PCI DSS 4.0 – How it Impacts Your Compliance

CONEXXUS 365

CONEXXUS
solve forward

Your Host:
Casey Brant

Standards Coordinator
Conexxus, Inc.

Your Moderator:
Kara Gunderson

Manager, Payment Card Operations
CITGO Petroleum Corporation

Agenda

- Housekeeping
- About Conexxus
- Presenters
- Presentation
- Q&A

Housekeeping

This webinar is being recorded and will be made available on Conexxus365.org

Participants

- Ask questions via webinar interface
- Please, no vendor specific questions
- Our webinars may be used toward PCI continuing education credits. Please contact 365@conexxus.org for questions regarding a certificate of webinar attendance for qualifying live events.

Interested in speaking or sponsoring a Conexxus365 event?
Contact 365@conexxus.org to discuss upcoming opportunities with our team.

Disclaimer

Conexxus does not endorse any products or services that may be described or mentioned in this presentation.

The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus.

By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.

Thank you to our 2023 Annual Sponsors!

Diamond Sponsors

Acumera

Bulloch TECHNOLOGIES INC. www.bullochtech.com

FORTINET

GILBARCO VEEDER-ROOT

HUGHES An EchoStar Company

K3DES

Mako NETWORKS

NACS

NCR

PDI TECHNOLOGIES

SUCCESS SYSTEMS 800 653 3345

Emerald Sponsors

AvaLAN NETWORKS

DOVER FUELING SOLUTIONS

Bluefin

CENEX

G&M

Kwik Trip

mashgin

RAI

Sagenet CONNECT | MANAGE | PROTECT

Verifone

W. Capra CONSULTING GROUP

Garnet Sponsors

CDE

nouria

STANDARD AI

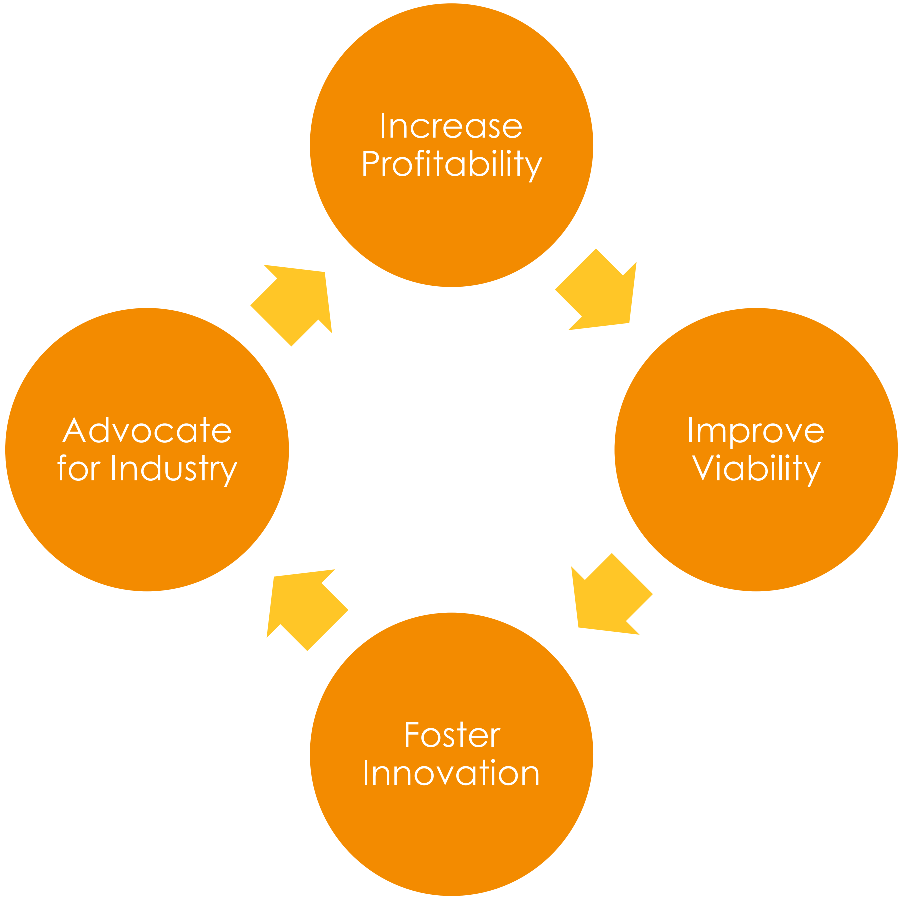
Stuzo

supplyit

TXB WE ARE TEXAS BORN.

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set **standards**…
  - Data exchange
  - Security
  - Mobile commerce
- We provide **vision**
  - Identify emerging tech/trends
- We **advocate** for our industry
  - Technology is policy



Connect with Conexxus

CONEXXUS 365

www.conexxus365.org

365@conexxus.org

CONEXXUS
solve forward

www.conexxus.org

info@conexxus.org

LinkedIn

@conexxus.org

Howard Glavin

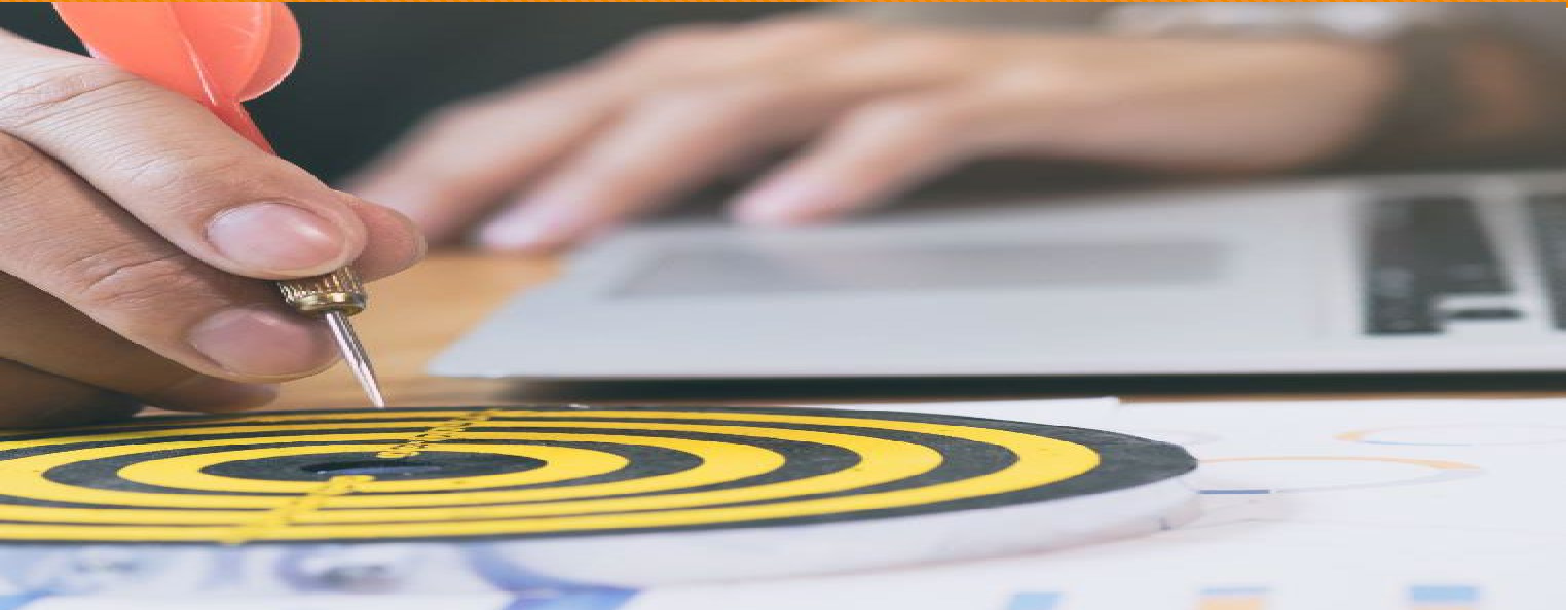
Executive Vice President
K3DES, LLC

PCI DSS 4.0 Impact to Compliance

Everything You Need to Know and Afraid to Ask?- Maybe

Approaching PCI DSS 4.0 Compliance

Hitting the Bulls Eye With Your Compliance Efforts



Transition to PCI DSS 4.0

- Requirements’ general changes
- Form and format changed significantly
- Almost every requirement at the lowest level has a change to it for more clarity and understanding
- The length of the Reports has increased in the number of pages required substantially

Transition to PCI DSS 4.0 cont.

- Requirements’ general changes
- SAQs have also dramatically grown in length
- A new method of Compliance is defined in a Custom Approach (CA)
- The CA requires a great deal more work and documentation and should only be undertaken by a robust organization that has a strong risk-based approach

PCI Alphabet Soup

- The below are common terms used in PCI
  - TRA – Targeted Risk Analysis
  - POI – Point of Interaction Device (POS devices are POIs)
  - NSC – Network Security Controls
  - COTS – Commercial of the shelf for Software
  - FIM – File Integrity Monitoring
  - CIO – Chief Information Officer
  - CISC – IBM Customer Information Control System
  - NSC – Network Security Controls

More PCI Alphabet Soup

- The below are common terms used in PCI
  - IDS/IPS – Intrusion detection/Intrusion protection systems
  - CHD – Cardholder Data
  - CDE – Cardholder Data Environment
  - SAD – Sensitive Authentication Data – Track Data – Security Code
  - INFI – Items Noted for Improvement
  - EOL – End of Life for software and hardware

P2PE POS and POI devices do not totally remove scope

- In both PCI DSS 3.2.1 and 4.0 this industry is of the general belief that the use of P2PE vendor managed PCI POI devices removes all scope form the retailer
  - This is a very bad assumption and is not accurate

Misconception for Retailers in Brick and Mortar Locations (Attended)

- All lot of Retailers that deal in Brick and Mortar believe they can report on SAQ-A or SAQ-A EP or similar reporting format
  - This is a misconception
    - In 99.9% of these cases the Found Card issue will move you to reporting on a SAQ-D
      - You are permitted to mark N/A to those items out of scope for you less the items in requirement 9 to cover the found cards

Misconception for Retailers in Brick and Mortar Locations (Unattended)

- The latest trends is to move to fully unattended retail locations
  - This raise PCI DSS Concerns (3.2.1 and 4.0) for the Inspection of the POS/POI devices in use
  - Fully unattended sites (24 by 7 by 365) will not meet the 3.2.1 requirements for inspection of the POS POI devices and you will fail PCI
  - Further if this is transitioned to PCI DSS 4.0 the TRA and the Inspection requirement will FAIL PCI DSS 4.0 – Skimmers are Real!

Targeted Risk Analysis (TRA)

PCI DSS 4.0 has several Requirements where a TRA is required even when you are not using a Custom Control

The Requirements with TRAs are:

1. 5.2.3.1 Antimalware

Targeted Risk Analysis (TRA)

- 7.2.5.1 User Management – Application and System Accounts
- 8.6.3 User Management – Account Misuse
- 9.5.1.2 POI Inspection
- 10.4.2 Periodic Log Review
- 11.3.1.1 Application Vulnerabilities

Targeted Risk Analysis (TRA)

- 11.6.1 Browser Code protection
- 12.3.1 Review of the TRA to ensure they are still accurate
- 12.3.2 For each Customized Control
- 12.10.4.1 Frequency for Incident Response training
- Appendix E2 shows specific elements for a TRA

Formal Assignment for all 12 Requirements

- PCI DSS 4.0 has a requirement for each of the 12 requirements to be “Formally” assigned
  - This assignment is not generally an IT assignment as many of the requirements individually have significant business impact

Quarterly Scanning (Internal and External)

You must have 4 consecutive passed scans to report, regardless of how many months beyond your reporting date takes place to meet the requirement for

"Four Passed Scans"

Quarterly Scanning (Internal and External)

- PCI DSS 4.0 does, and will not have the FAQ from PCI DSS 3.2.1 that stated a report cannot be withheld if the last scan is a passed scan
  - You MUST have Four Passed Scans

Quarterly Scanning (Internal and External)

- Four Passed Scans coupled with authenticated internal scanning, required by ***31 March 2025***, means it will take a lot of work in advance of this date to resolve ***all*** vulnerabilities this process will find
    - To meet the 31 March 2025 date you need to be running and remediating authenticated scans now

INFI Form Required

- This Items Noted for Improvement form must be completed if a QSA is used for your reporting
- This form replaces the "In Place with Remediation" process
- Even if you do not sign the form the QSA must sign retain
  - Signing is a Attestation – Legal Document
  - This has many Implications that should not be overlooked

Skimmers and POI – POS Devices

Skimmers are the unknown for all stores regardless of P2PE – EMV readers or not

Skimmers are unique in that they are designed to be installed quickly and never attended to again

Skimmers and POI – POS Devices

- Impact of inspection has a heavy effect on unattended stores
- Impact of inspection has a heavy impact on Grab-N-Go sales process with attendant stores
  - Today’s labor market is making staffing very difficult
  - Doing more with less leads to breaches due to skimmers

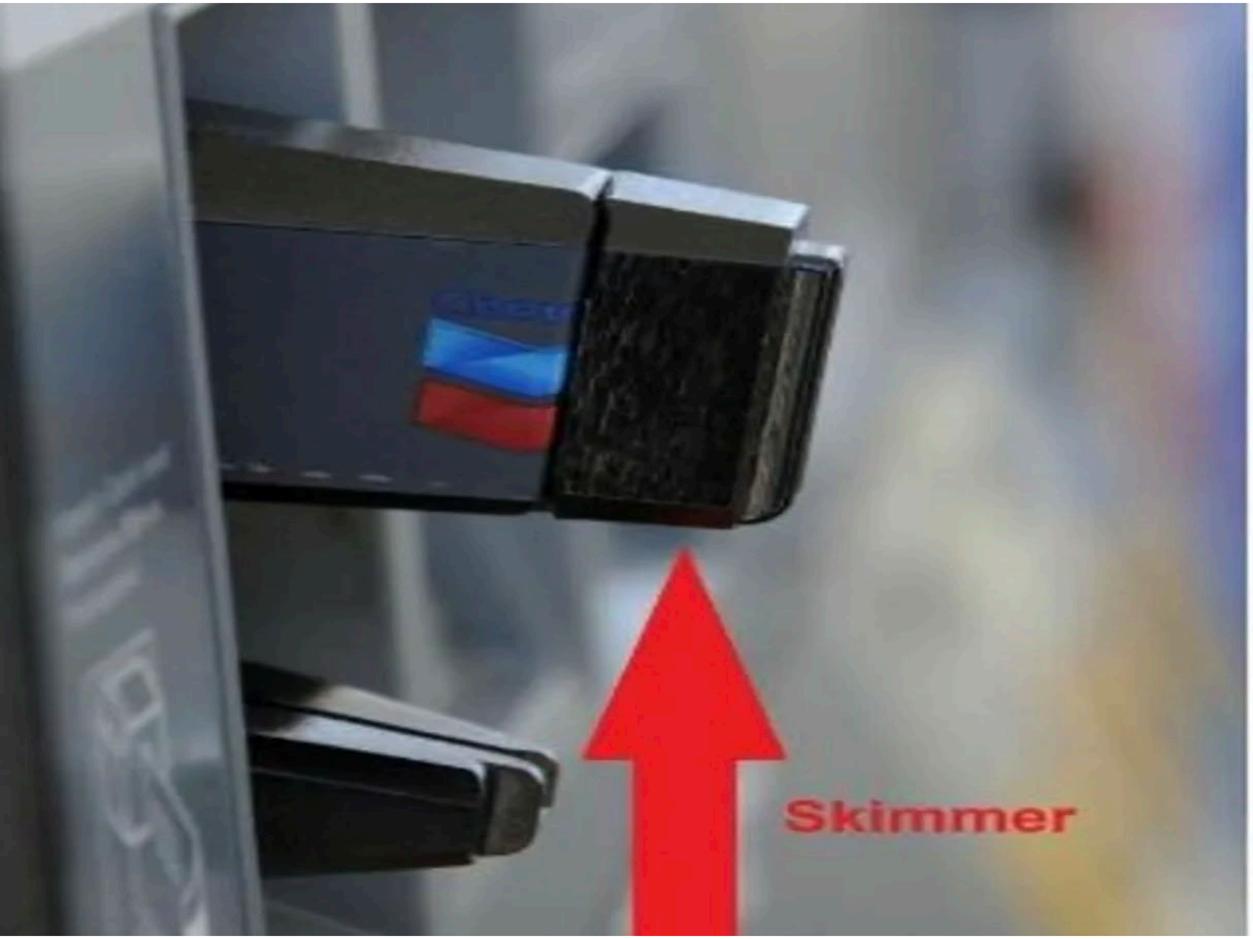
Skimmers and POI – POS Devices

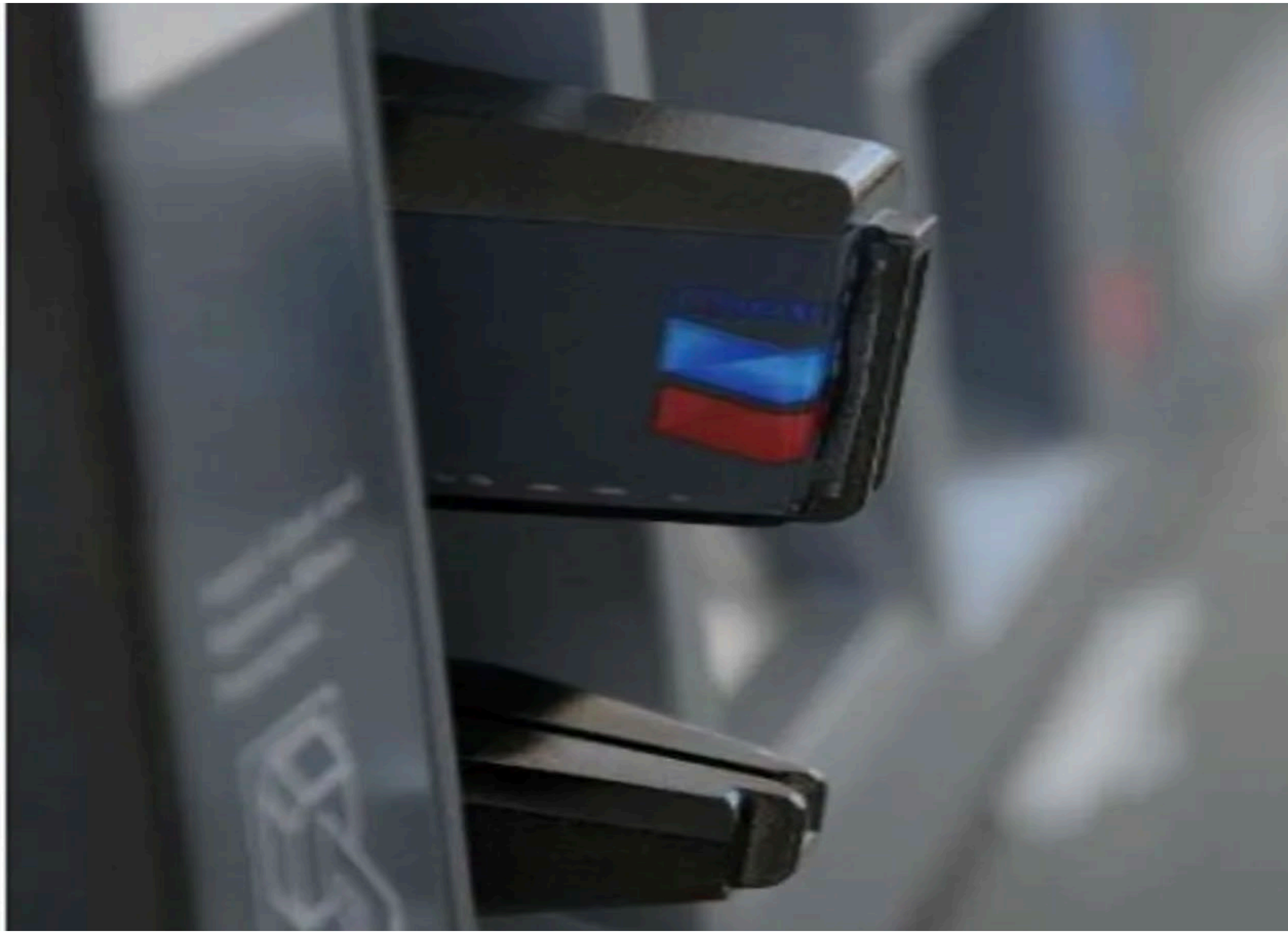
- Skimmers today generally use Bluetooth to pass the data to the installer (Thief)
- Skimmer are designed to replicate the actual POS POI device in use and read the Card being presented just like your device does

Skimmers and POI – POS Devices

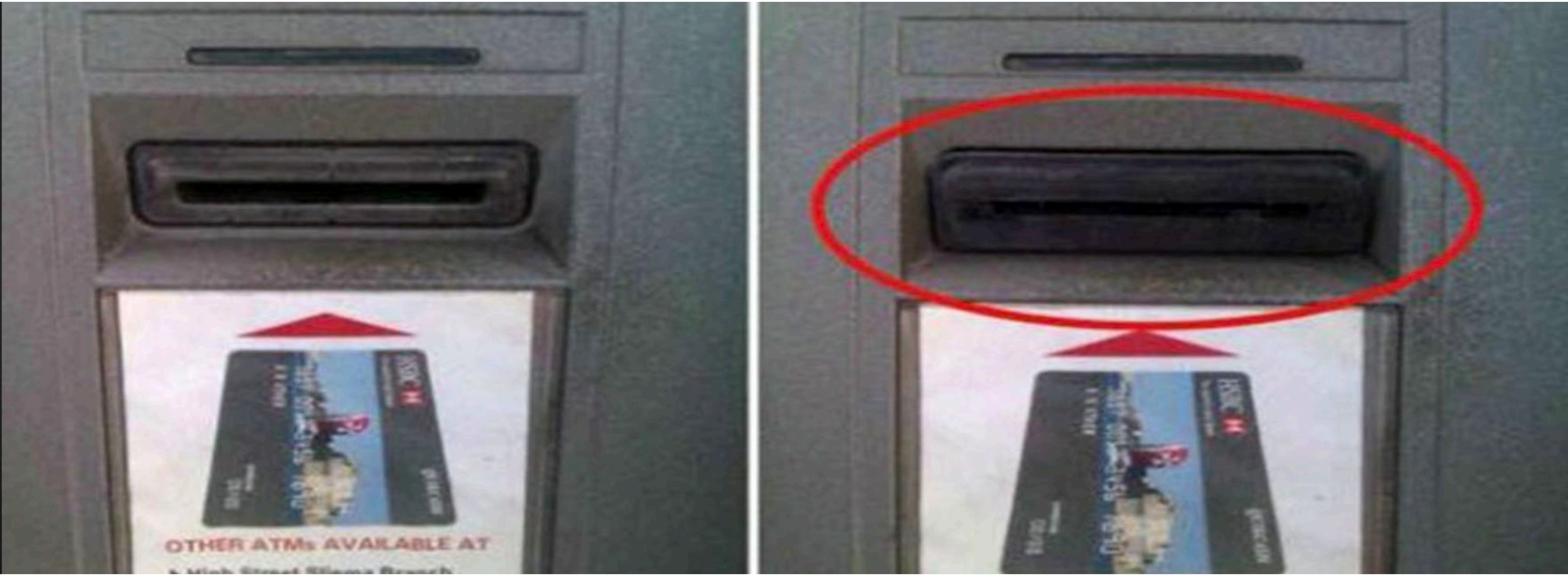
- The following slides give you examples of skimmers
  - Skimmers on pumps
  - Skimmers on POS in stores
  - Skimmers used by staff

Skimmers on Pumps

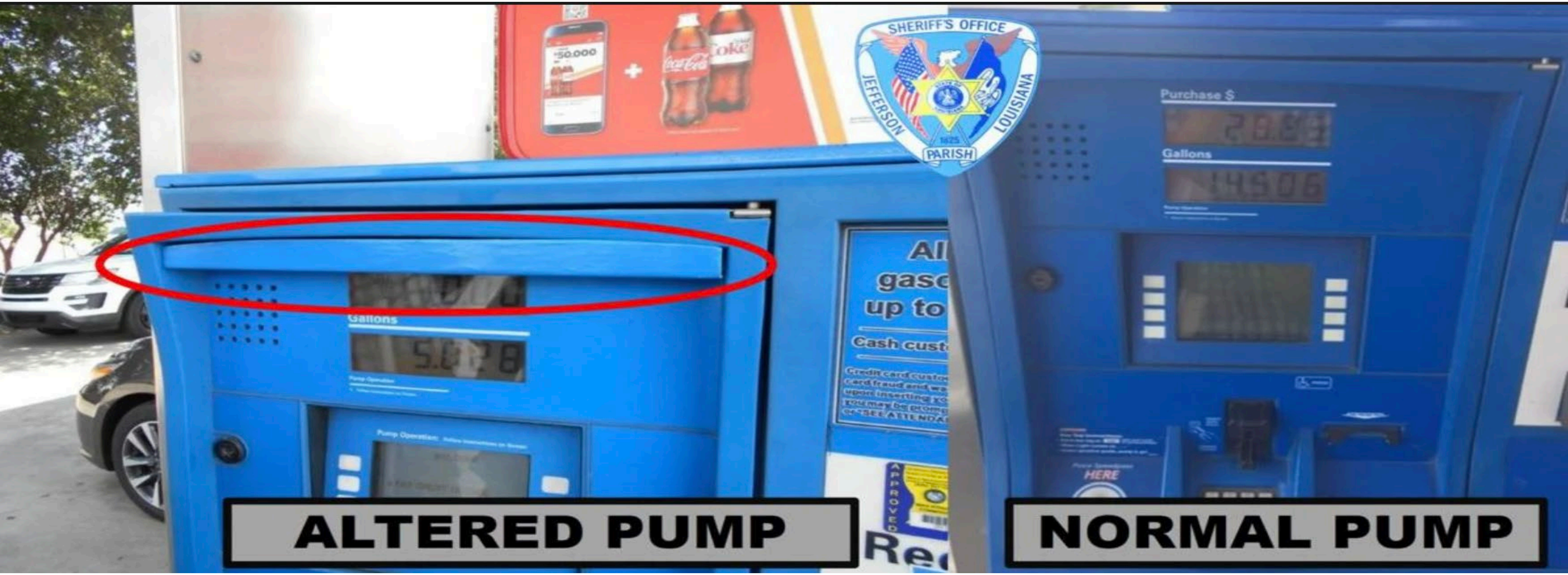




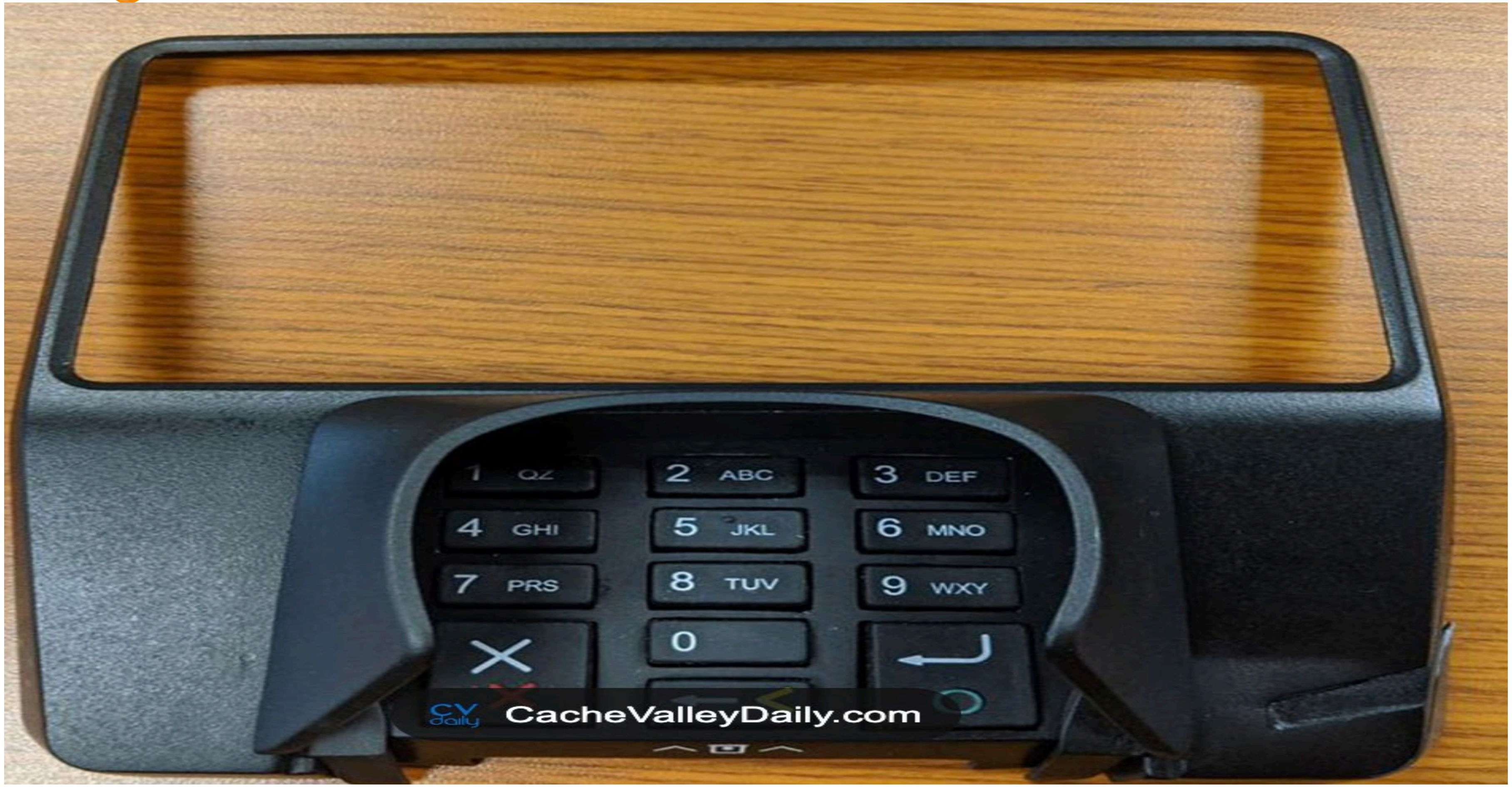
Skimmers on Pumps



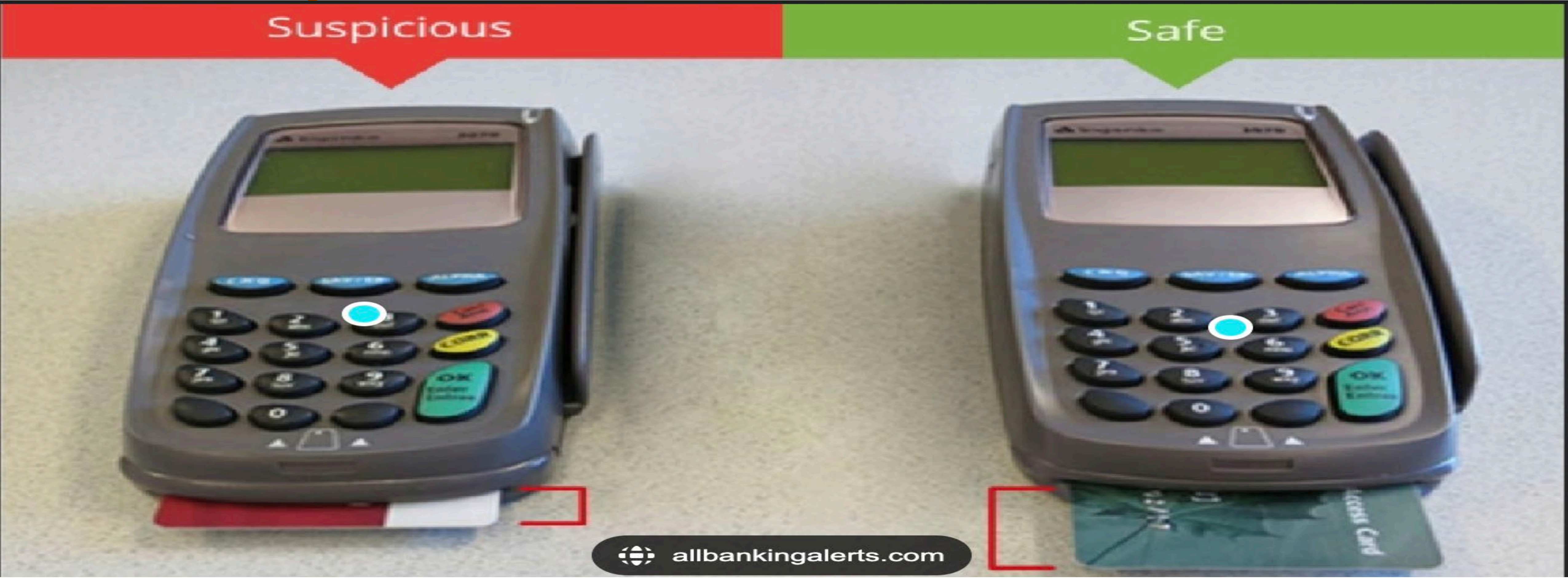
Skimmers on Pumps?



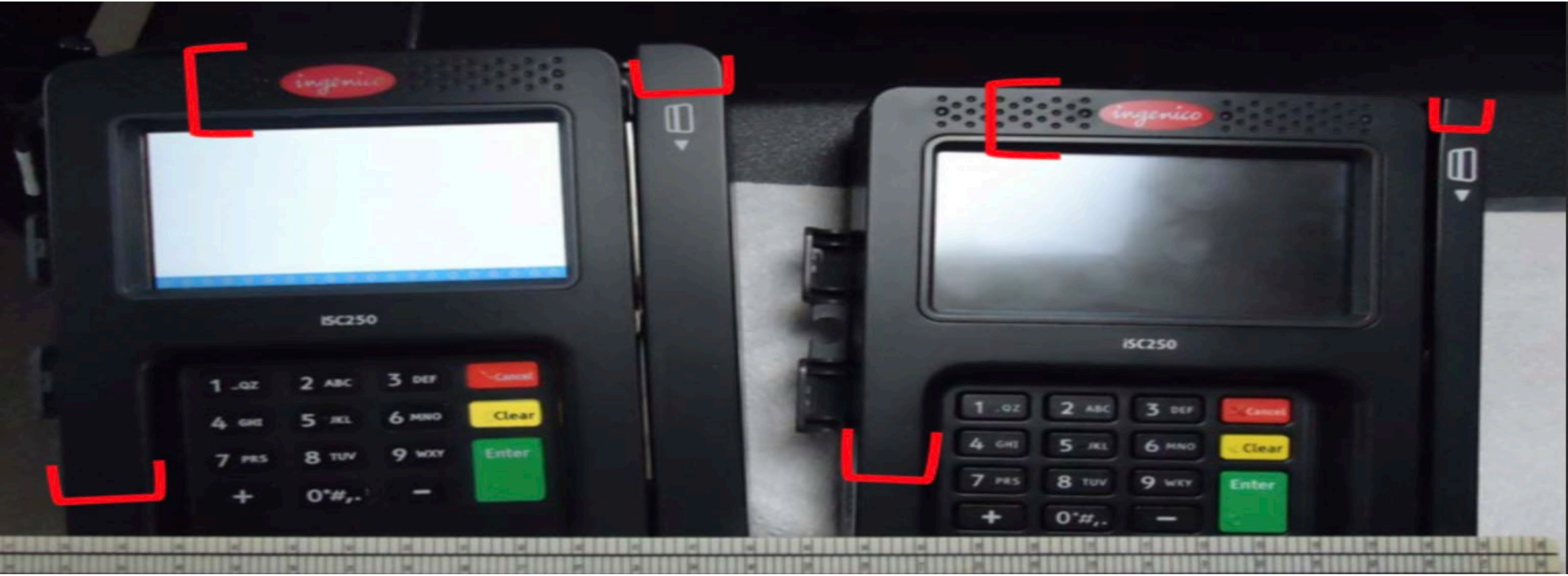
Skimmers for POS Devices in Stores



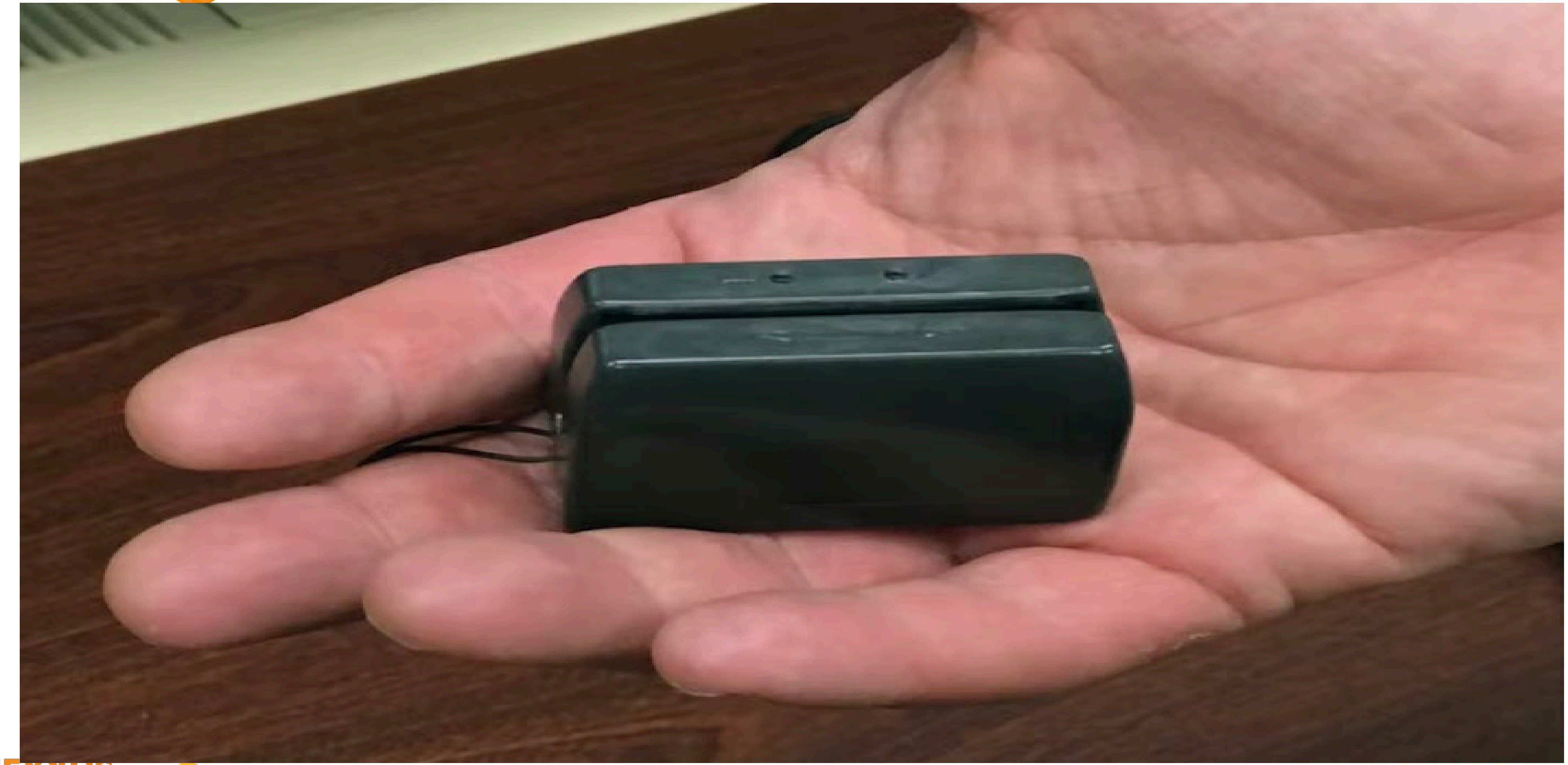
Skimmers for POS devices in Stores?



Skimmers for POS devices in Stores



Skimmers in Stores and at attended Pumps – Used By Staff



Controllers and Back Office

- The network equipment and related POS POI connection Points generally take place in the back office
- This area is generally a Managers Office, Storage room, or Break area
  - These devices can also be under the counter

What Does Your Store Network Look like for Physical Devices

- Do you have the controllers under the counter unprotected
- Do you have the controllers in the back office exposed to anyone who enters
- Impact of both of the above has a lot of overhead and can be removed by a simple locked rack in reducing scope

Controllers and Back Office

- If these devices are in the open (Office or Under the Counter) then you must:
  - Log all entry and exit with a lot of detail
  - Inspect the devices for tampering which most staff have no clue on how to do this and would take away from customer service

Controllers and Back Office

- The best way to take this area out of PCI scope is to put the IT devices in a wall or floor mounted LOCKED rack designed for this type of equipment.
  - Reduces the need for logging to the rack alone
  - Reduces the scope to just the rack entry

Reviewing the Significant Changes by Requirement

- The next series of slides will walk through the significant changes to the requirements from PCI DSS 3.2.1 to PCI DSS 4.0
  - These slides do not cover all of the changes just the ones with heavy impact to your work world
  - There are other changes that have impact as well depending on your business model

Requirement 1; Install and Maintain Network Security Controls (NCS)

- Language changed to more clearly apply to the cloud environment
- Ownership Formally assigned
- NSC used to describe Security Controls

Requirement 2; Apply Secure Configuration to All System Components

- Updates are focused on making clear that hardening controls (CIS Benchmarks for example) must be applied to all system components, not just network gear and servers
- 2.2.6 Insecure services/daemons and protocols have been moved to the hardening section for the business justification if used

Requirement 3; Protect Stored Account Data

- 3.3.2 SAD must be encrypted prior to authorization
  - This is Store and Forward mentioned previously
  - This will generally require application changes to meet this requirement

Requirement 3; Protect Stored Account Data

- 3.4.2 The ability to copy and paste PAN must be disabled by default with remote-access methods (SSH/RDP)
  - This is a high impact for places like call centers that use the Sticky Notes app for placing PAN into fields more than once

Requirement 3; Protect Stored Account Data

- 3.5.1.2 Disk and partition-level encryption may not be used as a control (except in removable media)
    - Absolute requirement for field level encryption on top of disk encryption

Requirement 3; Protect Stored Account Data

- 3.6.1.1 Encryption Keys may not be shared between test and production environments
  - This is for the companies with their own development shop in house or under contract for the most part

Requirement 4; Protect Cardholder Data with Strong Cryptography

- This covers open public networks
  - Open Public Networks are in part the Internet, Cellular, HF radio, Wireless (802.11.X) and other communications
- 4.2.1.1 New requirement for an inventory of keys and certificates used in transmission

Requirement 4; Protect Cardholder Data with Strong Cryptography

- When the reference is on certificates, it includes **ALL** certificates both internal and external along with self signed
- Self Signed certificates are permitted with provable independence from the user and/or installer of the certificate and proof they are using strong cryptography
  - NIST 800-52 is the source for strong cryptography

Requirement 5; Protect All Systems and Networks from Malicious Software

- 5.2.1 Clarifies that controls are around both networks and software protection from malicious software (rootkits, viruses, keyloggers, links, etc.)
- TRAs are required for the frequency of checking to see if equipment now need Antimalware – 5.2.3.1

Requirement 5; Protect All Systems and Networks from Malicious Software

- 5.3.3 Permits persistent behavioral analysis in place of “periodic scans”
- 5.3.3 Antimalware solution must include coverage for removable media (USBs, external drives, etc.)
- Note: All antimalware used must have automated anti-phishing capabilities

Requirement 6; Develop and Maintain Secure Systems and Software

- 6.1.1 Changes require to be documented, kept up to-date, used, and known to **all** affected parties
- 6.2 Now includes all software and not just those that are web facing.
  - COTS customized, and/or purposefully built from a third party and any Bespoke Software

Requirement 6; Develop and Maintain Secure Systems and Software

- 6.2.2 now includes the use of tools for detecting vulnerabilities in developed software
  - Tools are depending on the language used for the code

Requirement 6; Develop and Maintain Secure Systems and Software

- 6.3.1 covers vulnerabilities in Bespoke software, APIs, operating systems, and databases
  - Requires risk ranking assigned to each vulnerability
  - Meets the TRA for this activity

Requirement 6; Develop and Maintain Secure Systems and Software

- **6.4.1** For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows:
- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:
  - At least once every 12 months and after significant changes.
  - By an entity that specializes in application security.
  - Including, at a minimum, all common software attacks in Requirement 6.2.4.
  - All vulnerabilities are ranked in accordance with requirement 6.3.1.
  - All vulnerabilities are corrected.
  - The application is re-evaluated after the corrections
- Or

Requirement 6; Develop and Maintain Secure Systems and Software

- Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows:
  - Installed in front of public-facing web applications to detect and prevent web-based attacks.
  - Actively running and up to date as applicable.
  - Generating audit logs.
  - Configured to either block web-based attacks or generate an alert that is immediately investigated.
- **Note:** This requirement will be **superseded** by Requirement 6.4.2 after **31 March 2025** when Requirement 6.4.2 becomes effective.

Requirement 6; Develop and Maintain Secure Systems and Software

- 6.4.3 An inventory of all scripts is maintained with written justification as to why each is necessary
  - This covers ALL iFrames, Java Scripts, SQL scripts, Started Tasks, ,CICS, Etc.

Requirement 7; Restrict Access to System Components and Cardholder Data

- 7.1.1 Changes require to be documented, kept up to-date, used, and known to **all** affected parties
- 7.2.5.1 Requires a Risk Assessment for periodic review for this activity to review the access grants
- 7.3 Requires all access to be Roles based and reviewed for all types of access (Application – Started Tasks – Stored Procedures – Service Accounts – Etc.)

Requirement 8; Identify Users and Authenticate Access to System Components

- 8.1 Changes require to be documented, kept up to-date, used, and known to **all** affected parties
- 8.1.2 Requires the roles to be fully defined and the use of RBAC (Role-Based Access Control), not access to an individual user.
- 8.2.2 Address the exceptional use of shared and generic IDs which was not permitted in 3.2.1

Requirement 8; Identify Users and Authenticate Access to System Components

- 8.2.3 For Service Providers only – Requires unique credentials for each customer
- 8.3.6 This implies If passwords or passphrases are not used, there is a possibility of other forms of authentication for users to access the systems in a secure method
- Non Repudiation Systems are permitted

Requirement 8; Identify Users and Authenticate Access to System Components

- If passwords or passphrases are used, the length should be a minimum of 12, as long as the system supports this length and changes from minimum length of 7 characters in version 3.2.1
- 8.3.10 Service Providers must provide guidance to their customers on how to manage their user passwords, specifically on the period of password change. The effective date for this is 31 March 2025

Requirement 8; Identify Users and Authenticate Access to System Components

- 8.3.11 If authentication factors are used, for e.g. physical or logical tokens, smart cards, or certificates, these must be individually assigned and not to group or shared IDs
- 8.4.2 Multi-Factor Authentication (MFA) – the effective date for this is 31 March 2025
  - Covers all users and administrators for remote network access
  - Covers all customers of Service Providers

Requirement 8; Identify Users and Authenticate Access to System Components

- 8.5.1 MFA configured to prevent misuse (session cookies is an example of how to exploit).
  - Cannot be bypassed except for a specific need for a short period of time and fully documents as to the need and reason
- 8.6.1 Application, and System accounts and associated authentication factors are strictly managed (Covers Service Accounts capable of use by humans) (Required 31 March 2025)

Requirement 9; Restrict Physical Access to Cardholder Data

- 9.2.1.1 Entry and exit points to CHD areas are monitored. This has been updated from the PCI DSS version 3.2.1 to cover tamper protection for all devices doing the monitoring
- 9.3.2 Visitors MUST be escorted at all times within the CDE areas
- 9.5 has been established for POI/POS devices tamper protection which can be validated by the local store or place of use

Requirement 10; Log and Monitor All Access to System Components and Cardholder Data

- 10.1 Changes require to be documented, kept up to-date, used, and known to **all** affected parties
- 10.2 Requires the audit logs to be implemented to support detection of anomalies and suspicious activity, and the forensic analysis

Requirement 10; Log and Monitor All Access to System Components and Cardholder Data

- 10.2.2 Covers what should be part of the audit log captures
- 10.4.1 Requires daily log reviews for all security events, system logs within the CDE, all critical systems and servers used in the CDE
  - Automated review required

Requirement 10; Log and Monitor All Access to System Components and Cardholder Data

- 10.7 Failures of critical security controls are required to be logged and reported. They also require a response
- 10.7.1 For Service Providers, logs should be on IDS/IPS, FIM, Antimalware, Physical Access, Logical Access controls, Audit Logging Mechanisms, and Segmentation Controls

Requirement 11; Test Security of Systems and Networks Regularly

- 11.2.2 Requires an inventory of ALL authorized wireless access points to be maintained, including the business justification
- 11.3.1.1 Requires all vulnerabilities ranked below critical and high to be addressed per companies' risk ranking. This is mandatory effective 31 March 2025

Requirement 11; Test Security of Systems and Networks Regularly

- 11.3.1.2 Requires all vulnerability scans to be run as authenticated scans.
  - This is a big deal for most companies
  - This is mandatory effective 31 March 2025
- 11.3.1.3 Requires vulnerability scans to be run after any significant change

Requirement 11; Test Security of Systems and Networks Regularly

- Authenticated Scanning for Internal Scanning
  - Example if workstations connect to the CDE or can impact the CDE scanning is required
  - Do not loose site of the impact of Authenticated Scans. This type of scanning generally finds vulnerabilities at the 100 times or more level of an unauthenticated Scan

Requirement 11; Test Security of Systems and Networks Regularly

- 11.3.2 External vulnerability scans are not eligible for a custom approach
- 11.4 Penetration testing does permit a custom approach
- 11.6 Requires unauthorized changes to the payment pages are detected and responded to

Requirement 12; Support Information Security with Organizational Policies and Programs

- 12.1.4 Responsibility for information security is formally assigned to the CIO or other security knowledgeable executive management
- 12.3.4 Hardware and software technologies are reviewed to ensure they have patches still available and are under support. No EOL in Production
  - The mandatory date is 31 March 2025.

Requirement 12; Support Information Security with Organizational Policies and Programs

- 12.5 Hardware, software, scripts, service accounts, library calls, CISC started tasks, physical, logical, cloud, Roles etc.
  - Service providers must confirm all above data every six months
- 12.6.2 Security awareness program is reviewed every 12 months and updated to meet the current needs. This is mandatory effective 31 March 2025

Requirement 12; Support Information Security with Organizational Policies and Programs

- 12.6.3.1 Security awareness program covers threats and vulnerabilities that could impact CHD including but not limited to
  - Phishing
  - Social engineering

Requirement 12; Support Information Security with Organizational Policies and Programs

- 12.8 Third party risk and Third Party Service Providers (TPSP) are managed by a program for all CHD shared data
  - Requires written agreements with all companies meeting this threshold

Requirement 12; Support Information Security with Organizational Policies and Programs

- TPSP must have agreements on what they are required to do in writing and monitored every 12 months
- 12.8.5 Each TPSP must document each requirement they are responsible for (Responsibility Matrix)

Appendix D; Customized Approach

- Generally is not considered for use in this industry due to the sophistication and staffing required to implement.
  - The full Custom Approach MUST be in place and working prior to the start of the assessment
  - Testing of a Custom Approach is similar to a SOC audit and requires a great deal of time and staff involvement

Howard’s Contact Data

Howard Glavin

EVP K3DES, LLC

+1 904.631.9204 Mobile

+1 904.287.2212 FAX

Howard.Glavin@k3des.com

Stay Tuned for

Q&A