

Protecting Payments Throughout the Ecosystem

Emma Sutcliffe

Senior Director, Data Security Standards
PCI Security Standards Council



PCI Security Standards Council

- *Founded in 2006*
- *Guiding open standards for payment card security*



Role of PCI SSC

Standards, Best Practices & Services



Payment **Equipment**



Payment **Software**



Merchant & Service
Provider **Environments**

Validation & Qualification – Equipment, Services, Assessors, Investigators

Training – Merchants, Assessors, Acquirers, Integrators

Understanding the Ecosystem





Emerging Payment Technologies

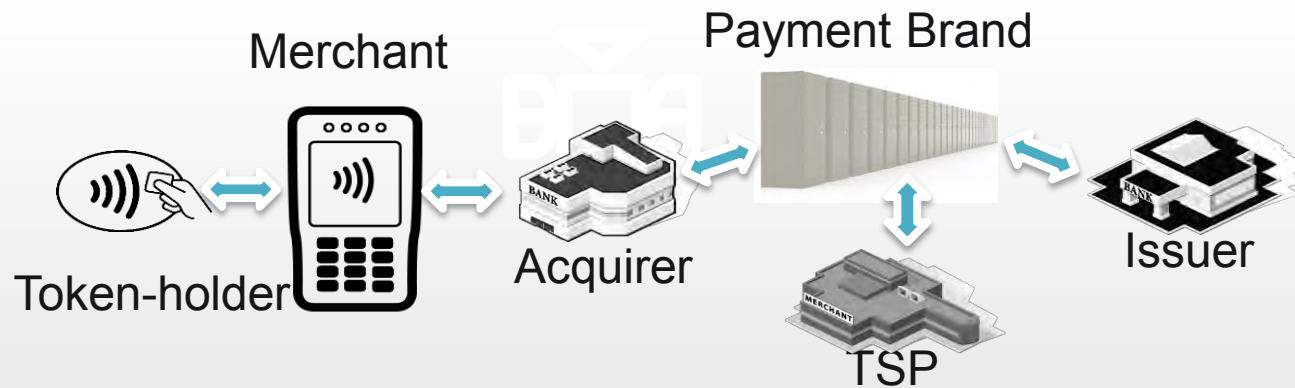
Mobile Technologies

- PCI DSS
 - Requirements applicable to mobile and other technologies as they emerge
- PA-DSS
 - Payment applications running on mobile hardware dedicated to payment acceptance
- Point-to-Point Encryption (P2PE)
 - PCI-listed P2PE solutions using PTS approved mobile PEDs



Token Service Provider (TSP)

- New standard to address Token Service Provider environments
 - Requirements for securing environments where payment tokens are generated / issued
- Token Service Provider defined by EMVCo



Mobile Provisioning Security Requirements

- Addendum to the Card Production standard
- Physical and Logical Security Requirements for vendors that:
 - › Perform cloud-based (host card emulation) or secure element (SE) provisioning services;
 - › Manage over-the-air (OTA) personalization, lifecycle management, and preparation of personalization data; or
 - › Manage associated cryptographic keys



EMV Chip

- **EMV Chip reduces face-to-face counterfeit fraud**
- **EMV Chip Needs PCI**



Common Goal: Devalue Data




EMV

Point-to-Point Encryption

Tokenization

A Holistic Approach

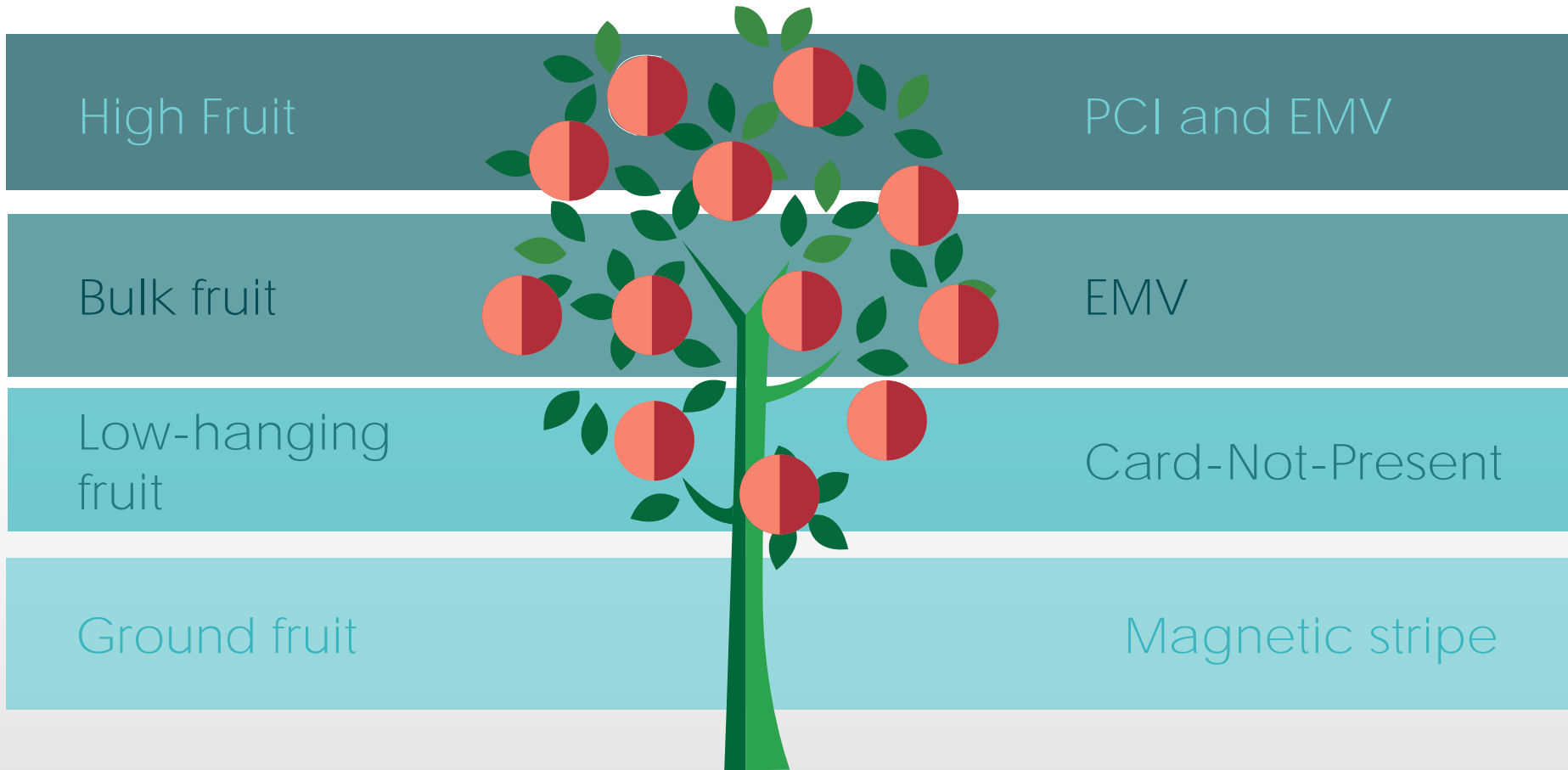
	Prevents counterfeit fraud of exposed data?	Protects data in transit?	Protects data at rest?
EMV Chip only	✓	✗	✗
Encryption + Tokenization	✗	✓	✓
EMV Chip + Encryption + Tokenization	✓	✓	✓



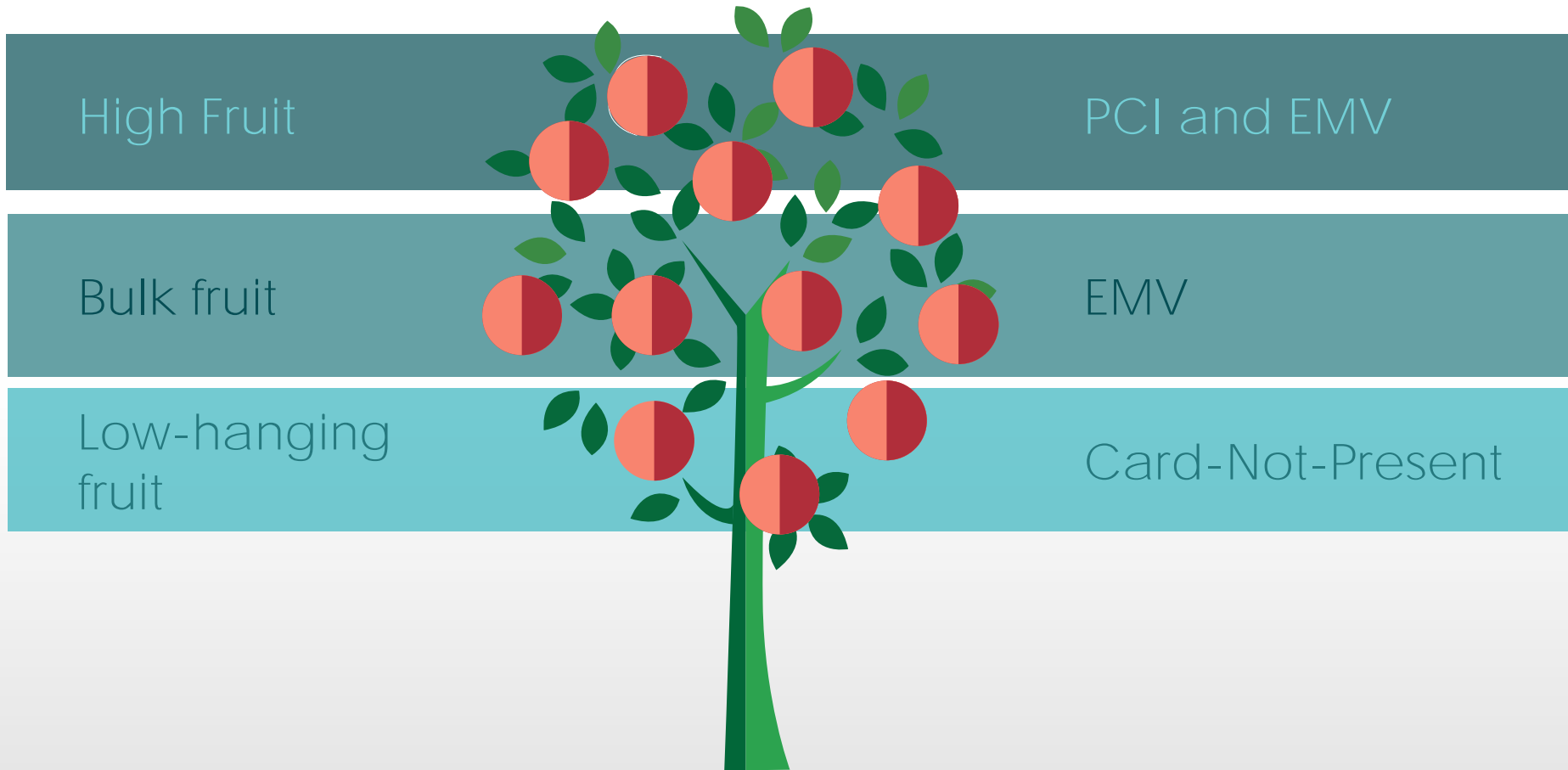


The Move to EMV

The Security Fruit Tree



The Security Fruit Tree after EMV migration



Global Trends

Canada



— Counterfeit and Lost/Stolen
— CNP

UK



Source: Financial Fraud Action UK

According to Aite Group, CNP fraud in the U.S. is projected to double by 2018 to \$6.4 billion



E-Commerce Security

Threats to E-Commerce

- E-commerce systems targeted to steal data
- Data stolen elsewhere used for e-commerce fraud



Protecting E-Commerce

E-Commerce systems as a target

- Controls that prevent, detect, & respond to threats
- PCI security standards

Common Implementations



Data capture on merchant website



Direct Post



iFrame



URL Redirect

PCI DSS v3.2 SAQ Updates

- Merchant web servers that perform redirect continue to be highly targeted
- Basic security controls not being applied.
- SAQs A and A-EP include new requirements to help organizations address this threat.

SAQ A

- Change default passwords and implement an incident response plan
- Implement basic authentication controls, such as a unique user ID and strong password

SAQ A-EP

- Added requirements related to secure configuration of the webserver and network, access controls, authentication, and audit logs
- Additional process/policy requirements

Protecting E-Commerce

E-Commerce systems as a target

- Controls that prevent, detect, & respond to threats
- PCI security standards

Protecting E-Commerce

E-Commerce systems as a target

- Controls that prevent, detect, & respond to threats
- PCI security standards

E-commerce used for fraudulent transactions

- Fraud detection and modelling
- Cardholder authentication

3-D Secure

- Collaboration with EMVCo
- Supports EMV® 3-D Secure 2.0 Specification
- Cardholder authentication for e-commerce and connected devices, including in-app purchases





Securing Telephone Payments

Telephone Recordings Containing PAN/SAD

- PCI DSS applies to audio recordings
- Methods are available to prevent storage of PAN/SAD
- Consider people, process, technology





Securing Software

Securing Software

- Software development is continuous
- The threat is continuous
- Application security must also be continuous





Promoting a Security Mindset

Compliance AND Security

- Security is a 24x7 mentality
- Not a “check-the-box” once a year and done



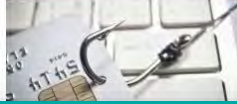


PCI Resources

Guidance Documents

Defending Against Phishing & Social Engineering Attacks A Resource Guide from the PCI Security Standards Council

Hackers use **phishing and other social engineering** methods to target organisations with legitimate-looking emails and social media messages that **trick users into providing confidential data**, such as credit card number, social security number, account number or password. These attacks are at the heart of many of today's most serious cyberattacks and **can put your business and your customers at risk**. With a few security basics and ongoing vigilance, businesses can be aware and defend against these attacks.



UNDERSTAND THE COST = THEFT + OF CUSTOMER DATA

On average, cybercriminals cost companies per attack:

Country	Cost per attack
JAPAN	US\$ 8,19M
GERMANY	US\$ 8,13M
U.S.A.	US\$ 12,6M

13% of annual cybercrime cost for companies is due to phishing and social engineering.

Skimming

A Resource Guide from the PCI Security Standards Council

WHAT IS SKIMMING?

Skimming is copying payment card numbers and personal identification numbers (PINs) and using them to make counterfeit cards, siphon money from bank accounts and make fraudulent purchases.

Criminals install equipment at merchant locations, on portable POS devices, automated teller machines (ATM), and kiosks that captures the information from the magnetic strip.

FACTS & FIGURES

- \$2 billion: The estimated global cost of skimming*
- \$50,000: The average loss from skimming crime*
- Skimming-related counterfeit card fraud is the leading type of third-party card fraud*
- Skimming is the #1 ATM crime globally making up 92% of all attacks at the ATM*
- From Jan-Apr 2015, the number of attacks on debit cards used at ATMs reached the highest level for that period in at least 25 years*

HOW HACKERS TRICK YOU

RECONNAISSANCE

- Information gathering for various online sources and networking sites
- Business applications and IoT

IN-DEPTH BACKGROUND MATERIALS

- Skimming Prevention - Overview of Best Practices for Merchants
- Skimming Prevention - Best Practices for Merchants
- ATM Security Guidelines

RELATED INDUSTRY RESOURCES

- Skimming the Surface
- All About Skimmers
- Skimming is a Scam

*All amounts are in U.S. Dollars.

© 2015 PCI Security Standards Council LLC. www.pcisecuritystandards.org

- Building a security awareness program
- Protecting against malware
- Skimming prevention
- Defending against phishing attacks
- Working with third parties
- Maintaining PCI DSS compliance
- Accepting payments with a mobile devices
- *Coming Soon: Securing E-Commerce*

Small Merchant Guidance

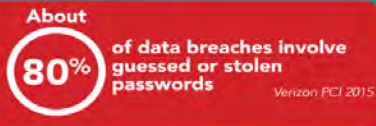
Small businesses globally are a prime target for cybercriminals.

DON'T LEAVE YOUR BUSINESS OPEN TO ATTACK

When your payment card data is breached, the fallout can strike quickly. Your customers lose trust in your ability to protect their personal information. They take their business elsewhere. There are potential financial penalties and damages from lawsuits, and your business may lose the ability to accept payment cards. A survey of 1,015 small and medium businesses found 60% of those breached close in six months. (NCSA)



Computer equipment and software out of the box often come with default (preset) passwords such as "password" or "admin," which are commonly known by hackers and are a frequent source of small merchant breaches.



Software often has flaws or mistakes made by programmers when they write the code, also called security holes, bugs or vulnerabilities. Hackers exploit these mistakes to break into your computer and steal payment data.



Your data is vulnerable when it travels to your bank, and when it's kept or stored on your computers and devices.



Start protecting your business today with these security basics:

- Use strong passwords and change default ones
- Protect your card data and only store what you need
- Inspect payment terminals for tampering
- Install patches from your vendors
- Use trusted business partners and know how to contact them
- Protect in-house access to your card data
- Don't give hackers easy access to your systems
- Use anti-virus software
- Scan for vulnerabilities and fix issues
- Use secure payment terminals and solutions
- Protect your business from the Internet
- For the best protection, make your data useless to criminals



#PCISMB

Copyright 2016 PCI Security Standards Council, LLC. All Rights Reserved.

For more information on how you can protect your business, download the *Small Merchant Guide to Safe Payments*.
https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf

FAQs

- New FAQs regularly added
 - › PCI DSS v3.2 transition dates
 - › SAQ eligibility
 - › Multi-factor authentication
 - › Migration dates for SSL/early TLS
- RSS Feed available

The screenshot shows the 'FREQUENTLY ASKED QUESTIONS' page on the PCI Security Standards Council website. The page features a navigation bar with links for PCI Security, Assessors & Solutions, Document Library, Training & Qualification, About Us, Get Involved, and FAQs. Below the navigation bar is a search bar for FAQs and a link to 'Have a specific Question? Contact Us'. A 'SUBMIT' button is located next to the search bar. Below the search bar is a category dropdown menu set to '- ALL CATEGORIES -'. At the bottom right, there is a pagination link: 'Page: << 1 2 3 >>'. The main content area is a table with three columns: 'ARTICLE NUMBER', 'NEWLY ADDED', and 'DATE UPDATED'. The table lists five articles with their respective article numbers, titles, and update dates.

ARTICLE NUMBER	NEWLY ADDED	DATE UPDATED
1438	How is the payment page determined for SAQ A merchants using iframe?	Sep 2016
1441	How do the updated SSL/early TLS migration dates apply to service providers?	Sep 2016
1440	Does PCI DSS Appendix A2 apply only to Requirements 2.2.3, 2.3 and 4.1?	Sep 2016
1439	How do PCI DSS Requirements 2 and 8 apply to SAQ A merchants?	Sep 2016
1435	What is the Council's guidance on the use of SHA-1?	Aug 2016



www.pcisecuritystandards.org/faq



Thank you