MOSSADAMS

WELCOME

E-Commerce Companies: How to Keep Customer Data Safe

- **We'll begin at the top of the hour**
- **Please have your computer speakers turned on**
  All audio is streamed directly through the console and heard through your computer speakers. There is not a dial-in number.
- **For technical support, please use the Q&A window**

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

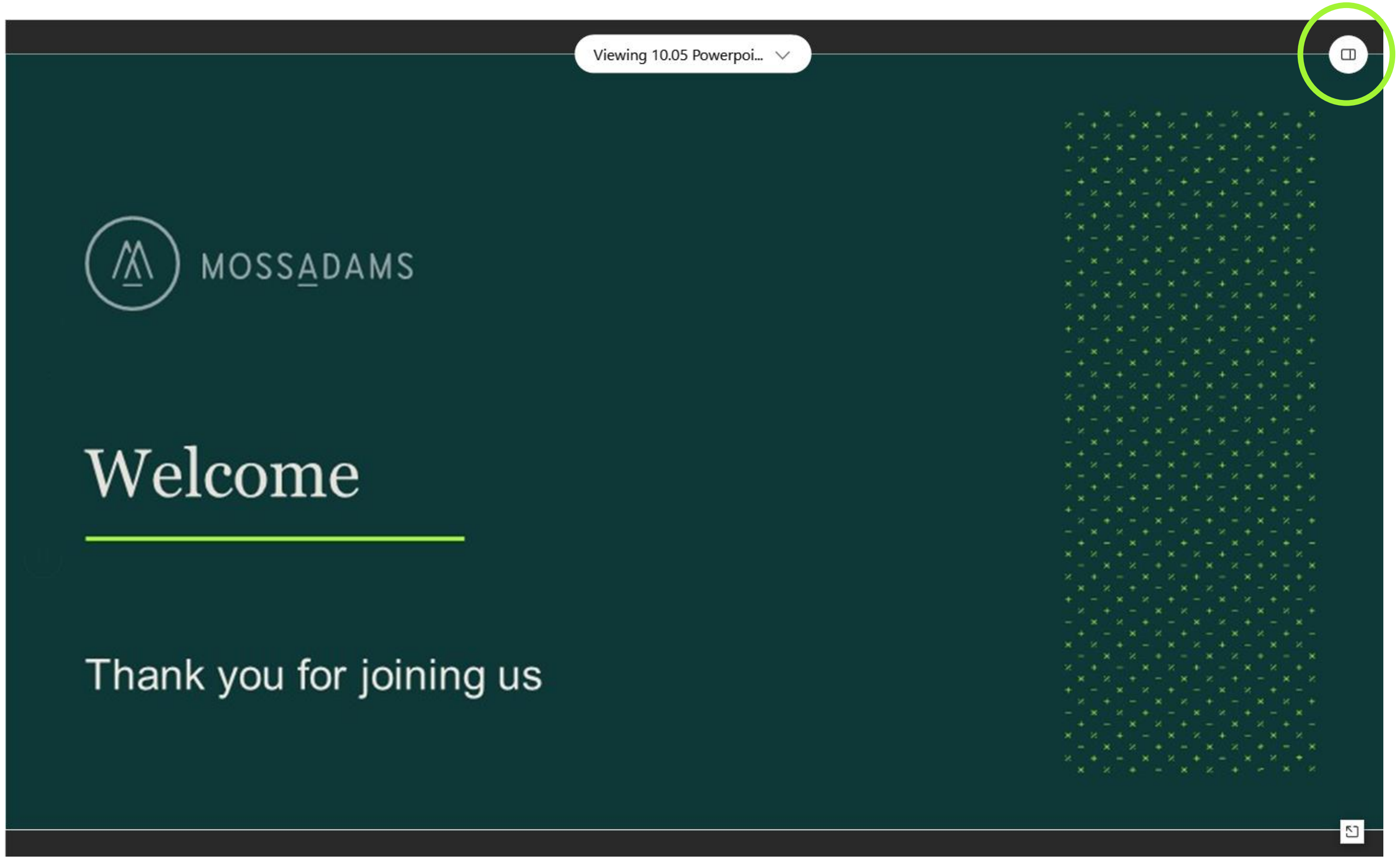
Assurance, tax, and consulting offered through Moss Adams LLP. Investment advisory offered through Moss Adams Wealth Advisors LLC.

MOSSADAMS

Welcome

Thank you for joining us

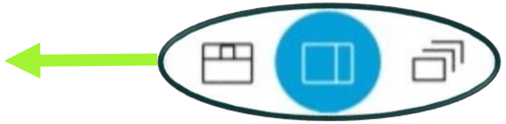
Viewing Options



MOSSADAMS

Welcome

Thank you for joining us

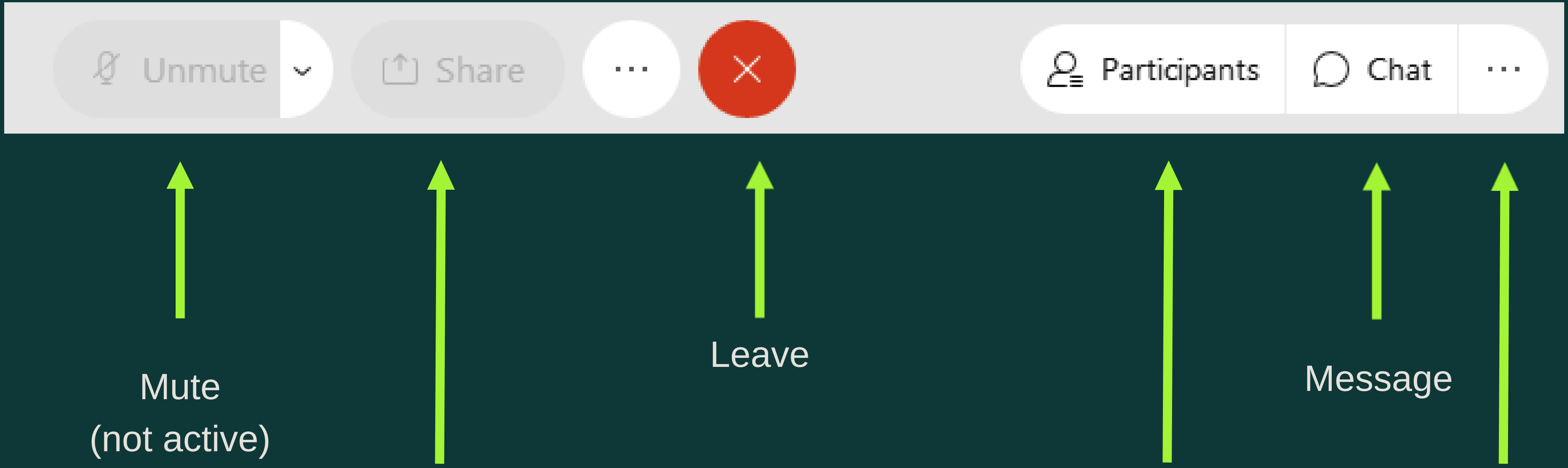


FOR OPTIMAL VIEWING SELECT “SIDE BY SIDE” VIEW FROM THE TOP RIGHT-HAND CORNER.

FOR BETTER VIEWING

- Close all other applications
- Turn up your speaker volume

WebEx Controls



Mute (not active)

Share (not active)

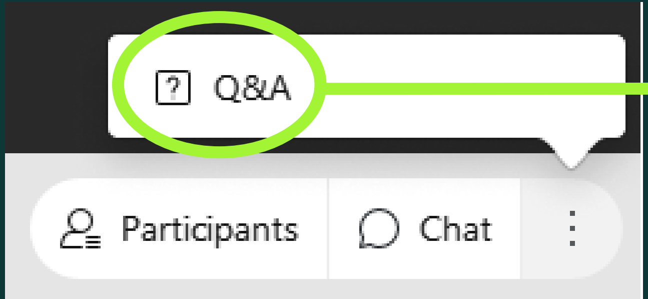
Leave

Participants

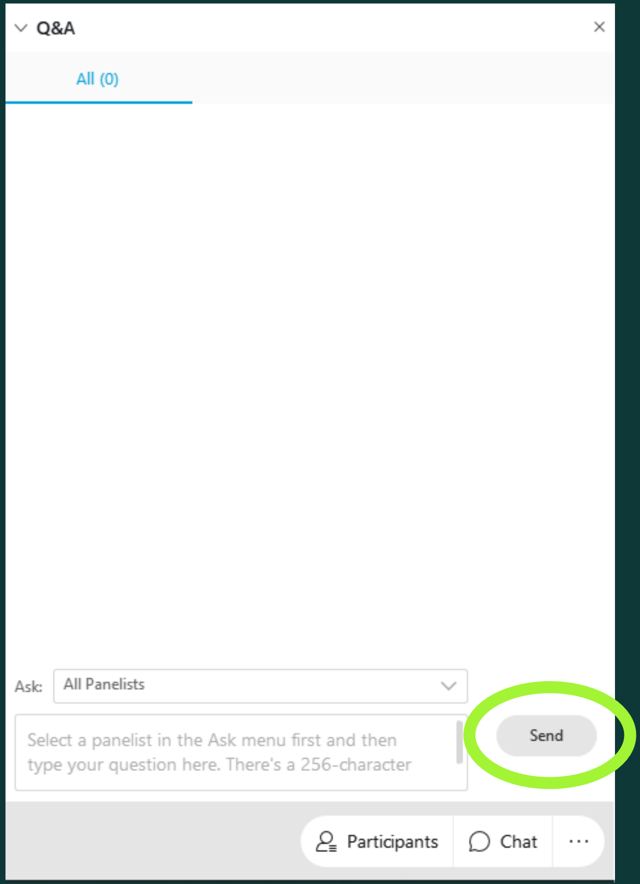
Message

More options

Questions?



- Under the “more options” button, select “Q&A”
- A new box will open on the right-hand side to type your question to the speakers or host



Select a panelist in the Ask menu first and then type your question here. There's a 256-character

Technical Difficulties?

⚠

REFRESH YOUR BROWSER BY CLICKING F5.

If you are still experiencing issues, please feel free to use the question box and direct your question to the “host”

OR

email meetings@mossadams.com

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. ISO/IEC 27001 services offered through Cadence Assurance LLC, a Moss Adams company. Investment advisory offered through Moss Adams Wealth Advisors LLC.

MOSSADAMS

WELCOME

E-Commerce Companies: How to Keep Customer Data Safe

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. ISO/IEC 27001 services offered through Cadence Assurance LLC, a Moss Adams company. Investment advisory offered through Moss Adams Wealth Advisors LLC.

Presenters

Frank Kaufman, CPA
Retail National Practice Leader

Moss Adams

(949) 933-9646
frank.kaufman@mossadams.com

Francis Tam
Partner, Cybersecurity

Moss Adams

(310) 295-3852
francis.tam@mossadams.com

Tyler Neuroth
VP of System Operations

Tangram

(888) 250-6204 x9005
tneuroth@tangrampayments.com

Agenda

01 ECOMMERCE TRENDS AND STATS

02 PROS AND CONS OF DIFFERENT PAYMENT PROCESSING SYSTEMS

03 REQUIREMENTS OF THE PCI DSS

04 SIGNS OF VULNERABILITIES THAT COULD LEAD TO BREACH

05 WAYS TO ENGAGE YOUR ORGANIZATION IN SELECTION AND ADOPTION OF SYSTEM AND POLICIES BEST PRACTICE

MOSSADAMS

eCommerce Trends and Stats

POLLING QUESTION #1

Fraud Chargebacks, which is when a transaction is disputed due to fraudulent or unauthorized activity, can impact a company’s bottom line. On a scale from 1-5, where do these Fraud Chargebacks rank as concern for your organization?

A. 1 (LOW – They rarely happen)
B. 2
C. 3
D. 4
E. 5 (HIGH – They frequently occur and impact our revenue)

Ecommerce U.S. Trends and Statistics

Overall, we’re seeing increases in payments fraud, but especially in the eCommerce sphere.

Consumer Sentinel Network – Data Book 2019

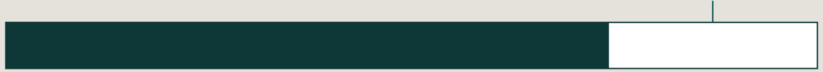
3.4 Million Reports

TOP THREE CATEGORIES

1) Imposter Scams
2) Identity Theft
3) Online Shopping and Negative Reviews

1.9
Million Fraud Reports

26%
Reported A Loss



$2.5 Billion
total fraud losses

$396
median loss

Consumer Sentinel Network – Data Book 2020

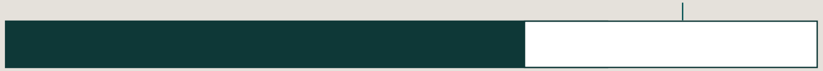
4.8 Million Reports

TOP THREE CATEGORIES

1) Identity Theft
2) Imposter Scams
3) Online Shopping and Negative Reviews

2.3
Million Fraud Reports

34%
Reported A Loss



$3.4 Billion
total fraud losses

$306
median loss

2019 **VS** **2020**

Top Statistics and Trends

- In 2019 nearly $29 Billion dollars were lost due to payment fraud worldwide and is continuing to rise.
- In 2020 Credit Card fraud rose by 44.7% from 2019
- Nearly 70% of all fraud begins with email or telephone contact. Social Engineering and Phishing making up the majority of these contacts.
- About one in four people who report losing money to fraud say it happened when a scammer tricked them into giving the numbers on the back of a gift card.
- Covid-19 has increased the number and amount of scams/fraud due to increases in ecommerce business .
- Trends and Fears play a large part as well – i.e. N-95 Masks during early Covid.

Security Technology

Various Technology currently exists in the Marketplace that is able to help mitigate and reduce exposure to payments fraud. These technologies focus on various parts of the transaction cycle

- CVV / AVS
- EMV (Chip)
- 3DS (Verified by Visa / MasterCard SecureCode, etc.)
- Tokenization
- Credential on File
- Velocity limits and Metering
- Multi-Factor Authentication

MOSSADAMS

Pros and Cons of Different Payment Processing Systems

Pros and Cons of Various Ecommerce Technologies

There are lots of factors that will go into your decision to implement an eCommerce solution.

- Costs
- Ease
- Control
- Flexibility and Scalability

Payment Processing Systems for eCommerce

These are some of the options available to you for implementation of an eCommerce Solution – each with their own Pros and Cons. Let’s discuss:

- Gateway with API – NMI, GGe4, Authorize.net, etc
- Shopping Cart – Shopify, Click Funnels, etc
- Virtual Terminal
- Software
- Mobile App / Website

MOSSADAMS

Requirements of the Payment Card Industry Data Security Standard (PCI DSS)

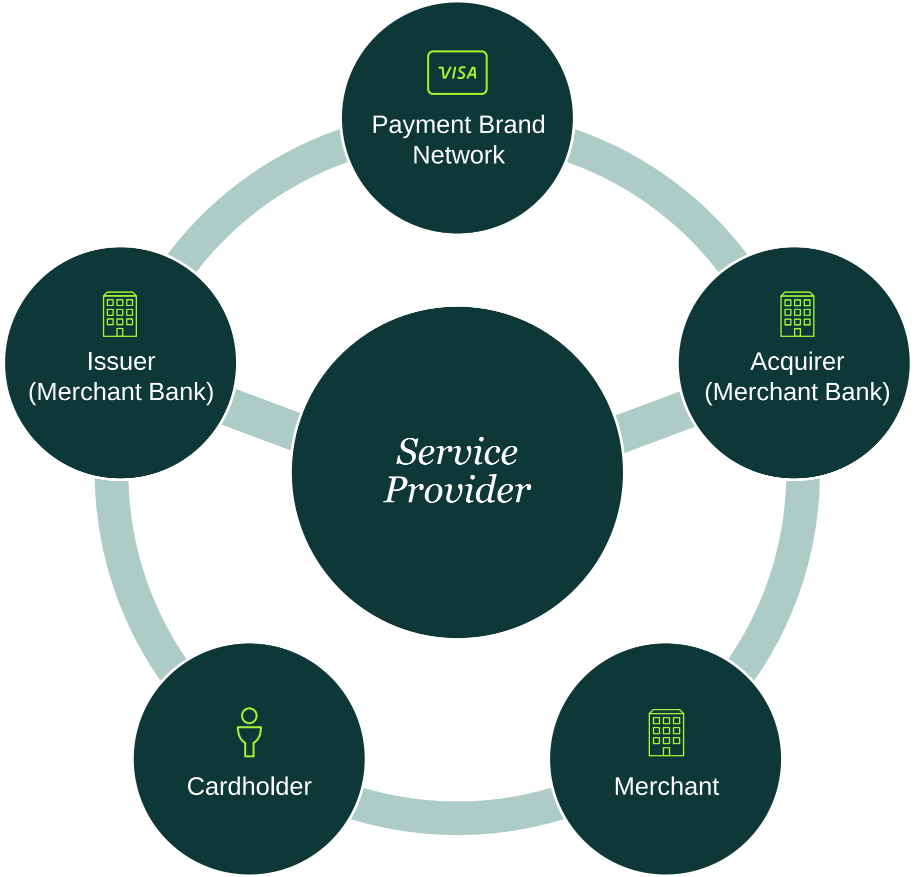
PCI Overview

- Not a government regulation, but an industry regulation
- Purpose is to help prevent credit card fraud and maintain public confidence in payment cards
- Applies to all entities that process, store, or transmit payment card information needs to comply—primary account number (PAN) is the deciding factor
- Card transaction players: card brands, merchants, service providers, acquirers, and issuers
- Effective compliance dates vary depending on merchant level or service provider level and card brand—all deadline enforcement will come from the acquiring bank
- Card brands have their own compliance programs and are responsible for compliance tracking, enforcement, penalties, and fees

PCI Overview

- **PCI Security Standards Council** (PCI SSC or *the Council*) founded in 2006 is responsible for the development, management, education, and awareness of the PCI Security Standards
- **PCI Data Security Standard** (PCI DSS) is a comprehensive set of international security requirements for protecting cardholder data
- **Payment Application Data Security Standard** (PA DSS) is a set of requirements for software vendors to develop secure payment applications
- **PCI PIN Transaction Security** (PCI PTS) is a set of requirements for device vendors and manufacturers for all personal identification number (PIN) terminals, including POS devices, encrypting PIN pads, and unattended payment terminals

The Payment Card Transaction



The Acquirer’s Role

ACQUIRERS (MERCHANT BANK) ARE RESPONSIBLE FOR:

- Ensuring their merchants are PCI DSS compliant
- Managing merchant communications
- Working with their level 1 merchants until full compliance has been validated
  - Merchants are NOT COMPLIANT UNTIL ALL REQUIREMENTS have been met and validated
  - Acquirer is responsible for providing Visa their merchants’ compliance status
- Any liability that may occur as a result of non-compliance

Role of the QSA and ASV

QUALIFIED SECURITY ASSESSOR (QSA)

- Certified to validate compliance with PCI DSS
- Qualified security assessor companies have been qualified to have their employees assess compliance to the PCI DSS standard
- Qualified security assessors are employees of these organizations who have been certified to validate an entity’s adherence to the PCI DSS

APPROVED SCANNING VENDOR (ASV)

- Approved scanning vendors are organizations that validate adherence to certain DSS requirements by performing vulnerability scans of internet-facing environments of merchants and service providers

PCI DSS Requirements

PCI DATA SECURITY STANDARD: HIGH-LEVEL OVERVIEW

Build and maintain a secure network

Requirement 1:	Install and maintain a firewall configuration to protect cardholder data
Requirement 2:	Don’t use vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data

Requirement 3:	Protect stored cardholder data
Requirement 4:	Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program

Requirement 5:	Use and regularly update anti-virus software
Requirement 6:	Develop and maintain secure systems and applications

Implement strong access control measures

Requirement 7:	Restrict access to cardholder data by business need-to-know
Requirement 8:	Assign a unique ID to each person with computer access
Requirement 9:	Restrict physical access to cardholder data

Regularly monitor and test networks

Requirement 10:	Track and monitor all access to network resources and cardholder data
Requirement 11:	Regularly test security systems and processes

Maintain an information security policy

Requirement 12:	Maintain a policy that addresses information security

Merchant Levels

Merchant Level	Description
1	Merchants processing over 6 million Visa transactions annually (all channels) or global merchants identified as Level 1 by any Visa region.
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels).
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually.
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually.

Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit, and prepaid) from a merchant Doing Business As (DBA).

Service Providers

Service Provider Level	Description	Posted on Visa’s Global List of Validated Service Providers
1	VisaNet ® processors or any service provider that stores, processes, and/or transmits over 300,000 Visa transactions annually.	Yes
2*	Any service provider that stores, processes, and/or transmits less than 300,000 Visa transactions annually.	No*

*Level 2 service providers may choose to validate as a Level 1 service provider in order to be listed on Visa’s Global List of Validated Service Providers.

Validation Requirements

		Compliance	Validation Actions		
GROUP	**LEVEL**	**COMPLY WITH PCI-DSS**	**ON-SITE SECURITY ASSESSMENT**	**SELF-ASSESSMENT QUESTIONNAIRE**	**NETWORK SCAN***
Merchant	1	Required	Required Annually		Required Quarterly
	2&3	Required		Required Annually	Required Quarterly
	4**	Required		Recommended	Recommended Quarterly
Service Provider	1	Required	Required Annually		Required Quarterly
	2	Required			Required Quarterly

*Network scanning is applicable to any internet facing system.

** Validation requirements are determined by the merchant's acquirer.

Self-Assessment Questionnaires (SAQs)

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This wouldn’t apply to face-to-face merchants.
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 processing 20,000 to 1 million Visa e-commerce transactions annually.
C	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually.
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.

Key Compliance Tips

- Encrypt databases and files prior to committing them to backup tape and removable media
- Install A/V on your database servers that store cardholder data or document compensating controls
- Segment, or *cocoon* your CDE and use two-factor authentication for remote access—internal pen testing isn't necessary
- Require password requirements of 90 days maximum, aging, seven-character minimum, complexity, and a history of the last four passwords used

Key Compliance Tips

- In virtualized environments, limit the number of mixed mode servers and use separate partitions for each virtual host
- Implement point-of-sale (POS) systems with point-to-point encryption (P2PE) functionality to reduce scope
- Conduct quarterly vulnerability scans and address vulnerabilities immediately.
- Look to information security best practice frameworks for guidance (ISO 27002, NIST 800-53a, COBIT).

Preparing for a PCI DSS Assessment

GATHER DOCUMENTATION:

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

SCHEDULE RESOURCES:

Obtain dedicated participation of a project manager and key people from IT, 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.

Leveraging PCI DSS Audit

Documentation collected for PCI DSS requirements can be repurposed for other audits.

- Test results completed for PCI requirements can be used or relied upon by SOC auditors
- Policies and templates developed for PCI compliance such as information security policies and user request forms can be used for systems without cardholder data
- Security awareness training and acceptable use policies can fill possible gaps in existing human resources polices

Leveraging PCI DSS Audit

Description of Good Practices	PCI DSS v2	ISO 27002	HIPAA	COBIT (SOX)
Install and maintain a firewall configuration to protect data	1	11.4.5	§164.312 (e) (1)	DS5.11
Use and regularly update anti-virus software or programs	5	10.4	§164.308 (a) (5)	DS5.9
Assign a unique ID to each person with computer access	8	11.2.1	§164.312 (a) (1)	DS5.4
Regularly test security systems and processes	11	10.10.1	§164.312(b)	AI2.3

Leveraging PCI DSS Audit

PCI requirements can be used to drive existing internal projects:

- In some areas, PCI requirements may be more stringent than existing practices and used to enforce stronger security. For example, two factor authentication required for remote access and prohibited weak wireless encryption such as Wired Equivalent Privacy (WEP).
- Communication of scheduled QSA assessment dates can force deadlines and uniform practices for unresponsive or isolated departments.

Leveraging PCI DSS Audit

Conversely, existing internal projects may be used to satisfy some PCI requirements:

- Adopt cloud computing to *eliminate* some of the requirements, such as req. 10, 11.2 and 11.4
- Safeguard private information initiatives, such as personally identifiable information (PII) or Gramm-Leach-Bliley act, may require point-to-point encryption (P2PE), tokenization, or two-factor authentication
- Risk assessment can be leveraged to satisfy req. 12.1.2, especially if the existing risk assessment is based on ISO 27005 or NIST SP 800-30

POLLING QUESTION #2

Which is currently your top data security priority?

A. Educating my organization to avoid behavior that could lead to risks and jeopardize customer data

B. Finding a payment processing system that has a reputation for strong cybersecurity controls

C. Strengthening our existing cybersecurity program and processes

D. Learning where the gaps are in our current payment processing system and operations that could make our data vulnerable

E. Other

MOSSADAMS

How To Identify Vulnerabilities That Could Lead To a Data Breach

Abnormal Data Behavior

Summary of findings

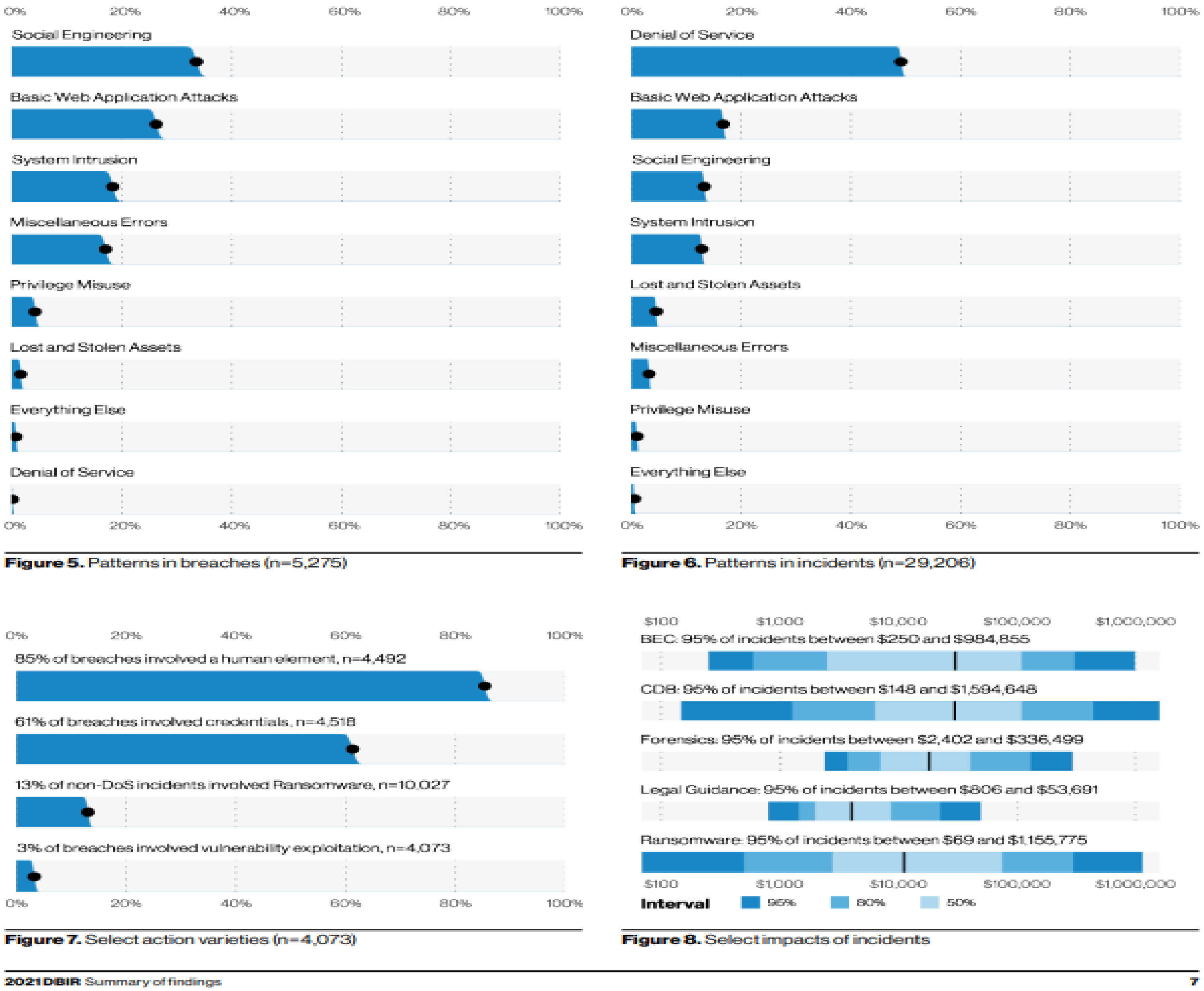


Figure 5. Patterns in breaches (n=5,275)

Figure 6. Patterns in incidents (n=29,206)

Figure 7. Select action varieties (n=4,073)

Figure 8. Select impacts of incidents

2021 DBIR Summary of findings 7

Abnormal Data Behavior

Some of the typical abnormal data behaviors:

- Permissions change alerts
- Large volume of data movement, especially to and from an unknown cloud
- Data patterns, data/files/folders getting encrypted, zipped, and sent/emailed
- Off-hour activities and activities originated from unusual physical and/or logical locations
- File type/contents mismatch, such as JPEG but containing source code
- Mysterious accounts, especially high-powered accounts, created

MOSSADAMS

Ways to Engage your Organization in Selection and Adoption of System and Policies and Best Practice

Activities and Actions You can Take as an Organization to Embrace Security

- Phishing Testing
- Security Awareness Training
- Use of Physical Security Systems
- Monitoring of Data and Access
- PCI Compliance

Security Considerations Through Business Model

- There is no right or wrong
- Do not “come in contact” with credit cards if you do not have to
- Minimize your attack surface whatever business model or architecture you have
- Do your due diligence when selecting third parties to facilitate your business model
- Always improve on your “IT hygiene”
- Always consider having multiple layers of security

PCI Data Security Standards

PCI DSS REQUIREMENT	EXAMPLE RESPONSIBILITY ASSIGNMENT FOR MANAGEMENT OF CONTROLS		
	IaaS	PaaS	SaaS
1. Install and maintain a firewall configuration to protect cardholder data.	Shared	Shared	Provider
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	Shared	Shared	Provider
3. Protect stored cardholder data.	Shared	Shared	Provider
4. Encrypt transmission of cardholder data across open, public networks.	Customer	Shared	Provider
5. Protect all systems against malware and regularly update anti-virus software or programs.	Customer	Shared	Provider
6. Develop and maintain secure systems and applications.	Shared	Shared	Shared
7. Restrict access to cardholder data by business need to know.	Shared	Shared	Shared
8. Identify and authenticate access to system components.	Shared	Shared	Shared
9. Restrict physical access to cardholder data.	Provider	Provider	Provider
10. Track and monitor all access to network resources and cardholder data.	Shared	Shared	Provider
11. Regularly test security systems and processes.	Shared	Shared	Provider
12. Maintain a policy that addresses information security for all personnel.	Shared	Shared	Shared
PCI DSS Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.	Provider	Provider	Provider

Build a Culture that Emphasizes Security

CREATING A CULTURE OF SECURITY AWARENESS AND PRACTICE

- Ensuring security is taken seriously from the top down
- Making sure all levels realize the true importance of the data
- Actively participating in and being aware of industry and security trends
- Regularly providing updates and details
- Celebrate and Reward

E-commerce Series: Up Next

E-COMMERCE COMPANIES: LEVERAGE PREDICTION TECHNOLOGIES

February 3, 2022 at 10AM PT

➤ QUESTIONS

Let’s start a conversation.

francis.tam@mossadams.com

tneuroth@tangrampayments.com