSNs and debit/credit card information.
 - b. In 2014, the average cost for companies that suffered a data breach was \$3.79 million, according to the Ponemon Institute.
- II. Consumer Education
 - a. CHIP and PIN cards
 - i. Chip cards are more effective because the technology encrypts the data for each individual transaction. Therefore, if the information is intercepted, the information is valid only for the one-time use. It is less vulnerable during transmission.
 - ii. Inform consumers how to use them and encourage their use whenever possible.
 - iii. However, also let consumers know that for transactions online, the chip technology will not apply. Therefore, follow good online safety practices
 - 1. i.e., only submitting information to trusted websites and checking for a secured site (https and lock)
 - b. Credit Card versus Debit Card use
 - i. Credit cards are generally better protected in the event of a fraudulent transaction than debit cards.
 - 1. First and foremost, a credit card is not tied to a bank account. Therefore, there is no immediate financial hit if your number is stolen. Debit cards, conversely, are backed by money.
 - 2. If your credit card number is stolen, you are not responsible for unauthorized purchases under federal law. No more than \$50 if the actual card is stolen.
 - 3. Debit cards – banks have discretion to determine if a theft was promptly reported (within 60 days) to decide if they will hold you not accountable for the transactions.
 - c. Identity Protection Services
 - i. There are commercial identity protection services that monitor use of personal information, and can help consumers minimize the risk of fraudulent activity, or alert them about fraud very quickly. However, consumers should know that

none of these companies can “guarantee” absolute security of personal information. LifeLock has paid 2 fines to the FTC and various states for misleading statements it made to consumers.

- ii. Even though there are no guarantees, consumers should take advantage of any complimentary identity protection services that a company may offer when it discovers a data breach. Many companies offer their customers 1 year of complimentary services, and due to the increased frequency of data breaches, consumers can get several years of overlapping or continuous free services.

III. New Legislation

a. Nevada’s notice requirement

- i. When a consumer’s personal information is exposed due to a data breach suffered by a business, the business generally has two options to inform the consumer; direct notification, or substitute notice. In the case of payment card data breaches, many companies avail themselves of the option to provide substitute notice. They choose this option because many companies don’t store the payment card data, so they are unable to specifically identify individuals who are impacted by the breach.
- ii. Substitute notice: NRS 603A.220(4) requires (i) notice by electronic mail when the business has email addresses for the customers involved; (ii) conspicuous posting of the notification on the business’ internet website, if it maintains a website, and (iii) notification to major statewide media.

b. Drawbacks to current statute (enacted in 2005)

- i. Some businesses don’t have emails; others have the emails, but avoid sending them on the basis that they are unable to specifically identify which consumers are impacted.
- ii. Conspicuous notice - there is some ambiguity regarding what constitutes “conspicuous notice”, and many companies post the notice in a manner that could easily be missed by many consumers.
- iii. Notifying statewide media - the fact that a business notifies statewide media doesn’t necessarily mean that the media will prominently alert consumers. Even in cases where the media runs a story featuring the breach, there has been a shift from print media to online media. The life cycle of many online stories is now 24 hours or less, so consumers who do not encounter a press release within hours of its release are less likely to encounter it later the same day, much less the following day, week or month.

c. Improving Nevada’s notice law

- i. Social media has grown exponentially since the statute was enacted in 2005. Many businesses use social media in a way that they use traditional websites, to advertise and draw customers. Social media could be an effective way for businesses to let their customers know there has been a data breach.
 - 1. Slight amendment to the 2nd element of substitute notice, to provide “conspicuous posting of the notification on all websites and social media sites maintained by, or for the benefit of, the data collector.”
- ii. Second, businesses could be required to post a conspicuous notice at the payment card terminal(s) in their physical location for some minimum time period, such as 30 days. Businesses would likely take data security more seriously if they know there will be heightened awareness if they suffer a data breach.

- iii. Third, businesses could be required to notify all customers for whom they have email addresses, even if they can't verify whether any specific individual was impacted by the data breach. Many companies already do this, but some companies use the current requirement as a shield to avoid providing email notice.
 - 1. The first element of substitute notice could be slightly revised to provide "notification by electronic mail to all persons the data collector has electronic mail addresses for."
- d. While we could also consider requiring that businesses notify the AG's office, that would only help consumers if the AG established a place on its website where copies of the notices would be posted. This would require some resources, and it's hard to predict the effort that would be required. For reference, on the California AG's website, 270 notices were posted during the 15 months from January 1, 2015 to March 31, 2016. Businesses have a direct relationship with their consumers, so enhancing the notification efforts required by businesses might be the most effective approach to increase awareness of these data breaches.