svb

Silicon Valley Bank

# PCI Risks and Compliance Considerations

July 21, 2015

Stephen Ramminger, Senior Business Operations Manager, ControlScan
Jon Uyterlinde, Product Manager, Merchant Services, SVB

# Agenda

1. Introduction
2. Card Compromise Trends
3. Europay, MasterCard, and Visa (EMV)
4. Payment Card Industry (PCI) Basics
5. Compliance
6. Best Practices
7. Next Steps
8. Q & A

# Is your company PCI compliant?

- ❑ Yes
- ❑ No
- ❑ No, but we've started

# If you're not compliant, why not?

- ❑ Too complicated
- ❑ Don't have the time
- ❑ Not sure we need it yet

# About ControlScan

- Delivers **security and compliance services** to more than **a million small and mid-sized businesses globally**.
- **Work directly with companies**, and through more than **150 active partnerships** with Acquirers, ISOs and other service providers that represent portfolios of **2M+ businesses.**
- Specialize in provision of **world class, no limits compliance support and education** that enables SMBs to meet security and compliance standards.

**Compliance Solutions**

- PCI DSS, HIPPA, EI3PA Compliance Solutions
- PCI Self-Assessment Questionnaire (SAQ)
- External ASV Vulnerability Scanning
- Breach Protection

**Managed Security Services**

- Managed Network Firewall and Unified Threat Management Services
- Internal Vulnerability Scanning
- Managed Web Application Firewall
- Mobile Scanning and Mobile Device Management

**Security Consulting Services**

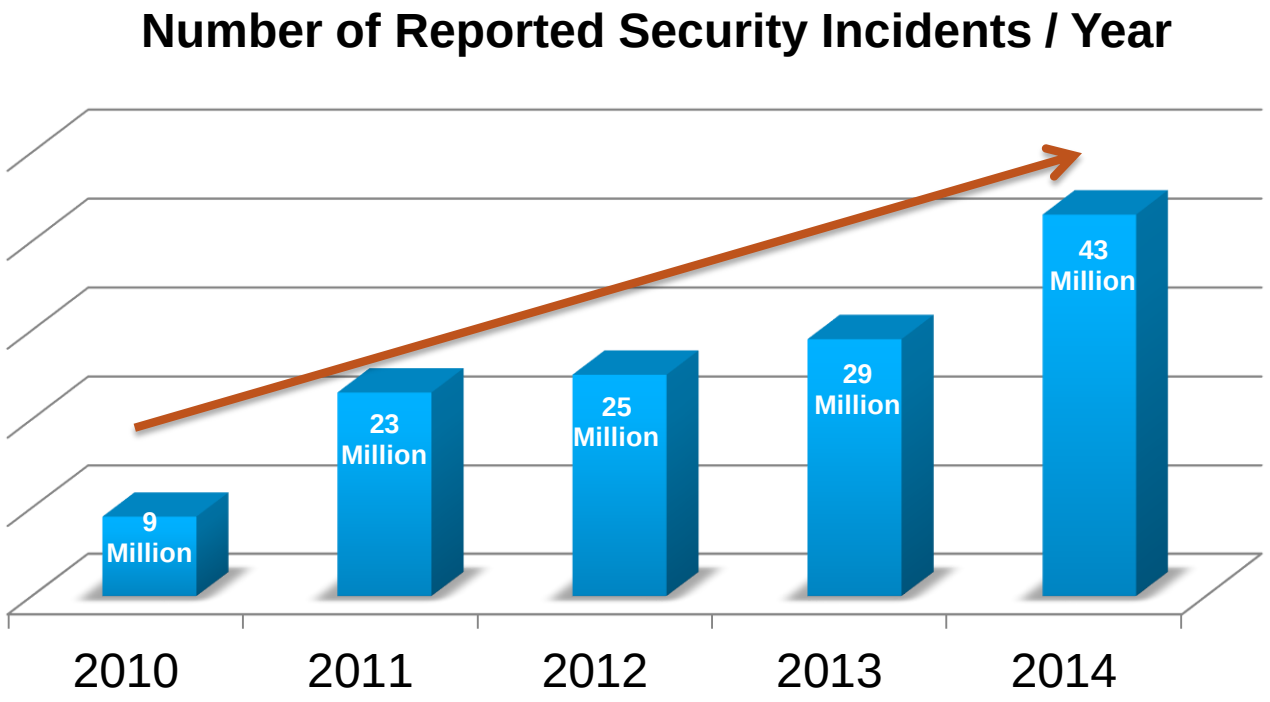
- Network & Web Application Penetration Testing
- Gap Analyses
- Full 'Report on Compliance' Audits
- QSA- led Consulting and Advisory Services

ControlScan is not affiliated with SVB Financial Group

# Card Compromise Trends

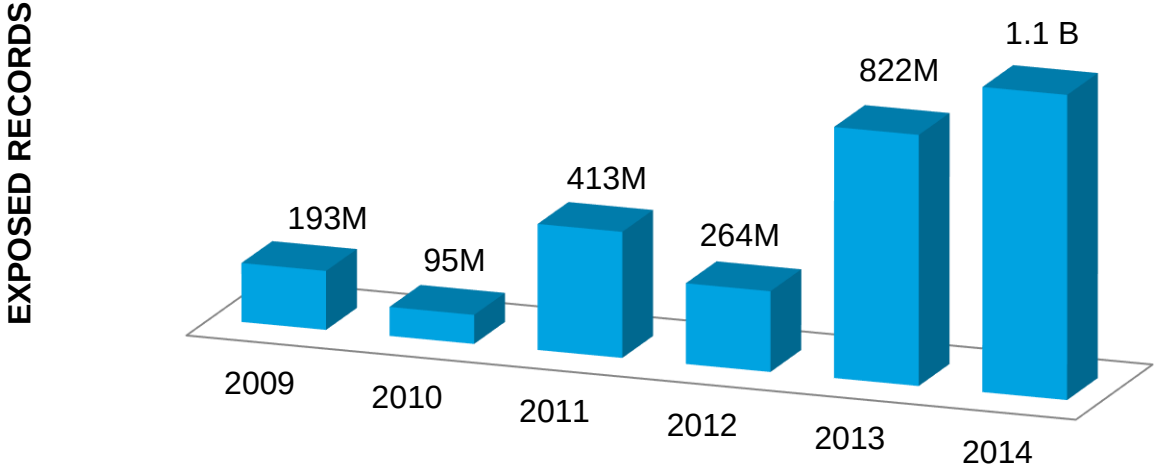

The New York Times
Home Depot Says Data From 56 Million Cards Was Taken in
ABC NEWS
Second credit card breach reported at Shaws, Star
IBC
Millions of Target customers' credit, debit card accounts may be hit by data breach
- NBC News, Dec 2013
Forbes
A third-party vendor
systems has taken
for the Goodwill Breach
INFOSECURITY
2014: The Year of the Data Breach
- Info Security News
THE HUFFINGTON POST
Data Breach May Have
Over 1 Million Payment
customers
Hacker
From
Dairy Queen Says 'Backoff' Malware Affected Payment-Card Information at 395 U.S. Locations
payment cards
USA TODAY
IS&S breach is yet another wake-up call for
retailers to evaluate their third-party
vendors
Latest to
each

# Security Breach Trends



# Key Findings: Hackers Like Low Hanging Fruit

The number of exposed records since 2012 has greatly increased, with a continued focus on Level 4 merchants, dubbing 2014 the “year of the retailer breach”.



# Card Compromise Trends

Basic vigilance can combat many of the common vulnerabilities

- Lack of Security Awareness
  - Storage of prohibited data
  - Mishandling of sensitive data
- Poorly Developed Web Applications
- Weak Passwords
  - Weak passwords account for 31% of all intrusions
  - Most frequently used password in the U.S. in 2014: 123456
- Unpatched Systems – Windows XP
- Misconfigured Firewalls and Remote Access Applications

# By The Numbers


**1,000,000**
New Malware Threats Daily

**$36,000**
Average Breach Cost

**70%**
Breaches Caused By Employees

**60%**
Unable to Stay in Business Six Months After Cyber Attack

# Typical Cost of a Data Breach

Costs of a data breach can range into the hundreds of thousands of dollars per breach and include:

- Mandatory Forensic Audit Costs
- Card Replacement Costs
- Compliance Fines
  - Fines are based on the actual fraudulent use of the cards, which may vary depending on the number of cards exposed
- Productivity Loss
  - Significant paperwork and overhead to manage the post-breach documentation process
    - Similar to an IRS audit
- Brand Damage
  - Customer Defection

# Europay, MasterCard and Visa (EMV)

# Does EMV affect PCI?

EMV, short for Europay, MasterCard, and Visa, is a set of standards that utilizes a chip embedded in a credit card rather than a magnetic strip.

- What does it do?
  - Limits damage that can be done if card data is stolen in a card present transaction
  - Focuses on card validation
- What does it not do?
  - Does not replace or affect PCI
  - Does not limit ecommerce breaches
  - Does not replace P2PE

# EMV Liability Shift

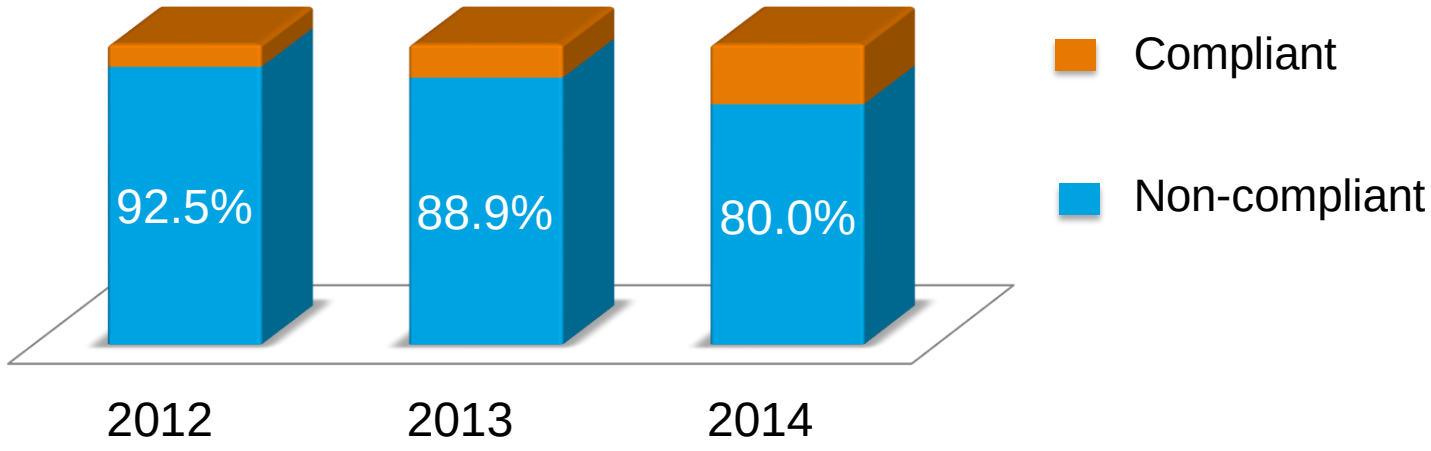
October 1, 2015 is the date in which the liability shift for fraudulent credit card transaction responsibility takes effect, putting the following scenarios into play:

- If you are still using the magnetic stripe only devices and your customer has an EMV enabled card, you are liable for any fraud that may result from that transaction. In other words, if the card number is replicated and used to buy $10,000 worth of stuff, you owe the $10,000 in addition to any fines or fees.
- If you have the new EMV enabled credit card readers but the bank hasn't issued the customer an EMV enabled card, the bank is liable for any fraud that may result from that transaction.
- If you use the new EMV enabled credit card readers on a customer's EMV enabled card and fraud still takes place, then the credit card company bears the liability, as is the case today.

# PCI Basics

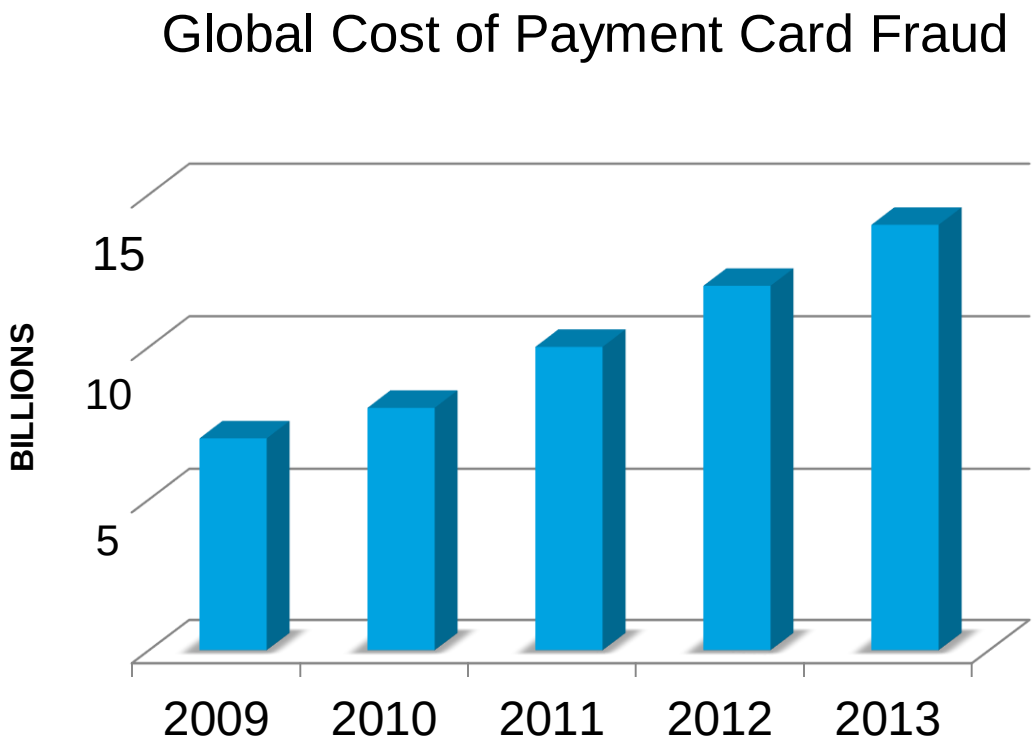
# Compliance Trends

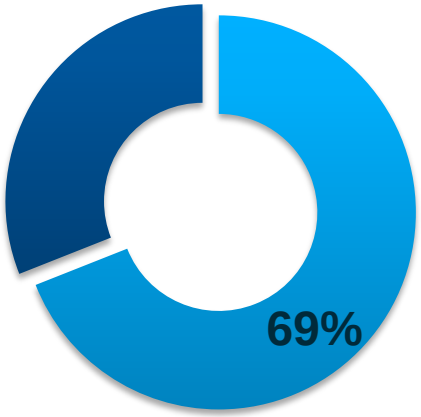
Compliance is improving, however, there is still a lot of work to do.




Data as of end of year

# Why Payment Security Matters




69% of consumers would be less inclined to do business with a breached organization

# PCI SSC and PCI DSS

- **Payment Card Industry Standards Council** (PCI SSC) was formed by the five major card brands to standardize the compliance requirements for all merchants accepting payment cards
- **PCI Data Security Standard** (PCI DSS) is a set of guidelines put in place to ensure that merchants follow best practices in order to protect consumers through steps that reduce credit card fraud and security breaches

# Compliance

# Merchant Levels

| Level / Tier | Merchant Criteria |
|---|---|
| 1 | Merchants processing over 6 million Visa or 6 million MasterCard transactions annually (all channels) or global merchants identified as Level 1 by any Visa region<br>Any merchant that has suffered a hack or an attack that resulted in account data compromise |
| 2 | Merchants processing 1 million to 6 million Visa or 6 million MasterCard transactions annually (all channels) |
| 3 | Merchants processing 20,000 to 1 million Visa or 6 million MasterCard e-commerce transactions annually |
| 4 | Merchants processing less than 20,000 Visa e-commerce or 20,000 MasterCard transactions annually, and all other merchants processing up to 1 million Visa or 1 million MasterCard transactions annually |

# How Does a Level 3 or 4 Merchant Become PCI Compliant

- Identify merchant processing method (Validation Type)
- Complete the Self-Assessment Questionnaire (SAQ) version appropriate for their business
- Complete the relevant Attestation of Compliance (located in the SAQ tool/form)
- Complete and obtain evidence of a passing Vulnerability Scan with a PCI SSC Approved Scanning Vendor (ASV) if applicable
- Submit Compliance Documentation to Acquirer

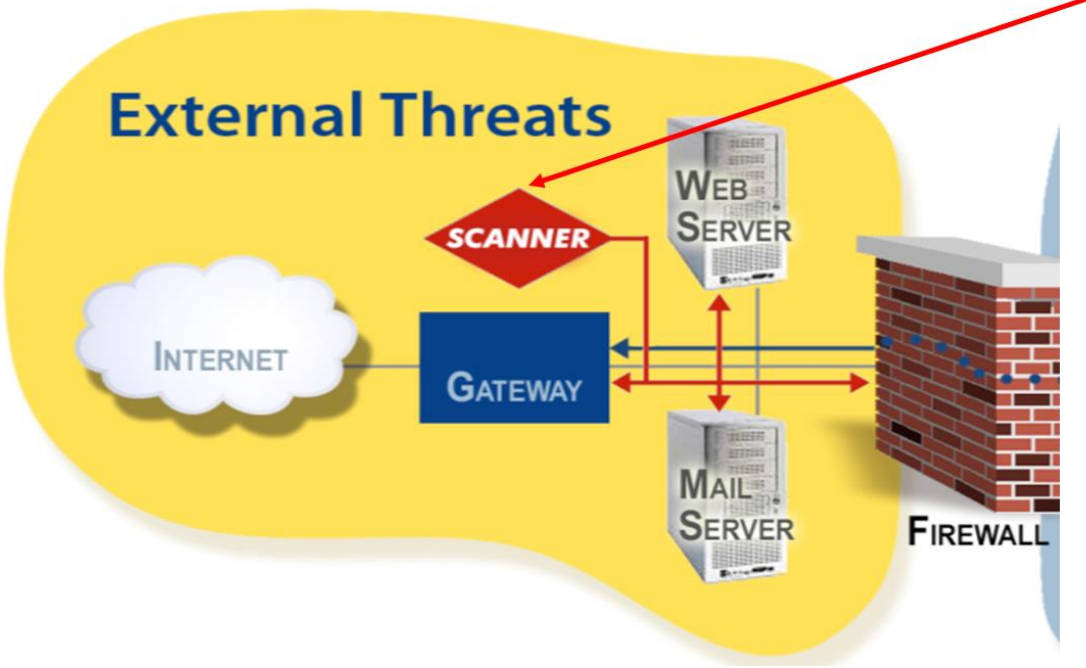
# Self Assessment Questions (SAQ) Basics

| SAQ Type | Eligibility | Number of Questions | Quarterly ASV Scan Required | Penetration Test Required |
|---|---|---|---|---|
| **A** | **Card-not-present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage** | **14** | **No** | **No** |
| **A-EP** | **E-commerce merchants re-directing to a 3rd-party website for payment processing, no electronic cardholder data storage** | **139** | **Yes** | **Yes** |
| B | Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage | 41 | No | No |
| B-IP | Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage | 83 | Yes | No |

# Self Assessment Questions (SAQ) Basics (con't)

| SAQ Type | Eligibility | Number of Questions | Quarterly ASV Scan Required | Penetration Test Required |
|---|---|---|---|---|
| C | Merchants with payment application systems connected to the Internet: No e-commerce or electronic cardholder data storage | 139 | Yes | Yes |
| **C-VT** | **Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage** | **73** | **No** | **No** |
| D-Mrch | All other SAQ-eligible merchants | 326 | Yes | Yes |
| D-SP | SAQ-eligible service providers | 347 | Yes | Yes |
| P2PE | Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage | 35 | No | No |

# What is Vulnerability Scanning




The Vulnerability Scanner probes all public-facing Internet access points to identify weaknesses that can be exploited by hackers.

Firewall to merchant network

Required for SAQ types: A-EP, B-IP, C, D-Mrch and D-SP

# What is Penetration Testing

- It's an active, manual testing process performed in an attempt to gauge the degree to which sensitive information could be exposed

- Two types – external and internal:

  - An External Penetration Test shows you what anonymous attackers on the Internet see when looking at your network

  - An Internal Penetration Test shows you the risks your employees, contractors and guests pose to your information systems

- Required for SAQ types A-EP, C, D-Mrch and D-SP

# Best Practices

# Best Practices

1. Understand your sensitive data, where it is, and who is responsible for it's protection
   - Assign individual responsibility and accountability for monitoring and protecting the sensitive data

2. Avoid storing sensitive data - and if you have to, secure it
   - Limit Database access to only those who absolutely need it
   - Do not store authentication data for either your employees or customers
   - Implement a tokenization solution to enable repeat online customers to securely store and access their payment information

3. Protect your perimeter with managed firewalls
   - Partner with a Managed Security Services company that can setup and monitor your firewall and settings to ensure maximum security with minimal downtime

# Best Practices

4. Fortify your interior with people, procedures and technology
   - Ensure security awareness training is conducted and documented for all employees.
   - Gather and maintain a list of processing devices with serial numbers

5. Know your service provider(s) and THEIR status of PCI DSS Compliance
   - Gather and maintain a list of all service providers, especially those that have influence over card data or the network that the data travels over
   - Understand how each service provider could influence your data security

# Next Steps

# Visit www.controlscan.com/svb

# Support Details

- Visit www.controlscan.com/svb
  - Merchant support options: email, chat, video demos
- Phone support hotline: 800-370-9180
  - Monday - Thursday, 8:30 AM to 8:00 PM ET
  - Friday, 8:30 AM to 6:00 PM ET
- Support Expertise
  - ControlScan is prepared to answer all merchant questions related to PCI, SAQ requirements and security solutions needed to complete SAQ and/or to protect their environments.
  - ControlScan is not involved in the billing process, so Merchant Support is not authorized to answer any billing-related questions.

ControlScan

# Q & A Session

# Appendix

# Speaker Bios

**Stephen Ramminger**
Senior Business Operations Manager, ControlScan

Stephen has been with ControlScan for five years after graduating from the University of Georgia. Stephen started as a Customer Operations Coordinator and is now responsible for the operational aspects of the cornerstone accounts at ControlScan.

**Jon Uyterlinde**
Product Manager, Merchant Services, Silicon Valley Bank

Jon is product manager for SVB's Merchant Services offering, responsible for planning future developments and managing day-to-day responsibilities for the platform. He has over seven years of merchant industry experience, and he was with Wells Fargo Merchant Services for three years. Jon holds a Bachelor's Degree in Economics from Bemidji State University.