



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

AGENDA

July 26, 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

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, Esq., 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 members.**
Adam Laxalt, Nevada Attorney General.
4. **Swearing in of new members.** Adam Laxalt, Nevada Attorney General.
5. **Approval of minutes of April 5, 2017 meeting.** (*Attachment One (1), Minutes from April 5, 2017 Meeting.*). **Discussion and for possible action.**
6. **FBI Presentation on the Dark Web. Discussion only.** Supervisory Special Agent Adam Pranter.
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.**

8. **Presentation on the EMV and PCI Security Standards for possible inclusion in the outreach plan. Discussion and for possible action.** Greg Weber. (*Attachment Two (2), PCI SSC Quick Reference Guide*).
9. **Presentation of Henderson Police Department’s brochure on locating skimmers. Discussion only.** Sergeant Troy Herring, Henderson Police Department. (*Attachment Three (3), photos of skimmers and “Protect Yourself from ATM and Gas Pump Skimming” brochure*.)
10. **Presentation on agenda topics and participants in the outreach plan to small business and local communities. Discussion and for possible action.** Laura Tucker. (*Attachment Four (4), NRS 603A Compliance Checklist, and Attachment Five (5), PowerPoint - Cybersecurity for Individuals and Small Businesses in Nevada*.)
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
12. **Accepting the \$1,344.69 forfeiture funds into the Attorney General’s general operating budget to promote National Cybersecurity Month in October. Discussion and for possible action.**
13. **Next meeting is set for November 16, 2017 at 10 a.m. in Attorney General’s offices.**
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.
15. **Adjournment.**

In accordance with NRS 241.020, this agenda was posted on or before July 21, 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
- Nevada State Capitol Building, 101 N. Carson Street, Carson City, NV 89701
- Nevada State Library, 100 N. Stewart Street, Carson City, NV 89701

Meeting materials may be requested from Patricia D. Cafferata, Esq., 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 1
Meeting Minutes 4/5/17



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: April 5, 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:
<p><u>Members in Attendance:</u> Adam Laxalt, Chair Patricia Cafferata, Executive Director Jacob Cinco Mathew McCarthy Edward Wallace (with proxy for Patrick Moers) Greg Weber</p> <p><u>Guests in Attendance:</u> Rod Swanson Monica Moazez Jim Lewis Judy Reich Eric Bonnici</p>	<p><u>Members in Attendance:</u> (Eric) Andrew Campbell Edward Grassia Greg Herrera (with proxy for Jerry Baldrige)</p> <p><u>Guests in Attendance:</u> Catherine Krause Laura Tucker</p> <p><u>Members Absent:</u> Senator Moises Denis Assemblyman Edgar Flores</p>

- 1. Call to order and Roll Call.**
 Meeting called to order at 10:04 a.m., Patricia Cafferata called roll and confirmed there was a quorum present.
- 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, Senator Moises Denis, (Eric) Andrew Campbell, Jacob Cinco, and Matthew McCarthy.

Laxalt swore in (Eric) Andrew Campbell, Jacob Cinco, and Matthew McCarthy, Senator Moises Denis was not present.

5. Discussion for possible action to approve minutes of January 11, 2017 meeting.

Laxalt asked for approval of the January 11, 2017 meeting minutes. Mathew McCarthy moved to approve the minutes. Patrick Moers seconded the motion, and the motion passed unanimously.

6. Report on the survey of the Technological Crime Advisory Board committee members on various issues.

Patricia Cafferata reported results of the survey in terms of outreach to the Hispanic and small business community. One of the goals is to kick off the outreach program in October, Cyber Security Month. The survey asked members how they could participate, what they could contribute, what forms of outreach seemed best, and what legislative suggestions could be made.

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

Out of eight (8) responses, most were willing to participate in Chamber of Commerce briefings and Cybersecurity Clinics. Laxalt asked for a show of hands who would be a part of an on-the-road outreach program. This training and the agendas are to include what types of crimes being seen, how to better spot those crimes, and what can be done to prevent the crimes. He thought the likely training would be through the Chambers of Commerce. He is looking to hold a handful of trainings in Las Vegas and Reno, and in a couple rural areas. At the next meeting, a clearer agenda for a program will be proposed, and specific contributions will be noted.

8. Possible Report on outreach to broadcasting entities and the development of a Public Service Announcement (PSA) for the Board.

Senator Moises Denis was not in attendance, the item was moved to the next agenda.

9. Presentation on the PSA Process.

Judy Reich and Eric Bonnici from the Nevada Broadcasters Association introduced themselves and gave their presentation. The Nevada Broadcasters Association represents all of the television and radio stations in Nevada, and is the liaison between the FCC and the broadcasting companies. The Public Education Partnership is an FCC sanctioned program setting up NCSAs (non-commercial sustaining announcements), which can be broadcast widely to television and radio stations for a longer time period and on a larger platform, than a PSA which needs to be solicited to each individual platform. Affidavits would be received from every station, to prove who and when our information is being broadcast. The Nevada

Broadcasters Association effectively assisted the Attorney General's Office for Human Trafficking Awareness month in January 2017. Laxalt noted that the board's budget would be looked over to determine how much money the board would have to create a proposal for a NCSA. Bonnici mentioned that their company could obtain matching grants. The lead-time needed to produce a NCSA is about a month. Laxalt wanted to move this item to the agenda for the next meeting to bring a clearer idea of what the budget is, and obtain quotes from the company. Reich and Bonnici were excused from the rest of the meeting.

10. Presentation regarding information on ways to communicate without digital technology.

Andrew Campbell was unable to present his paperwork in time to be submitted for review prior to the meeting. Laxalt allowed Campbell to speak on his proposal. Campbell spoke about training received at the Washington State School for the Deaf. His concerns lay with the consideration of communicating without digital means in the event of catastrophic loss, and the trend of reduction of hard copies of texts. Laxalt noted he is happy to speak about this outside of the meeting, but the board has previously strayed from technological crime topics, and he does not want to have that happen again.

11. Report on forfeiture funds received.

Cafferata reported a check was received from LVMPD of forfeiture funds from a guilty plea. The check was for \$1,344.69.

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

Laxalt would like the money to help with the October kick-start of Cybersecurity Awareness Month.

13. Report from the Attorney General's Fraud Unit on skimmer device legislation in other states.

Daniel Westmeyer was not in attendance, but his memo as Attachment Four (4) detailed other states' legislation. Cafferata explained how the word "skimmer" was lacking clear definition an earlier proposal to the board, so it was rejected as too broad. If any members would like Westmeyer to be at the July meeting for a questions and answers, please let Cafferata know.

Back to Agenda item 6. Laxalt asked if anyone else had comments or things to add to the July meeting agenda. Ed Wallace informed the board that brochures have been created by the Henderson Police Department to be placed in local business (starting with gas stations, and moving to other susceptible businesses). The department found that business employees are not being taught by employers on how to identify a skimmer and how to report it. Laxalt questioned whether skimmers and the education regarding skimmers should be part of the presentations to be set up for the next year. Greg Weber considers them part of emerging technology, so yes. All attendees agreed. Weber would like to see employees of small businesses trained on what skimmers are, and how to identify when a machine has been tampered with. Cafferata noted in a previous board meeting, the members discussed that gas pump skimming devices were one of the most frequently used devices to commit ID theft crimes in Clark County.

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

Jacob Cinco suggested that at the next meeting the board may want to discuss online technological crimes for businesses that sell items online.

15. Public Comment. Discussion only.

None.

16. Adjournment.

Laxalt called for a motion to adjourn the meeting. McCarthy moved to adjourn, Wallace seconded, and the motion passed unanimously. The meeting adjourned at approximately 11:04 a.m.

Minutes respectfully submitted by Allison E. Johnson, Office of the Attorney General.

DRAFT

ATTACHMENT 2
PCI DSS QUICK REFERENCE GUIDE

Copyright 2010 PCI Security Standards Council, LLC. All Rights Reserved.

This Quick Reference Guide to the PCI Data Security Standard is provided by the PCI Security Standards Council to inform and educate merchants and other entities that process, store or transmit cardholder data. For more information about the PCI SSC and the standards we manage, please visit www.pcisecuritystandards.org.

The intent of this document is to provide supplemental information, which does not replace or supersede PCI Security Standards Council standards or their supporting documents. Full details can be found on our Web site.

October 2010

Contents

Introduction: Protecting Cardholder Data with PCI Security Standards	4
Overview of PCI Requirements.....	6
The PCI Data Security Standard	8
PIN Transaction Security Requirements	10
Payment Application Data Security Standard	10
Security Controls and Processes for PCI DSS Requirements	11
Build and Maintain a Secure Network	12
Protect Cardholder Data	14
Maintain a Vulnerability Management Program	16
Implement Strong Access Control Measures.....	18
Regularly Monitor and Test Networks	20
Maintain an Information Security Policy	23
Compensating Controls for PCI DSS Requirements	24
How to Comply with PCI DSS	25
Choosing a Qualified Security Assessor	26
Choosing an Approved Scanning Vendor.....	27
Scope of Assessment for Compliance.....	28
Using the Self-Assessment Questionnaire (SAQ).....	30
Reporting.....	31
Web Resources	32
About the PCI Security Standards Council	33

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

Introduction: Protecting Cardholder Data with PCI Security Standards

The twentieth century U.S. criminal Willie Sutton was said to rob banks because “that’s where the money is.” The same motivation in our digital age makes merchants the new target for financial fraud. Occasionally lax security by some merchants enables criminals to easily steal and use personal consumer financial information from payment card transactions and processing systems.

It’s a serious problem – more than 510 million records with sensitive information have been breached since January 2005, according to PrivacyRights.org. As a merchant, you are at the center of payment card transactions so it is imperative that you use standard security procedures and technologies to thwart theft of cardholder data.

Merchant-based vulnerabilities may appear almost anywhere in the card-processing ecosystem including point-of-sale devices; personal computers or servers; wireless hotspots or Web shopping applications; in paper-based storage systems; and unsecured transmission of cardholder data to service providers. Vulnerabilities may even extend to systems operated by service providers and acquirers, which are the financial institutions that initiate and maintain the relationships with merchants that accept payment cards (see diagram on page 5).

Compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) helps to alleviate these vulnerabilities and protect cardholder data.

RISKY BEHAVIOR

A survey of businesses in the U.S. and Europe reveals activities that may put cardholder data at risk.

81% store payment card numbers

73% store payment card expiration dates

71% store payment card verification codes

57% store customer data from the payment card magnetic stripe

16% store other personal data

Source: Forrester Consulting: The State of PCI Compliance (commissioned by RSA/EMC)

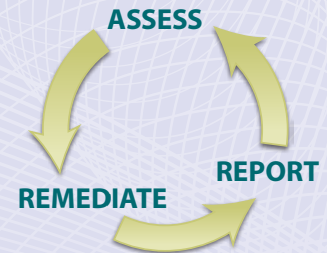


The intent of this PCI DSS Quick Reference Guide is to help you understand the PCI DSS and to apply it to your payment card transaction environment.

There are three ongoing steps for adhering to the PCI DSS: **Assess** — identifying cardholder data, taking an inventory of your IT assets and business processes for payment card processing, and analyzing them for vulnerabilities that could expose cardholder data. **Remediate** — fixing vulnerabilities and not storing cardholder data unless you need it. **Report** — compiling and submitting required remediation validation records (if applicable), and submitting compliance reports to the acquiring bank and card brands you do business with.

PCI DSS follows common sense steps that mirror best security practices. The DSS globally applies to *all* entities that store, process or transmit cardholder data. PCI DSS and related security standards are administered by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Participating Organizations include merchants, payment card issuing banks, processors, developers and other vendors.

PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS



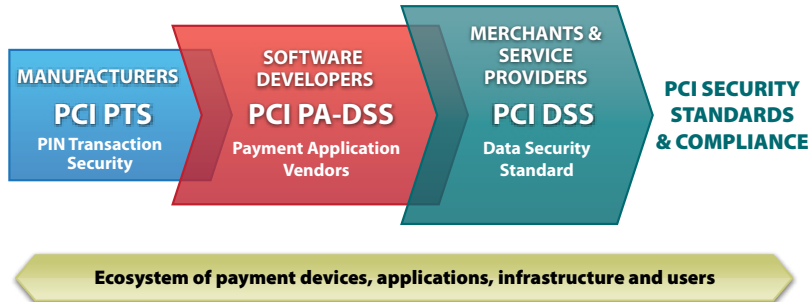
This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

Overview of PCI Requirements

PCI security standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council, American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



PCI Security Standards Include:

PCI Data Security Standard (DSS)

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you are a merchant who accepts or processes payment cards, you must comply with the PCI DSS.

PIN Transaction Security (PTS) Requirements

The PCI PTS (formerly PCI PED) is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. The requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it. Financial institutions, processors, merchants and service providers should only use devices or components that are tested and approved by the PCI SSC (www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php).

Payment Application Data Security Standard (PA-DSS)

The PA-DSS is for software developers and integrators of payment applications that store, process or transmit cardholder data as part of authorization or settlement when these applications are sold, distributed or licensed to third parties. Most card brands encourage merchants to use payment applications that are tested and approved by the PCI SSC. Validated applications are listed at: www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

The Council monitors new threats to cardholder data and may issue information supplements and other guidance for compliance. Changes to the PCI Security Standards follow a three-year lifecycle; the newest (version 2.0) was published in October 2010. For more information on the lifecycle, see: www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data. It consists of common sense steps that mirror security best practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none"> 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
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for all personnel

Tools for Assessing Compliance with PCI DSS

The PCI SSC sets the PCI security standards, but each payment card brand has its own program for compliance, validation levels and enforcement. More information about compliance can be found at these links:

- American Express: • www.americanexpress.com/datasecurity
- Discover Financial Services: • www.discovernetwork.com/fraudsecurity/disc.html
- JCB International: • www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: • www.mastercard.com/sdp
- Visa Inc: • www.visa.com/cisp
Visa Europe: • www.visaeurope.com/ais

Qualified Assessors. The Council manages programs that will help facilitate the assessment of compliance with PCI DSS: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs are approved by the Council to assess compliance with the PCI DSS. ASVs are approved by the Council to validate adherence to the PCI DSS scan requirements by performing vulnerability scans of Internet-facing environments of merchants and service providers. The Council also provides PCI DSS training for Internal Security Assessors (ISAs). Additional details can be found on our Web site at: www.pcisecuritystandards.org/approved_companies_providers/index.php

Self-Assessment Questionnaire. The Self-Assessment Questionnaire (SAQ) is a validation tool for eligible organizations who self-assess their PCI DSS compliance and who are not required to submit a Report on Compliance (ROC). Different SAQs are available for various business environments; more details can be found on our web site at: www.pcisecuritystandards.org. An organization's acquiring financial institution or payment brand can also determine if you should complete an SAQ.

PIN Transaction Security Requirements

These requirements, referred to as PCI PTS (formerly PCI PED), applies to companies which make devices or components that accept or process personal identification numbers as a part of a PIN based transaction and for other payment processing related activities. Recognized PTS laboratories validate adherence to the PTS requirements. Financial institutions, processors, merchants and service providers should ensure that they are using approved PTS devices or components. Non financial institutions should check with their acquiring financial institution to understand requirements and associated timeframes for compliance. The PTS requirements cover devices, including the physical and logical security characteristics of their components, and device management. For details and a list of approved PTS devices and components see: www.pcisecuritystandards.org/security_standards/ped/index.shtml

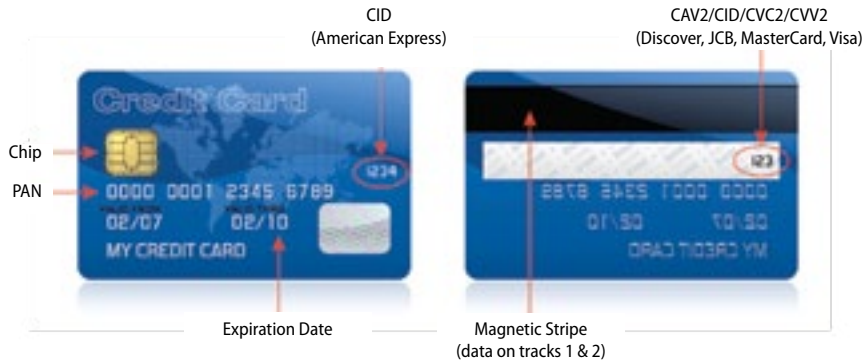
Payment Application Data Security Standard

The PA-DSS is a standard for developers of payment applications. Its goal is to help software vendors and others develop secure commercial payment applications that do not store prohibited data, and ensure that payment applications support compliance with the PCI DSS. The PA-DSS does not apply to payment applications developed by merchants in-house; those are covered by the PCI DSS. Merchants and service providers should ensure that they are using Council-approved payment applications; check with your acquiring financial institution to understand requirements and associated timeframes for implementing approved applications. PA-DSS has 13 requirements: For details and a list of approved Payment Applications, see: www.pcisecuritystandards.org/security_standards/index.php.

Security Controls and Processes for PCI DSS Requirements

The goal of the PCI Data Security Standard (PCI DSS) is to protect cardholder data wherever it is processed, stored or transmitted. The security controls and processes required by PCI DSS are vital for protecting cardholder account data, including the PAN – the primary account number printed on the front of a payment card. Merchants and any other service providers involved with payment card processing must never store sensitive authentication data after authorization. This includes sensitive data that is printed on a card, or stored on a card's magnetic stripe or chip – and personal identification numbers entered by the cardholder. This chapter presents the objectives of PCI DSS and related 12 requirements.

Types of Data on a Payment Card



This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

Build and Maintain a Secure Network

In the past, theft of financial records required a criminal to physically enter an organization's business site. Now, many payment card transactions (such as debit in the U.S. and "chip and pin" in Europe) use PIN entry devices and computers connected by networks. By using network security controls, entities can prevent criminals from virtually accessing payment system networks and stealing cardholder data.

Requirement 1: Install and maintain a firewall and router configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed into and out of an organization's network, and into sensitive areas within its internal network. Firewall functionality may also appear in other system components. Routers are hardware or software that connects two or more networks. All such devices are in scope for assessment of Requirement 1 if used within the cardholder data environment.

- 1.1 Establish firewall and router configuration standards that formalize testing whenever configurations change; that identify *all* connections to cardholder data (including wireless); that use various technical settings for each implementation; and stipulate a review of configuration rule sets at least every six months.
- 1.2 Build firewall and router configurations that restrict all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.
- 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.
- 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization's network.

CONTROLS FOR NETWORK SECURITY



Firewall

Device that controls the passage of traffic between networks and within an internal network



Router

Hardware or software that connects traffic between two or more networks

Illustration / Photo: Wikimedia Commons

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

The easiest way for a hacker to access your internal network is to try default passwords or exploits based on default system software settings in your payment card infrastructure. Far too often, merchants do not change default passwords or settings upon deployment. This is akin to leaving your store physically unlocked when you go home for the night. Default passwords and settings for most network devices are widely known. This information, combined with hacker tools that show what devices are on your network can make unauthorized entry a simple task – if you have failed to change the defaults.

- 2.1 Always change vendor-supplied defaults *before* installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.
- 2.2 Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified.
- 2.3 Encrypt using strong cryptography all non-console administrative access such as browser/web-based management tools.
- 2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data (details are in PCI DSS Appendix A: "Additional PCI DSS Requirements for Shared Hosting Providers.")

TYPICAL DEFAULT PASSWORDS THAT MUST BE CHANGED

[none]

[name of product / vendor]

1234 or 4321

access

admin

anonymous

database

guest

manager

pass

password

root

sa

secret

sysadmin

user

Protect Cardholder Data

Cardholder data refers to any information printed, processed, transmitted or stored in any form on a payment card. Entities accepting payment cards are expected to protect cardholder data and to prevent their unauthorized use – whether the data is printed or stored locally, or transmitted over a public network to a remote server or service provider.

Requirement 3: Protect stored cardholder data

In general, no cardholder data should ever be stored unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored. If your organization stores PAN, it is crucial to render it unreadable (see 3.4, and table below for guidelines).

- 3.1 Limit cardholder data storage and retention time to that required for business, legal, and/or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.
- 3.2 Do not store sensitive authentication data after authorization (even if it is encrypted). See guidelines in table below. Issuers and related entities may store sensitive authentication data if there is a business justification, and the data is stored securely.
- 3.3 Mask PAN when displayed; the first six and last four digits are the maximum number of digits you may display. Not applicable for authorized people with a legitimate business need to see the full PAN. Does not supersede stricter requirements in place for displays of cardholder data such as on a point-of-sale receipt.
- 3.4 Render PAN unreadable anywhere it is stored – including on portable digital media, backup media, in logs, and data received from or stored by wireless networks. Technology solutions for this requirement may include strong one-way hash functions of the entire PAN, truncation, index tokens with securely stored pads, or strong cryptography. (See PCI DSS Glossary for definition of strong cryptography.)

ENCRYPTION PRIMER

Cryptography uses a mathematical formula to render plaintext data unreadable to people without special knowledge (called a “key”). Cryptography is applied to stored data as well as data transmitted over a network.

Encryption changes plaintext into ciphertext.

Decryption changes ciphertext back into plaintext.

This is secret stuff, PSE do not...
 → 5a0 (k\$hQ% ...
 → This is secret stuff, PSE do not...

Illustration: Wikimedia Commons

- 3.5 Protect any keys used for encryption of cardholder data from disclosure and misuse.
- 3.6 Fully document and implement all appropriate key management processes and procedures for cryptographic keys used for encryption of cardholder data.

Guidelines for Cardholder Data Elements

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data¹	Full Magnetic Stripe Data ²	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
PIN/PIN Block		No	Cannot store per Requirement 3.2	

¹ Sensitive authentication data must not be stored after authorisation (even if encrypted).

² Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Cyber criminals may be able to intercept transmissions of cardholder data over open, public networks so it is important to prevent their ability to view these data. Encryption is a technology used to render transmitted data unreadable by any unauthorized person.

- 4.1** Use strong cryptography and security protocols such as SSL/TLS, SSH or IPSec to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, Global System for Mobile communications [GSM], General Packet Radio Service [GPRS]). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. The use of WEP as a security control is prohibited.
- 4.2** Never send unprotected PANs by end user messaging technologies.

Maintain a Vulnerability Management Program

Vulnerability management is the process of systematically and continuously finding weaknesses in an entity's payment card infrastructure system. This includes security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

Requirement 5: Use and regularly update anti-virus software or programs

Many vulnerabilities and malicious viruses enter the network via users' e-mail and other online activities. Anti-virus software must be used on all systems affected by malware to protect systems from current and evolving malicious software threats.

- 5.1** Deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers).
- 5.2** Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

VULNERABILITY MANAGEMENT



Create policy governing security controls according to industry standard best practices (e.g., IEEE 802.11i)

Regularly scan systems for vulnerabilities

Create remediation schedule based on risk and priority

Pre-test and **deploy** patches

Rescan to verify compliance

Update security software with the most current signatures and technology

Use only software or systems that were securely developed by industry standard best practices

Requirement 6: Develop and maintain secure systems and applications

Security vulnerabilities in systems and applications may allow criminals to access PAN and other cardholder data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation. Entities should apply patches to less-critical systems as soon as possible, based on a risk-based vulnerability management program. Secure coding practices for developing applications, change control procedures and other secure software development practices should always be followed.

- 6.1** Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Deploy critical patches within a month of release.
- 6.2** Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Risk rankings should be based on industry best practices and guidelines. Ranking vulnerabilities is a best practice that will become a requirement on July 1, 2012.
- 6.3** Develop software applications (internal and external, and including web-based administrative access) in accordance with PCI DSS and based on industry best practices. Incorporate information security throughout the software development life cycle.
- 6.4** Follow change control processes and procedures for all changes to system components.
- 6.5** Develop applications based on secure coding guidelines and review custom application code to identify coding vulnerabilities. Follow up-to-date industry best practices to identify and manage vulnerabilities.
- 6.6** Ensure all public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications.

Implement Strong Access Control Measures

Access control allows merchants to permit or deny the use of physical or technical means to access PAN and other cardholder data. Access must be granted on a business need to know basis. Physical access control entails the use of locks or restricted access to paper-based cardholder records or system hardware. Logical access control permits or denies use of PIN entry devices, a wireless network, PCs and other devices. It also controls access to digital files containing cardholder data.

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. Need to know is when access rights are granted to only the least amount of data and privileges needed to perform a job.

- 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.
- 7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Requirements apply to all accounts, including point of sale accounts, with administrative capabilities and all accounts with access to stored cardholder data.

- 8.1 Assign all users a unique user name before allowing them to access system components or cardholder data.

RESTRICTING ACCESS IS CRUCIAL!



Restrict Access to Cardholder Data Environments by employing access controls such as RBAC (Role Based Access Control)

Limit access to only those individuals whose job requires such access

Formalize an access control policy that includes a list of who gets access to specified cardholder data and systems

Deny all access to anyone who is not specifically allowed to access cardholder data and systems

Photo: Wikimedia Commons

- 8.2 Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric.
- 8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. For example, use technologies such as remote authentication and dialin service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication. Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication.
- 8.4 Render all passwords unreadable during storage and transmission, for all system components, by using strong cryptography.
- 8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components.

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hardcopies, and should be appropriately restricted. "Onsite personnel" are full- and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity's premises. "Visitors" are vendors and guests that enter the facility for a short duration - usually up to one day. "Media" is all paper and electronic media containing cardholder data.

- 9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
- 9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.

GIVE EVERY USER A UNIQUE ID



Every user with access to the Cardholder Data Environment must have a unique ID. This allows a business to trace every action to a specific individual.

PHYSICALLY SECURE THE PAYMENT SYSTEM



Businesses must physically secure or restrict access to printouts of cardholder data, to media where it is stored, and to devices used for accessing or storing cardholder data. It's important to understand that PCI DSS is about protecting both electronic data and paper receipts as well.

Illustration: Wikimedia Commons

- 9.3 Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained; given a physical token that expires and that identifies visitors as not onsite personnel; and are asked to surrender the physical token before leaving the facility or at the date of expiration.
- 9.4 Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name and company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law.
- 9.5 Store media back-ups in a secure location, preferably off site.
- 9.6 Physically secure all media.
- 9.7 Maintain strict control over the internal or external distribution of any kind of media. Classify media so the sensitivity of the data can be determined.
- 9.8 Ensure that management approves any and all media moved from a secured area, especially when media is distributed to individuals.
- 9.9 Maintain strict control over the storage and accessibility of media.
- 9.10 Destroy media when it is no longer needed for business or legal reasons.

Regularly Monitor and Test Networks

Physical and wireless networks are the glue connecting all endpoints and servers in the payment infrastructure. Vulnerabilities in network devices and systems present opportunities for criminals to gain unauthorized access to payment card applications and cardholder data. To prevent exploitation, organizations must regularly monitor and test networks to find and fix vulnerabilities.

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is very difficult without system activity logs.

- 10.1** Establish a process for linking all access to system components to each individual user – especially access done with administrative privileges.
- 10.2** Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of the audit logs; creation and deletion of system-level objects.
- 10.3** Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.
- 10.4** Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time.
- 10.5** Secure audit trails so they cannot be altered.
- 10.6** Review logs for all system components related to security functions at least daily.
- 10.7** Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.

MONITOR ALL ACTIVITY



Organizations must track and monitor all access to cardholder data and related network resources – in stores, regional offices, headquarters, and other remote access.

Photo: Wikimedia Commons

Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security is maintained over time. Testing of security controls is especially important for any environmental changes such as deploying new software or changing system configurations.

- 11.1** Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. Typical methods are wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.
- 11.2** Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, pass four consecutive quarterly scans as a requirement for compliance. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes may be performed by internal staff.
- 11.3** Perform external and internal penetration testing, including network- and application-layer penetration tests, at least annually and after any significant infrastructure or application upgrade or modification.
- 11.4** Use network intrusion detection systems and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.
- 11.5** Deploy file integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly.

SEVERITY LEVELS FOR VULNERABILITY SCANNING

CVSS Score	Severity Level	Scan Results
7.0 through 10.0	High Severity	Fail
4.0 through 6.9	Medium Severity	Fail
0.0 through 3.9	Low Severity	Pass

“To demonstrate compliance, a scan must not contain high-level vulnerabilities in any component in the cardholder data environment. Generally, to be considered compliant, none of those components may contain any vulnerability that has been assigned a Common Vulnerability Scoring System (CVSS) base score equal to or higher than 4.0.”

Maintain an Information Security Policy

A strong security policy sets the tone for security affecting an organization's entire company, and it informs employees of their expected duties related to security. All employees should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

Requirement 12: Maintain a policy that addresses information security for all personnel

- 12.1** Establish, publish, maintain, and disseminate a security policy that addresses all PCI DSS requirements, includes an annual process for identifying vulnerabilities and formally assessing risks, and includes a review at least once a year and when the environment changes.
- 12.2** Develop daily operational security procedures that are consistent with requirements in PCI DSS.
- 12.3** Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.
- 12.4** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
- 12.5** Assign to an individual or team information security responsibilities defined by 12.5 subsections.
- 12.6** Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
- 12.7** Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. Example screening includes previous employment history, criminal record, credit history, and reference checks.

"PCI DSS represents the best available framework to guide better protection of cardholder data. It also presents an opportunity to leverage cardholder data security achieved through PCI DSS compliance for better protection of other sensitive business data – and to address compliance with other standards and regulations."

AberdeenGroup
IT Industry Analyst

- 12.8** If cardholder data is shared with service providers, maintain policies and procedures to formally identify service provider responsibilities for securing cardholder data, and monitor service providers' PCI DSS compliance status at least annually.
- 12.9** Implement an incident response plan. Be prepared to respond immediately to a system breach.

Compensating Controls for PCI DSS Requirements

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of compensating controls. In order for a compensating control to be considered valid, it must be reviewed by a qualified assessor. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Entities should be aware that a particular compensating control will not be effective in all environments. See PCI DSS, Appendices B and C for details.

How to Comply with PCI DSS

Merchants and other entities that store, process and/or transmit cardholder data must comply with PCI DSS. While the Council is responsible for managing the data security standards, each payment card brand maintains its own separate compliance enforcement programs. Each payment card brand has defined specific requirements for compliance validation and reporting, such as provisions for performing self-assessments and when to engage a QSA.

Depending on an entity's classification or risk level (determined by the individual payment card brands), processes for validating compliance and reporting to acquiring financial institutions usually follow this track:

1. **PCI DSS Scoping** – determine what system components are governed by PCI DSS
2. **Assessing** – examine the compliance of system components in scope
3. **Compensating Controls** – assessor validates alternative control technologies/processes
4. **Reporting** – assessor and/or entity submits required documentation
5. **Clarifications** – assessor and/or entity clarifies/updates report statements (if applicable) upon request of the acquiring bank or payment card brand

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

Specific questions about compliance validation levels should be directed to your acquiring financial institution or payment card brand. Only the acquiring financial institution can assign a validation level to merchants. Links to card brand compliance programs include:

- American Express: • www.americanexpress.com/datasecurity
- Discover Financial Services: • www.discovernetwork.com/fraudsecurity/disc.html
- JCB International: • www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: • www.mastercard.com/sdp
- Visa Inc: • www.visa.com/cisp
- Visa Europe: • www.visaeurope.com/ais

Choosing a Qualified Security Assessor

A Qualified Security Assessor (QSA) is a data security firm that has been trained and is certified by the PCI Security Standards Council to perform on-site security assessments for verification of compliance with PCI DSS. The QSA will:

- Verify all technical information given by merchant or service provider
- Use independent judgment to confirm the standard has been met
- Provide support and guidance during the compliance process
- Be onsite for the validation of the assessment or duration as required
- Review the work product that supports the PCI DSS Requirements and Security Assessment Procedures
- Ensure adherence to the PCI DSS Security Assessment Procedures
- Validate the scope of the assessment
- Select systems and system components where sampling is employed
- Evaluate compensating controls
- Produce the final report

PREPARING FOR A PCI DSS ASSESSMENT



Gather Documentation: Security policies, change control records, operational procedures, network diagrams, PCI DSS letters and notifications

Schedule Resources: Ensure participation of a project manager and key people from IT, security applications, business operations, human resources and legal

Describe the Environment: Organize information about the cardholder data environment, including cardholder data flows and locations of cardholder data repositories

The QSA you select should have solid understanding of your business and have experience in assessing the security of similar organizations. That knowledge helps the QSA to understand business sector-specific nuances of securing cardholder data under PCI DSS. Also, look for a good fit with your company's culture. The assessment will conclude whether you are compliant or not – but the QSA will also work with your organization to help you understand how to achieve and maintain compliance. Many QSAs also can provide additional security-related services such as ongoing vulnerability assessment and remediation. A list of QSAs is available at www.pcisecuritystandards.org/approved_companies_providers/qa_companies.php.

Choosing an Approved Scanning Vendor

An Approved Scanning Vendor (ASV) is a data security firm using a scanning solution to determine whether or not the customer is compliant with the PCI DSS external vulnerability scanning requirement. ASVs have been trained and are qualified by the PCI Security Standards Council to perform external network and system scans as required by the PCI DSS. An ASV may use its own software or an approved commercial or open source solution to validate compliance. ASV solutions must be non-disruptive to customers' systems and data – they must never cause a system reboot, or interfere with or change domain name server (DNS) routing, switching, or address resolution. Root-kits or other software should not be installed unless part of the solution and pre-approved by the customer. Tests not permitted by the ASV solution include denial of service, buffer overflow, brute force attack resulting in a password lockout, or excessive usage of available communication bandwidth.

An ASV scanning solution includes the scanning tool(s), the associated scanning report, and the process for exchanging information between the scanning vendor and the customer. ASVs may submit compliance reports to the acquiring institution on behalf of a merchant or service provider. A list of ASVs is available at www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php.

ISA PROGRAM

The PCI SSC Internal Security Assessor (ISA) Program provides an opportunity for eligible internal security assessment professionals of qualifying organizations to receive PCI DSS training and certification that will improve the organization's understanding of the PCI DSS, facilitate the organization's interactions with QSAs, enhance the quality, reliability, and consistency of the organization's internal PCI DSS self-assessments, and support the consistent and proper application of PCI DSS measures and controls.

Please see the PCI SSC web site for details – www.pcisecuritystandards.org/approved_companies_providers/internal_security_assessors.php

Scope of Assessment for Compliance

The first step of a PCI DSS compliance effort is to accurately determine the scope of the environment. The scoping process includes identifying all system components that are located within or connected to the cardholder data environment. The cardholder data environment is comprised of people, processes, and technology that handle cardholder data or sensitive authentication data. System components include network devices (both wired and wireless), servers and applications. Virtualization components, such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors, are also considered system components within PCI DSS.

Scoping must occur at least annually and prior to the annual assessment. Merchants and other entities must identify all locations and flows of cardholder data to ensure all applicable system components are included in scope for PCI DSS. Entities should confirm the accuracy and appropriateness of PCI DSS scope by performing these steps:

- The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE).
- Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).
- The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE unless such data is deleted or migrated/consolidated into the currently defined CDE.
- The entity retains documentation that shows how PCI DSS scope was confirmed and the results, for assessor review and/or for reference during the next annual PCI SCC scope confirmation activity.

Network Segmentation

Scope can be reduced with the use of segmentation, which isolates the cardholder data environment from the remainder of an entity's network. Reduction of scope can lower the cost of the PCI DSS assessment, lower the cost and difficulty of implementing and maintaining PCI DSS controls, and reduce risk for the entity. For more information on scoping, see PCI DSS Appendix D: Segmentation and Sampling of Business Facilities/System Components.

Sampling of Business Facilities and System Components

The assessor may independently select representative examples of business facilities and system components to assess PCI DSS requirements. This practice, called sampling, is not required by PCI DSS. Sampling must follow rules and processes defined in PCI DSS. Sampling does not reduce scope of the cardholder data environment or the applicability of PCI DSS requirements. If sampling is used, each sample must be assessed against all applicable PCI DSS requirements. Sampling of the PCI DSS requirements themselves is not permitted. For more information on sampling, see PCI DSS Appendix D: Segmentation and Sampling of Business Facilities/System Components.

Compensating Controls

On an annual basis, any compensating controls must be documented, reviewed, and validated by the assessor and included with the Report on Compliance. For more information on compensating controls, see PCI DSS Appendix B: Compensating Controls and Appendix C: Compensating Controls Worksheet.

Using the Self-Assessment Questionnaire (SAQ)

The SAQ is a validation tool for eligible merchants and service providers who self-assess their PCI DSS compliance and who are not required to submit a Report on Compliance (ROC). The SAQ includes a series of yes-or-no questions for compliance. If an answer is no, the organization must state the future remediation date and associated actions. In order to align more closely with merchants and their compliance validation process, the SAQs provide flexibility based on the complexity of particular merchant environments (see chart below). The PCI DSS Self-Assessment Questionnaire Guidelines and Instructions document provides more details on each SAQ type (see www.pcisecuritystandards.org).

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. <i>This would never apply to face-to-face merchants.</i>
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment card brand as eligible to complete an SAQ

Reporting

Reports are the official mechanism by which merchants and other entities verify compliance with PCI DSS to their respective acquiring financial institutions or payment card brand. Depending on payment card brand requirements, merchants and service providers may need to submit an SAQ or annual attestations of compliance for on-site assessments. Quarterly submission of a report for network scanning may also be required. Finally, individual payment card brands may require submission of other documentation; see their web sites for more information (URLs listed above).

Information Contained in PCI DSS Report on Compliance

The template for an entity's annual Report on Compliance includes the following:

1. Executive Summary (description of entity's payment card business; high level network diagram)
2. Description of Scope of Work and Approach Taken (description of how the assessment was made, environment, network segmentation used, details for each sample set selected and tested, wholly-owned or international entities requiring compliance with PCI DSS, wireless networks or applications that could impact security of cardholder data, version of PCI DSS used to conduct the assessment)
3. Details about Reviewed Environment (diagram of each network, description of cardholder data environment, list of all hardware and software in the CDE, service providers used, third party payment applications, individuals interviewed, documentation reviewed, details for reviews of managed service providers)
4. Contact Information and Report Date
5. Quarterly Scan Results (summary of four most recent ASV scan results)
6. Findings and Observations (detailed findings on each requirement and sub-requirement, including explanations of all N/A responses and validation of all compensating controls)

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

COMPLIANCE PROGRAM

Assess

Assess your network and IT resources for vulnerabilities. You should constantly monitor access and usage of cardholder data. Log data must be available for analysis

Remediate

You must fix vulnerabilities that threaten unauthorized access to cardholder data

Report

Report compliance and present evidence that data protection controls are in place

Web Resources

PCI Security Standards Council Web site, including Frequently Asked Questions (FAQs): www.pcisecuritystandards.org

Membership Information

www.pcisecuritystandards.org/get_involved/join.php

Webinars

www.pcisecuritystandards.org/news_events/events.shtml

Training (for assessors)

QSAs: www.pcisecuritystandards.org/training/qa_training.php

PA-DSS: www.pcisecuritystandards.org/training/pa-dss_training.php

PCI SSC approved applications and devices

PIN Transaction Security (PTS) Devices: www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Payment Applications: www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

PCI Data Security Standard (PCI DSS)

The Standard: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

Supporting Documents: https://www.pcisecuritystandards.org/security_standards/documents.php

Approved Assessors and Scanning Vendors: https://www.pcisecuritystandards.org/approved_companies_providers/index.php

Navigating the Standard: https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf

Self-Assessment Questionnaire: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

Glossary: https://www.pcisecuritystandards.org/security_standards/glossary.php

Approved QSAs: https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

Approved ASVs: https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

About the PCI Security Standards Council

The PCI Security Standards Council (PCI SSC) is a global open body formed to develop, enhance, disseminate and assist with the understanding of security standards for payment account security. The Council maintains, evolves, and promotes the Payment Card Industry security standards. It also provides critical tools needed for implementation of the standards such as assessment and scanning guidelines, a self-assessment questionnaire, training and education, and product certification programs.

The PCI SSC founding members, American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., have agreed to incorporate the PCI Data Security Standard as part of the technical requirements for each of their data security compliance programs. Each founding member also recognizes the Qualified Security Assessors and Approved Scanning Vendors qualified by the PCI SSC to assess compliance with the PCI DSS.

The PCI SSC's founding member card brands share equally in the Council's governance and operations. Other industry stakeholders participate in reviewing proposed additions or modifications to the standards, including merchants, payment card issuing banks, processors, hardware and software developers, and other vendors.

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

PCI SSC FOUNDERS



PARTICIPATING ORGANIZATIONS

Merchants, Banks, Processors,
Hardware and Software
Developers and Point-of-Sale
Vendors

PCI Data Security Standard

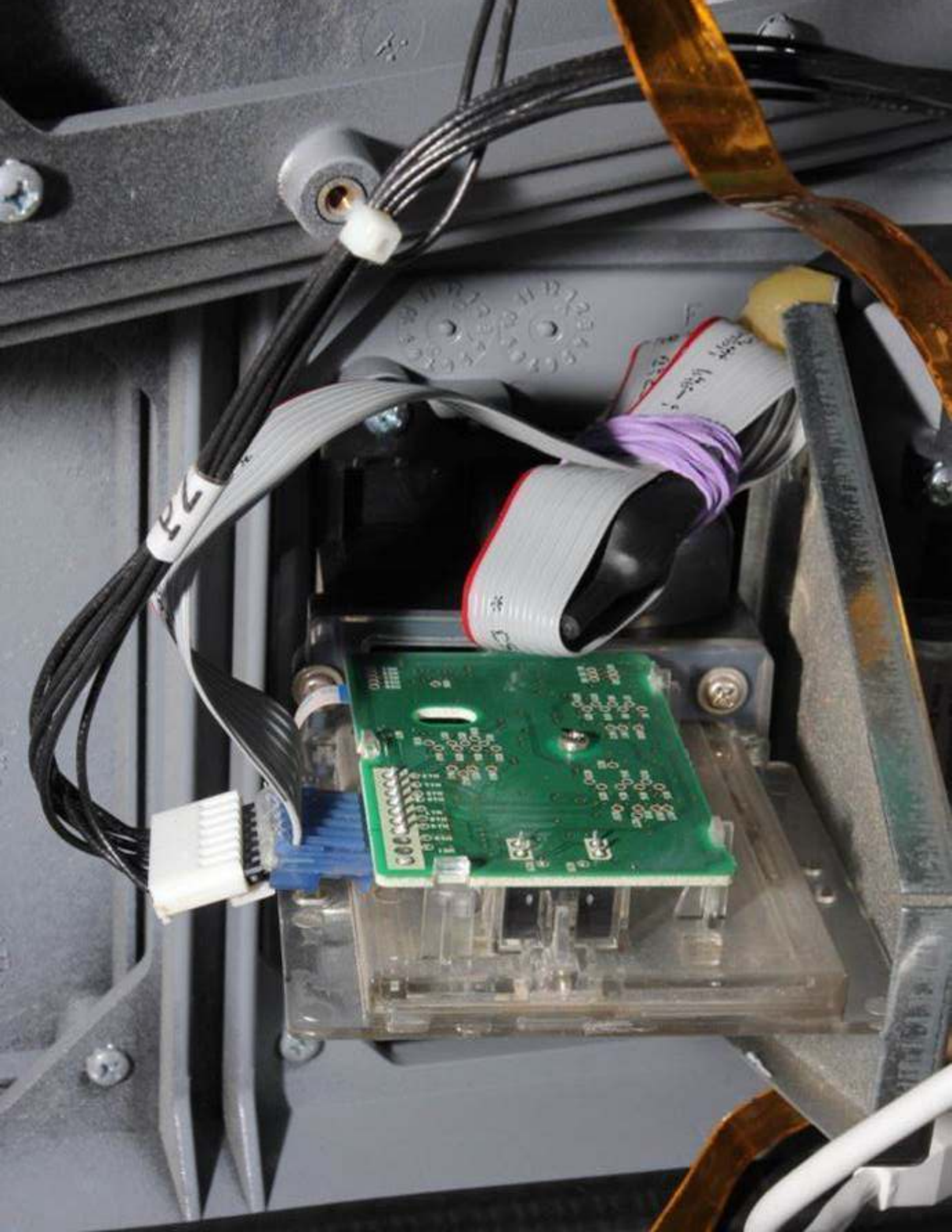
The PCI DSS is a set of comprehensive requirements for enhancing payment account data security. It represents common sense steps that mirror security best practices. Learn more about its requirements, security controls and processes, and steps to assess compliance inside this PCI DSS Quick Reference Guide.

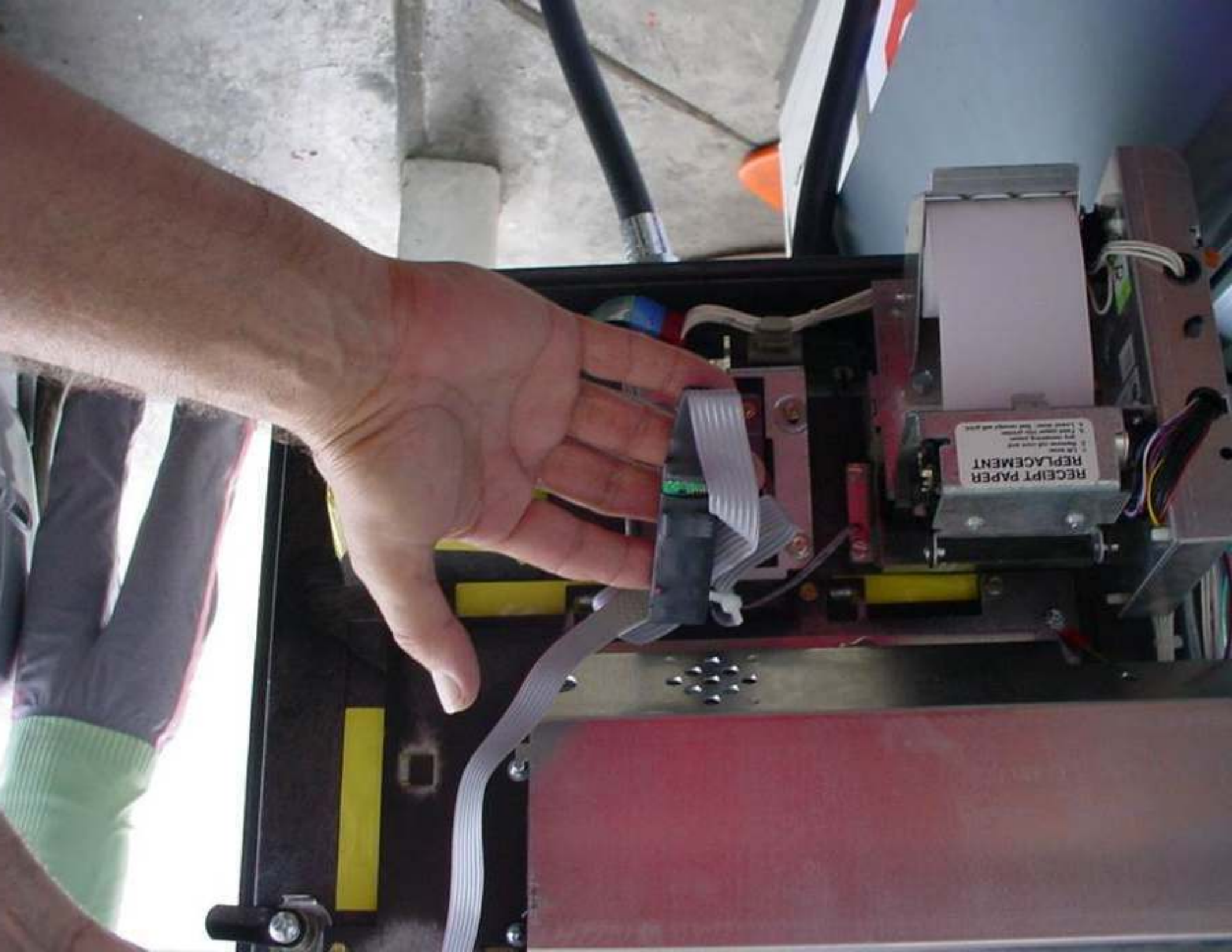
Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need to know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for all personnel

ATTACHMENT 3
PHOTOS & BROCHURE RE SKIMMERS

ATM Terminal # TX0044

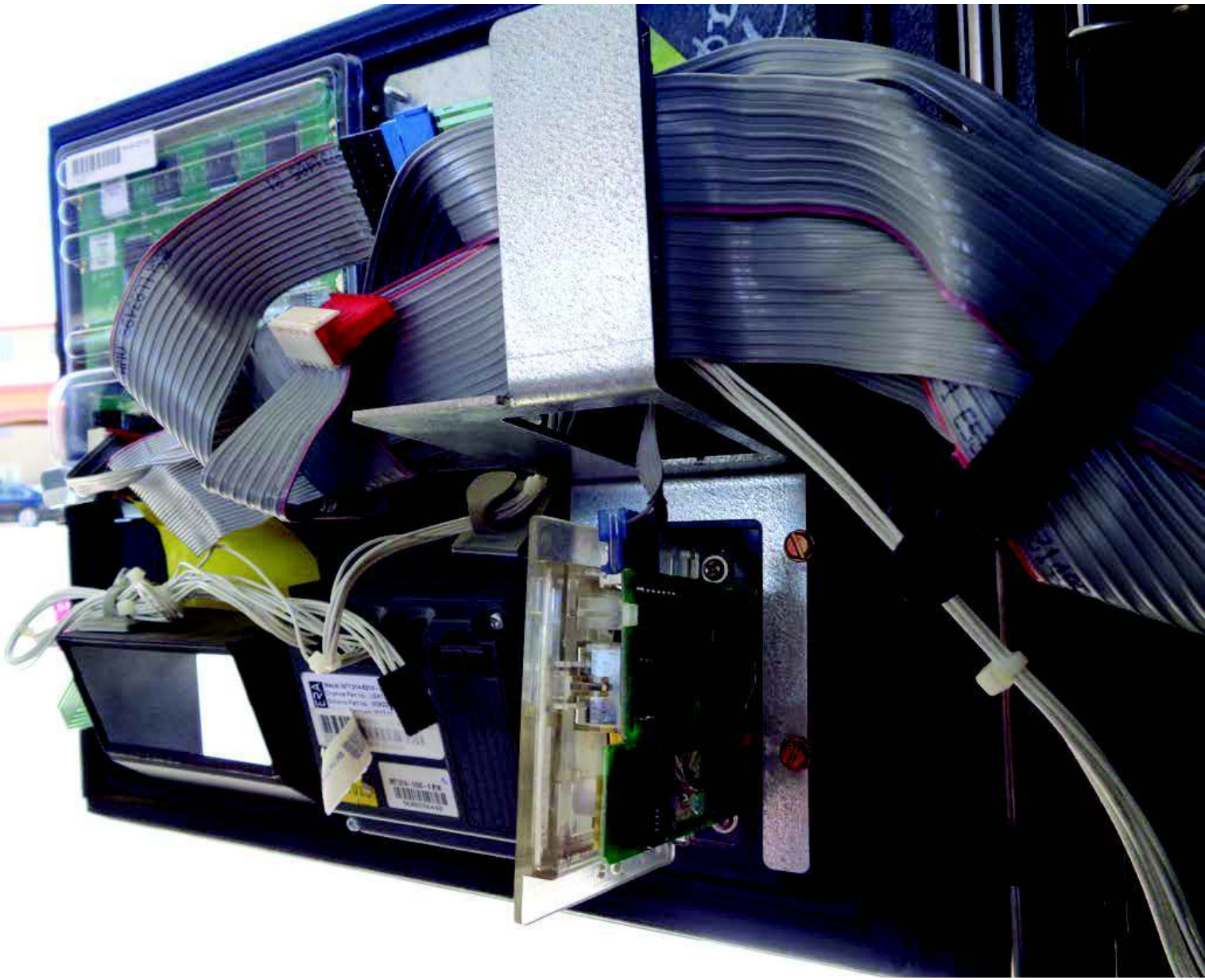


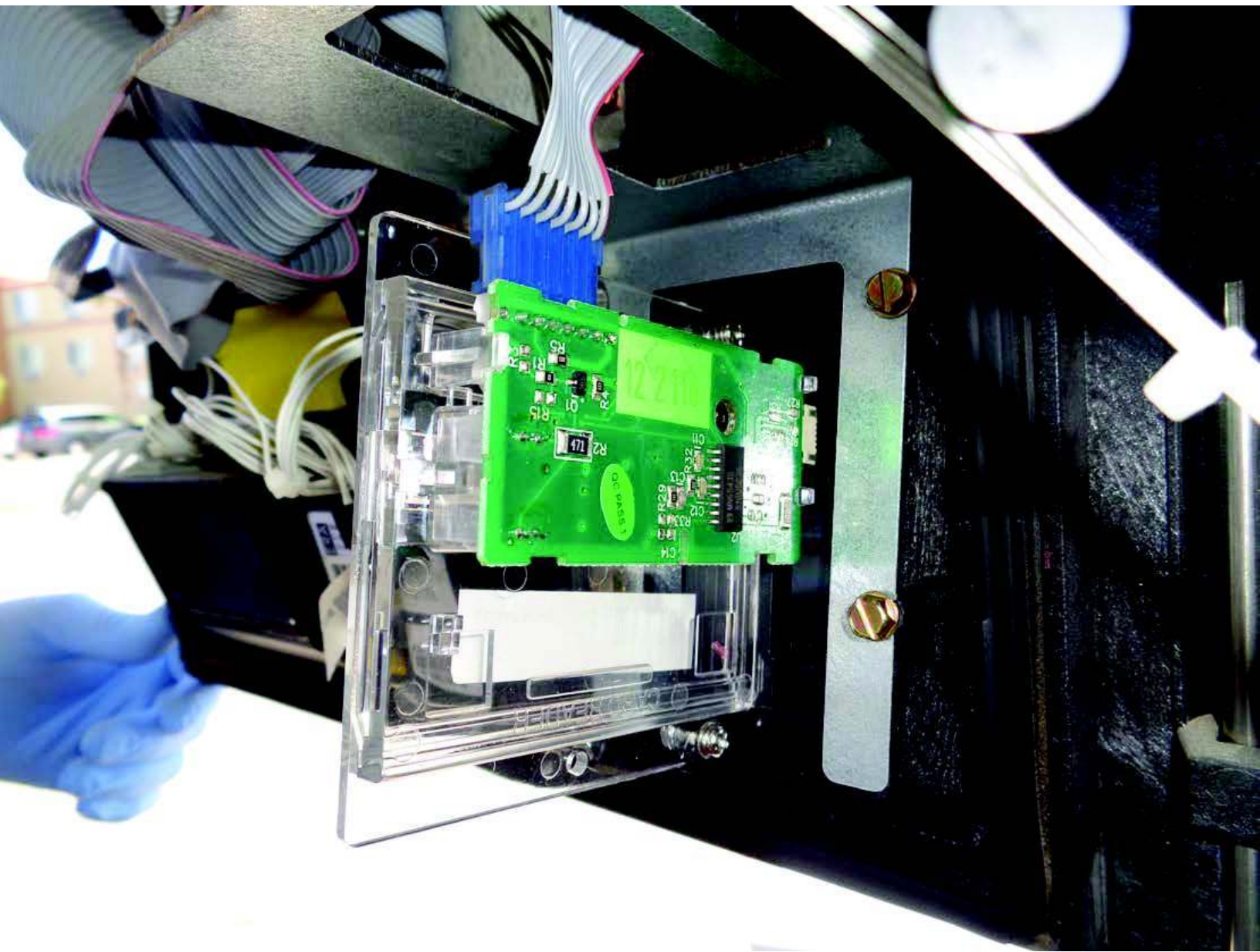














FLEXI RULER







MSD 0128

SAMSUNG

DOUBLE



3. Many gas pumps use the same master key to open the door. These master keys can be easily obtained. Secure the master key and limit access to those deemed necessary.
4. Security seals placed on the door should be stored in a secure area and not inside of the gas pump or an area easily accessible by a criminal.

Be aware of indicators which may indicate Gas Pump Skimming Activity is or has occurred:

1. Card slot of the gas pump is loose or has fallen off, or other parts of the machine have dislodged from the pump.
2. The presence of double sided tape on the gas pump or presence of glue or pry marks around the card slot area.
3. Excessive or out of the ordinary electrical tape on internal components.
4. Observation of person(s) attaching or removing or tampering with parts of the gas pump or at the pump for an unusual amount of time.
5. Skimmers are often placed on the outside of gas pumps furthest away from the store and often out of camera view.

Police advise that if a skimming device is located, for the best chance of identifying those involved, please do not touch or remove the device. Immediately contact store management and law enforcement.

Please contact the Henderson Police Department Financial Crimes Division with any questions at (702) 267-4750.



cityofhenderson.com

**Henderson Police Department
702-267-5000**

**PROTECT
YOURSELF**
From ATM and Gas Pump Skimming

**To protect your customers
from becoming a victim,
follow these simple steps.**

ATM Skimming

ATM skimming involves the attachment of electronic devices on or around the ATM for the purposes of capturing both the magnetic strip data contained on the back of a debit card as well as the PIN number that is entered by the customer when using the ATM. The devices used to capture the information will vary in shapes, sizes and designs but are made to be unobtrusive or mimic legitimate components.

To reduce the risk of becoming a victim of ATM skimming:

1. Inspect ATM regularly and look for any signs of tampering or anything out of the ordinary.
2. Lightly tug the area of the card slot. Many skimming devices have the appearance of standard equipment but are overlays which are affixed by double sided tape for quick install and removal.
3. Inspect the machine for an attachment installed around or above the PIN pad containing a small pinhole camera. These are also often made to resemble a factory piece of the ATM and are often affixed with double-sided tape.

Be aware of indicators which may indicate ATM Skimming Activity is or has occurred:

1. Card slot of the ATM is loose or has fallen off, or other parts of the ATM machine have dislodged from the ATM.
2. The presence of double sided tape on the ATM machine or presence of glue or pry marks around the card slot of the ATM.
3. Observation of person(s) attaching, removing or tampering with parts of the ATM machine.
4. Person(s) who are using the ATM and are intentionally covering their faces to avoid being depicted (ex. hats, scarfs and sunglasses).
5. Person(s) spending long periods of time at or around ATM machines and periodically inspect the machine but do not conduct transactions.
6. Person(s) who show up at an ATM multiple times in a short period (may be conducting an inspection or ensuring the device is working properly).

Police advise that if a skimming device is located, for the best chance of identifying those involved, please do not touch or remove the device. Contact your store manager and law enforcement.

Gas Pump Skimmers

Gas pump skimmers can be installed externally over the card reader, or internally. These devices also come in various configurations.

The most common example includes placing a standard appearing overlay over the card slot and/or PIN pad to capture electronic data as customers swipe their cards. These are made to mimic legitimate devices and are often affixed using double-sided tape.



Broken seal



Inside card reader

Another type of Gas Pump Skimming device involves gaining access to the inside of the Gas Pump and installing a cable with an inline recording device that runs between the card reader and main circuit board.

To reduce the risk of becoming a victim of Gas Pump Skimming:

1. Inspect both the exterior and interior regularly and look for any signs of tampering or anything out of the ordinary.
2. Lightly tug the area of the card slot. Many skimming devices have the appearance of standard equipment but are overlays which are affixed by double sided tape for quick install and removal.



ATTACHMENT 4
NRS 603A COMPLIANCE CHECKLIST

NRS 603A COMPLIANCE CHECKLIST

The Bureau of Consumer Protection has compiled this checklist and guide to help data collectors (NRS 603A.030) in their effort to comply with NRS 603A. **This Checklist is not a substitute for compliance with 603A.** Instead, it is designed as a useful tool to aid in the development of a written information security program for data collectors that handle “personal information.” Each item requires proactive attention in order for a plan to be comprehensive. **While following these guidelines should assist a data collector in its efforts to adequately protect the personal information of its employees and customers, it is the responsibility of the data collector to review NRS 603A in its entirety and implement the most appropriate practices and procedures for its business.**

1. Assessment Checklist

The following checklist is designed to help data collectors identify any gaps that may exist in their current information security program. **This checklist is not exhaustive and should not be relied upon as a definitive authority for compliance with NRS 603A. Each data collector should retain the assistance of legal and/or technical consultants, as necessary, to formally assess the adequacy of the data collector’s current practices.**

I. Characterization and Usage of the Information

<input type="checkbox"/> A natural person’s first name or first initial and last name in combination with any one or more of the following data elements is considered personal information (“PI”): <input type="checkbox"/> Social security number <input type="checkbox"/> Driver’s license number, driver authorization card number or identification card number <input type="checkbox"/> Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person’s financial account <input type="checkbox"/> A medical identification number or a health insurance identification number <input type="checkbox"/> A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account
<input type="checkbox"/> Is PI collected and stored by paper and electronically?
<input type="checkbox"/> Is PI that is collected and stored necessary and relevant to the corresponding transaction? <input type="checkbox"/> If not, can PI be properly disposed of? (NRS 603A.200) <input type="checkbox"/> If not, is the maintenance, retention, or disposal of PI governed by a particular statute?
<input type="checkbox"/> Does data collector require the use of all PI marked above?
<input type="checkbox"/> Does data collector use PI in any other manner?
<input type="checkbox"/> Do third party businesses have on-site or remote access to PI stored with or used by data collector? <input type="checkbox"/> If so, does data collector know how PI is accessed, retained and used by the third party? <input type="checkbox"/> Is data collector notified each time a third party gains remote access to its system?
<input type="checkbox"/> Does data collector have use and retention policies for PI?
<input type="checkbox"/> Does data collector comply with the current version of Payment Card Industries (“PCI”) Data Security Standard? (NRS 603A.215)
<input type="checkbox"/> Does data collector store sensitive authentication data after authorization?

II. Retention

<input type="checkbox"/> Do the employees, with or without knowledge, handle PI?
<input type="checkbox"/> Does data collector physically store PI in any other manner?
<input type="checkbox"/> Does data collector store PI in any other format(s)?
<input type="checkbox"/> Can the data collector identify all connections between the data network in your business?
<input type="checkbox"/> Does data collector destroy media when it is no longer needed for business or legal reasons?
<input type="checkbox"/> Does data collector have a procedure for consumers requesting a copy of their PI?
<input type="checkbox"/> Do employees understand and abide by the processes for retaining and disseminating PI?
<input type="checkbox"/> Does data collector encrypt any PI stored on its computer network, disks, or portable storage devices? <input type="checkbox"/> Is PI sent internally or externally encrypted?

III. Notification and Redress

<input type="checkbox"/> Does data collector notify consumers concerning updates to policies or procedures in a timely manner?
<input type="checkbox"/> Does data collector notify consumers concerning changes to usage in PI or dissemination of PI in a timely manner?
<input type="checkbox"/> Does data collector have a policy or plan ready to implement when a data breach has been detected or identified? (NRS 603A.020)
<input type="checkbox"/> Does data collector have a policy or process that will notify persons affected by a data breach? (NRS 603A.220)
<input type="checkbox"/> Does data collector have a risk assessment process in place?
<input type="checkbox"/> Does data collector regularly implement the established risk assessment process at least once every six months?
<input type="checkbox"/> Does data collector have a procedure for customers wishing to file a grievance or complaint?
<input type="checkbox"/> Does data collector offer different avenues for redressability of a grievance or complaint?
<input type="checkbox"/> Does data collector record and document all investigations and findings?

IV. Controls on Access

<input type="checkbox"/> Is the internal network secure from unauthorized electronic access?
<input type="checkbox"/> Is the internal system appropriately restricting inbound and outbound traffic?
<input type="checkbox"/> Does the data collector collect and store PI that includes payment card data? <input type="checkbox"/> If so, is the PI protected by requiring the use of a token, "smart card," thumb print, or other biometric—as well as a password—to access the central computer?
<input type="checkbox"/> Does data collector, specialized employee, or third-party IT company regularly run up-to-date anti-virus and anti-spyware programs on individual computers and on servers on your network?
<input type="checkbox"/> Does data collector restrict the use of laptops or work-related electronic devices to those employees who need them to perform their jobs? <input type="checkbox"/> Does data collector require employees to store work-related laptops and electronic devices in a secure place? <input type="checkbox"/> Does data collector restrict laptop use to only network access of PI and not storage? <input type="checkbox"/> Are all work-related laptops and electronic devices encrypted?

<input type="checkbox"/> Is the network protected by requiring the use of a token, “smart card,” thumb print, or other biometric—as well as a password—to access the central computer?
<input type="checkbox"/> Does data collector require an employee’s user name and password to be different? <input type="checkbox"/> Do employees have unique strong passwords—the longer, the better—that use a combination of letters, symbols, and numbers? <input type="checkbox"/> Do employees change their passwords regularly or at least once every three months?
<input type="checkbox"/> Does data collector, specialized employee, or third party IT company regularly check for patches that address new vulnerabilities? <input type="checkbox"/> Does data collector have an implementation policy—addressing time, manner, and training—in place for installing new patches?
<input type="checkbox"/> Are employees trained to handle PI? <input type="checkbox"/> Are employees provided with written policies and procedures on how to safeguard personal information? <input type="checkbox"/> Are such policies and procedures updated regularly and at least every six months?
<input type="checkbox"/> Are key employees certified by PCI to assess risk to PI in the normal course of business?
<input type="checkbox"/> Do employees have regular access to PI in the normal course of business?
<input type="checkbox"/> Do employees who are authorized to access PI have a unique ID?
<input type="checkbox"/> When data collector receives or transmits PI, does data collector protect the information in transit using a secure connection?

2. Implementation and Goals

After identifying any gaps in your current infrastructure, or if you are developing an information security program for the first time, the following guide may be useful. This guide identifies some of the public policies served by implementing a comprehensive information security program and, with those goals in mind, offers some suggestions for its development. **This guide is not exhaustive and should not be relied upon as a definitive authority for compliance with NRS 603A. Each data collector should familiarize itself with all obligations imposed by NRS 603A, and retain the assistance of legal and/or technical consultants, as necessary, to implement the most appropriate practices and procedures for its business.**

Data Collector’s Responsibilities:

Accountability at the beginning

- Determine if you collect or use Personal Information, as described in NRS 603A.040.
- Commit to compliance with NRS 603A.200.
- Commit to compliance with NRS 603A.210.
- Commit to compliance with NRS 603A.215, and if applicable, PCI data security standards.
- Appoint an individual (or individuals) to be responsible for your organization’s compliance, and determine if an Information Security manager is needed.
- Establish an internal hierarchy that identifies what security issues should be escalated to the data collector’s board of directors or chief executive officer(s).
- Protect all personal information held by your organization or transferred to a third party for processing.
- Develop and implement personal information policies, procedures and practices.

- Review all written policies and procedures regularly, at least every 6 months, and update them as necessary to guard against emerging security threats.
- Inform customers, clients and employees that you have policies and practices for the management and security of personal information.
- Make these policies and practices understandable and easily available.

Data Collecting Boundaries and Purposes

- Before or when any personal information is collected, identify why it is needed and how it will be used.
- Document why the information is collected.
- Inform the individual from whom the information is collected why it is needed.
- Identify any new purpose for the information and obtain the individual's consent before using it, or provide the individual with a reasonable opportunity to deny any new uses of such information.

Consent

- Specify what personal information you are collecting and why in a way that your customers and clients can clearly understand.
- Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal information.
- Obtain the individual's consent before or at the time of collection, as well as when a new use of their personal information is identified.

Collection Practices

- Do not collect personal information indiscriminately.
- Do not deceive or mislead individuals about the reasons for collecting personal information.

Restrictions on use, disclosure, and retention

- Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by law.
- Keep personal information only as long as necessary to satisfy the purposes.
- Put guidelines and procedures in place for retaining and destroying personal information.
- Keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress.
- Securely destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

Accuracy

- Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

Safeguards

- Protect personal information against loss or theft.
- Safeguard the information from unauthorized access, disclosure, copying, use or modification.
- Protect personal information regardless of the format in which it is held.

Access

- Give individuals access to their information.
- Provide a copy of the information requested, or reasons for not providing access, subject to exceptions set out in law.
- An organization should note any disagreement on the file and advise third parties where appropriate.

Redressability

- Develop simple and easily accessible complaint procedures.
- Inform complainants of their avenues of recourse.
- Investigate all complaints received.
- Take appropriate measures to correct information handling practices and policies.

ATTACHMENT 5
POWERPOINT RE CYBERSECURITY

CYBERSECURITY FOR INDIVIDUALS AND SMALL BUSINESSES IN NEVADA

A RESOURCE FROM THE OFFICE OF THE NEVADA ATTORNEY GENERAL AND THE TECHNOLOGICAL CRIMES ADVISORY BOARD

PRESENTERS

- Information on the presenters

I. TRENDS IN TECHNOLOGICAL ID THEFT AGAINST INDIVIDUALS AND BUSINESS OWNERS

LEGITIMATE SOURCES OF PERSONAL INFORMATION

- Secretary of State
- County Assessor
- County Recorder
- City and County Business License Databases

PERSONAL INFORMATION THAT YOU PUBLISH VOLUNTARILY

- Personal social media accounts (e.g., Facebook)
- Professional social media accounts (e.g., LinkedIn)
- Blogs



SUMMARY OF PUBLICLY AVAILABLE PERSONAL INFORMATION

- Full name, and names of spouse and/or children
- DOBs
- Current and prior residential addresses
- Current and former employers
- Colleges attended, and when you graduated
- Companies and/or businesses that you own or manage, or used to, and their addresses
- Loans and other debts
- Phone numbers
- Email addresses

COMMON METHODS OF CYBER ID THEFT OF ADDITIONAL PERSONAL INFORMATION

- Phone, Mail, or e-mail Scams
- Ransomware and Malware
- Data breaches of Companies with Your PII
- Skimmers
- Good Ol' Fashioned Theft



HOW CRIMINALS USE YOUR INFORMATION

- Open New Accounts in Your Name
- Create Counterfeit Payment Cards Linked to Your Account
- File False Income Tax Returns
- Fraud May Occur Immediately, or in the Future.



TRENDS IN PHONE, MAIL, AND EMAIL SCAMS

- Utilities/IRS phone scam – A person calls you saying your utility will be shut off or that you owe taxes and you will be arrested unless you wire money. There are many variations of this (friend in jail/hospital/stuck overseas/immigration).
- Fake invoices, pay for government documents, directory scams
- Phishing – E-mail message that appears to be from a trustworthy source, but is actually someone trying to obtain your personal information

PROTECT YOURSELF: ALWAYS ASK QUESTIONS

PHONE SCAMS

- Individuals: Don't answer calls from unfamiliar numbers (realize that spoofing is a problem)
- Don't wire money to people you don't know
- Don't be afraid to hang up the phone
- Call an official number from an independent source
- You will always have warning of a power shut off, owed taxes, or pending arrest

DOCUMENT AND DIRECTORY SCAMS

- Many government documents and records are available for free to individuals and businesses. Check online or call and ask.
- Keep good accounting records and train employees on what services to send payments to.
- Sign up for electronic payments and bill pay to trustworthy sources.

PHISHING

- Don't click on links you receive via email; instead, visit the source or pick up the phone.
- Hover over email addresses and links to make sure they don't look fishy
- Businesses: Set a communication protocol, always follow it, and train your employees to do the same

RANSOMWARE AND MALWARE



- Ransomware – malicious software designed to block access to a computer system until a sum of money is paid.
- Malware – malicious software referring to any program harmful to a computer; in this case, stealing sensitive data.

PREVENTION IS THE KEY TO MALWARE

- Update your operating system and other software regularly on all devices (including smart phones)
- Look for secure connections (padlock in the browser and https)
- Use strong passwords (pneumatic devices and mixture of numbers, symbols and letters)
- Use multi-step verification, especially when you regularly sign on to accounts from elsewhere
- Train your employees in safe browsing practices; make strong passwords and multi-step verification a requirement
- Install anti-virus software
- Perform regular back-ups of your data, particularly for businesses



WHAT TO DO AS A RANSOMWARE VICTIM

1. CALL LAW ENFORCEMENT

Contact law enforcement and file a report. It is not likely they will be able to provide you with individual help, but every bit of information is helpful to stop thieves in the future.

2. TURN OFF AND DISCONNECT PC

If the computer is connected to any other device on the network (including smart phones and tablets), it could infect those as well. Take the computer offline and remove it from the network as soon as possible.

3. DON'T PAY THE RANSOM

If you have backed up your information, you will at least have access to that data. Realize that if you decide to pay the thief, it is still unlikely your data will be released back to you. The data may be gone forever.

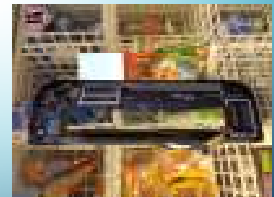
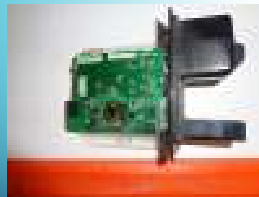
4. Remove the Software: Check out www.nomoreransom.com, a site run by law enforcement and IT companies. You may also want to hire a professional.

II. WHAT SKIMMERS DO AND HOW TO SPOT THEM

SKIMMERS AND IDENTITY THEFT

- A skimmer is a device used to copy payment card numbers and personal identification numbers (PINs). Skimmers are installed at merchant locations, point-of-sale (POS) devices, automated teller machines (ATM), and stand-alone kiosks.
- Most of skimmers are very difficult to spot, even for law enforcement

PICTURES OF SKIMMERS – HENDERSON PD





TIPS FOR SPOTTING ATM SKIMMERS

- ATM skimmers are attached on or around ATMs for the purposes of capturing both the magnetic strip data and the PIN. They are made to be unobtrusive or to mimic legitimate components.
- Inspect the ATM for any signs of tampering. Lightly tug the area of the card slot; some are easily removed. Examine above the PIN pad for a small pinhole camera.
- Look for the following: a card slot that is loose or has fallen off; the presence of double-sided tape, glue, or pry marks around the card slot.
- Look for individuals who are tampering with the machine, who are intentionally covering their faces (with hats and sunglasses), who are spending a large amount of time around the machine without making a transaction, or someone showing up multiple periods of time.

TIPS FOR SPOTTING GAS PUMP SKIMMERS

- Gas pump skimmers can be installed externally over the card reader or internally. Commonly, it is an overlay over the card slot and/or PIN pad. Another device is placed inside the gas pump.
- Inspect the pump for any signs of tampering; business owners should also regularly check inside the pump for anything out of the ordinary.
- Lightly tug the area of the card slot. Like ATM devices, they are usually stuck to the outside with double-sided tape for quick removal.
- Look for similar signs as on the ATM devices: tampering, glue, out of the ordinary tape.

SKIMMERS: MINIMIZING YOUR RISK

- Cover the PIN pad while you enter your PIN. Keep your wits about you when you're at the ATM, and avoid dodgy-looking and standalone cash machines in low-lit areas, if possible. Stick to ATMs that are physically installed in a bank. Stand-alone ATMs are usually easier for thieves to hack into.
- Be especially vigilant when withdrawing cash on the weekends, as thieves tend to install skimming devices on a weekend — 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 or withdrawals immediately.

III. DATA BREACHES: FOR INDIVIDUALS AND SMALL BUSINESSES

RECOVERING FROM DATA BREACHES AND GENERAL CYBER IDENTITY THEFT

DATA BREACHES

- 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.
- Prevention is the key to surviving a data breach (both as an individual consumer and as the breached business)




- Different Breaches Target Different Categories of Information
- Payment Card Data Breaches (e.g. Target, Home Depot)
- User Account Data Breaches (Zappos)
- Medical Information Data Breaches (Anthem)
- Collectively, these breaches have the potential to expose financial account information, email addresses, usernames/passwords, drivers' license numbers, SSNs, healthcare ID numbers, and income data

MINIMIZING YOUR RISK: INDIVIDUALS


- Limit the amount of public information you voluntarily disclose
- Be suspicious of scare tactics
- Order and review your free annual credit reports at <https://www.ftc.gov/faq/consumer-protection/get-my-free-credit-report>
- Fraud alerts and credit freezes
- Monitor your bank accounts regularly
- File tax returns as soon as possible

INDIVIDUALS: RECOVERING FROM A DATA BREACH OR ID THEFT



- Place a fraud alert on your account. To place a fraud alert, contact Experian, TransUnion and Equifax to let them know you are a victim of a data breach or ID theft and would like a fraud alert placed on your credit file. The alert is free and will stay on your credit report for 90 days.
- Order your credit report. You can order one free copy per year from each Credit Bureau at Annualcreditreport.com. Once you have a copy, dispute any errors you find with the credit reporting agency and fraud department of each business.
- Set up a credit freeze, if you are worried about damage to your credit. A credit freeze limits access to your credit and makes it more difficult for a hacker to open an account in your name. A credit freeze will last until you choose to remove it. Keep in mind that a credit freeze will require a fee of approximately \$10.
- Whether you place a fraud alert or a credit freeze on your account, you should still monitor your credit for potential fraud.

NEVADA LAW ON PERSONAL INFORMATION: DEFINITIONS





- Data collector: Any business entity that handles, collects, disseminates or otherwise deals with nonpublic personal information.
- Personal Information (PII): Includes a person's first name or first initial and last name in combination with any one or more of the following: social security number; driver's license, authorization card or ID card number; account number, credit or debit card number, in combination with the security code, access code or password permitting access to the person's financial account; medical or health insurance ID number; or a username or unique identifier in combination with a password, access code, or security question that would permit access to an online account.

NEVADA LAW ON PERSONAL INFORMATION: NRS 603A

- A data collector that maintains records containing the personal information of a NV resident must implement and maintain reasonable security measures to prevent unauthorized access, destruction, use, modification, or disclosure
- Additionally, any business that collects payment card information in connection with the sale of services must comply with the current version of the Payment Card Industry Data Security Standard. Ask your payment card servicer if it is PCI compliant, and familiarize yourself with the guidelines.

PCI IN A NUTSHELL

- The Payment Card Industry Data Security Standard is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.
- The PCI DSS applies to any organization, regardless of size or number of transactions, that accepts, transmits, or stores any card holder data.
- The current PCI Data Security Standard can be found at the PCI Security Council's website at www.pcisecuritystandards.org.
- It is not enough that your third-party payment processor is PCI compliant (although that should be the standard to reduce risk exposure). Your business must also be PCI compliant.

SMALL BUSINESSES AND DATA BREACHES: THE BEST DEFENSE IS A GOOD OFFENSE



- Maintain and follow, without exception, a written data retention policy.
- Have a "crisis management plan" in place, and test it out
- Encryption is key; password and PIN protect EVERY device (don't forget smart phones). Change generic passwords on routers. Have all employees update their passwords regularly, and make sure the passwords are complicated. Use multi-step verification when possible.
- Make servers and files need-to-access: every employee does not need to get to every file
- Review system logs manually or use an automatic tool to check for suspicious activity
- Consider outsourcing your security.

STEPS TO TAKE AFTER A BREACH: SMALL BUSINESS



1. DON'T PANIC

This is when your crisis management plan should spring into effect. Seek an outside forensics team (preferably one you have previously vetted) and legal counsel as soon as possible to guide you through the next steps.

2. LIMIT DATA EXPOSURE AND DETERMINE SCOPE

Make sure you know how to isolate a system without simply turning it off. If the source computer is known, take it off the network. Determine what information was stolen and look for the source of the breach. Do not wipe the servers; this will destroy evidence that could help.






3. NOTIFY STAFF AND LAW ENFORCEMENT


Also alert your insurance company and any business partners. Regularly validate the contact information of these people ahead of time.

STEPS TO TAKE AFTER A BREACH

4. MANAGE THIRD-PARTY CONTRACTS


Ensure that all contracts with third-party service providers, hosting providers, and other relevant parties sufficiently address incident response management. These contracts should allow for your response team to review evidence from those environments.





5. ALERT AFFECTED CLIENTS

Nevada law requires that data collectors disclose a breach to affected victims "in the most expedient time possible and without unreasonable delay." NRS 403A.220(1). The timing should be decided with local law enforcement.



6. TREAT THIS AS A LEARNING EXPERIENCE

Find out where the weakness is, and improve next time.

ANY QUESTIONS?