Managing Risk in the Digital World

Jose A. Rodriguez, Director
Visa Consulting and Analytics

What is driving the security landscape?

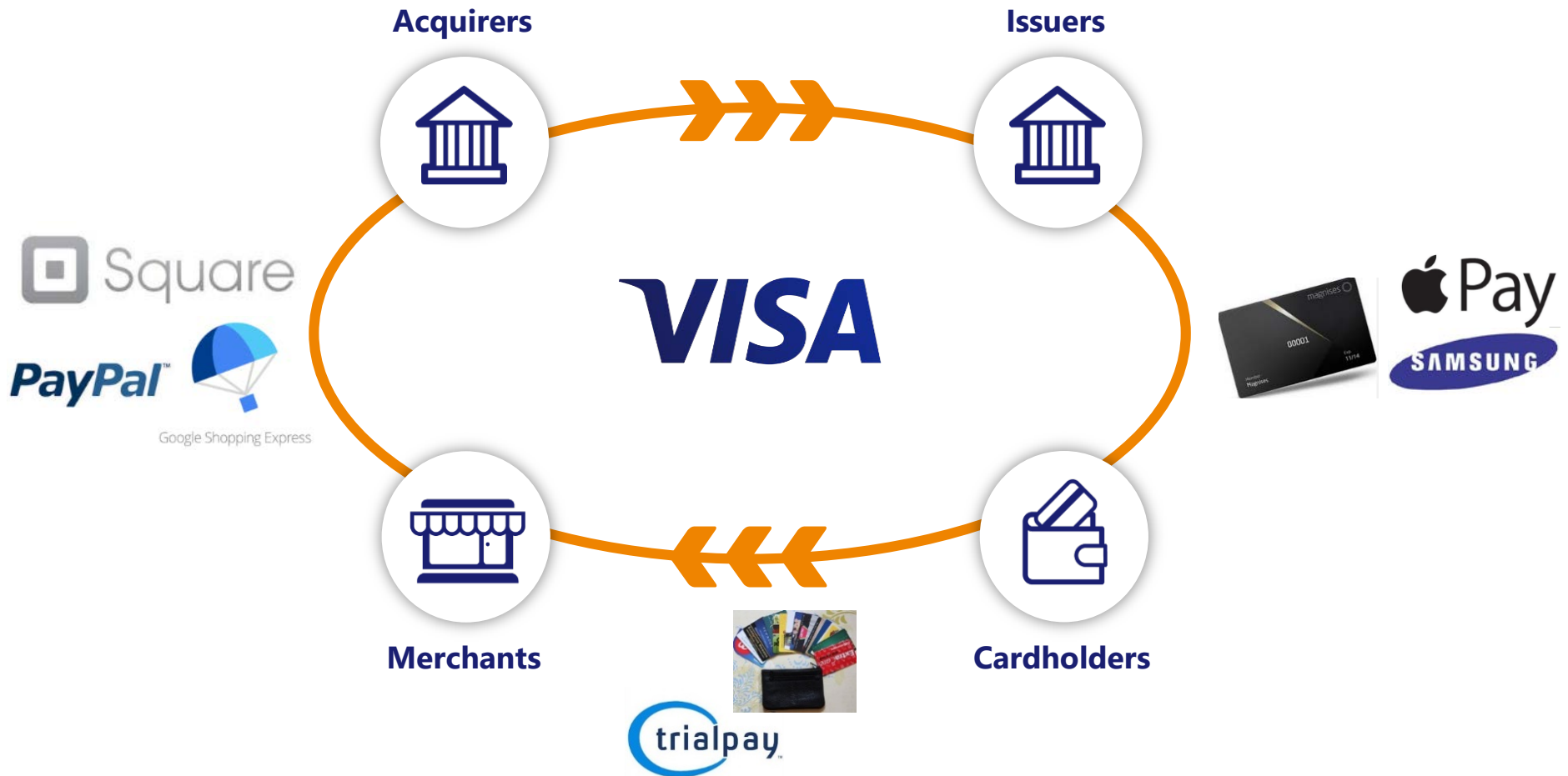| Innovation	Data Compromises	Government
• New entrants • New technologies • New business models	• Increasing attacks against data aggregators/third parties • Enhanced risk in card-not-present channel	• Security mandates • Regulation

The Expanding Payments Ecosystem

Acquirers

Issuers

Merchants

Cardholders

VISA

Square

PayPal

Google Shopping Express

Apple Pay

SAMSUNG

trialpay

Note: All brand names and logos are the property of their respective owners, are used for identification purposes only, and do not imply product endorsement or affiliation with Visa

Transitioning Payments from Physical to Digital

Provisioning

Tokenization

Risk Management

Lifecycle Management

Remote Commerce

Face-to-Face Commerce

eCommerce

mCommerce

Buy Buttons

Near-Field Communication (NFC)

Quick Response (QR)

Future (BLE)

Wearables

Payment Security: Where are we now?

Fraud remains near historic lows, but data losses continue to accelerate
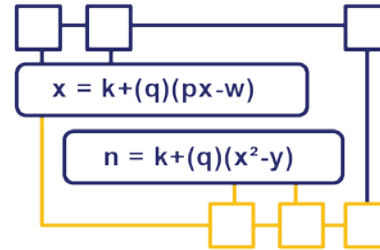
Gross Fraud Rate
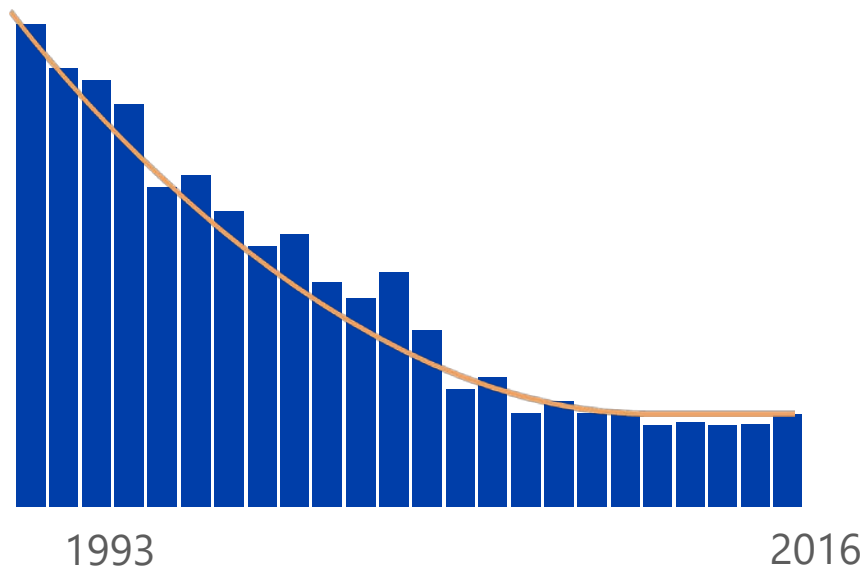
Personal Data Exposed

1993   2016   2004   2017 YTD
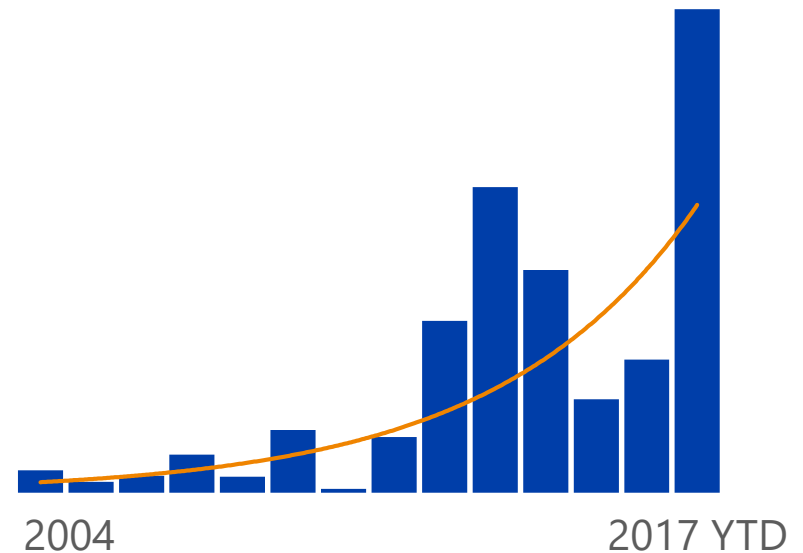
Changes in Criminal Attacks are Keeping Pace

Frequency   Magnitude   Sophistication   Organization

$$x = k+(q)(px-w)$$

$$n = k+(q)(x^2-y)$$
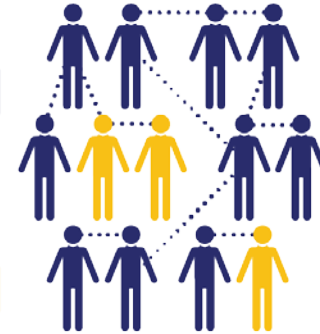
Shifting Breach Types

❖ Decrease in magnetic stripe data breaches

❖ Increase in card-not-present compromises

❖ Proliferation of third-party breaches

Hackers Moving Beyond Merchants

❖ Pursuing data aggregators

❖ Targeting integrators/re-sellers

❖ Penetrating financial institutions

Increasing Threat: Card-Not-Present Breaches

- Less sophisticated attack required

- Harder to identify breaches

- Low barrier of entry for merchants

2015
Brick & Mortar = 70%
eCommerce = 27%

2016
Brick & Mortar = 44%
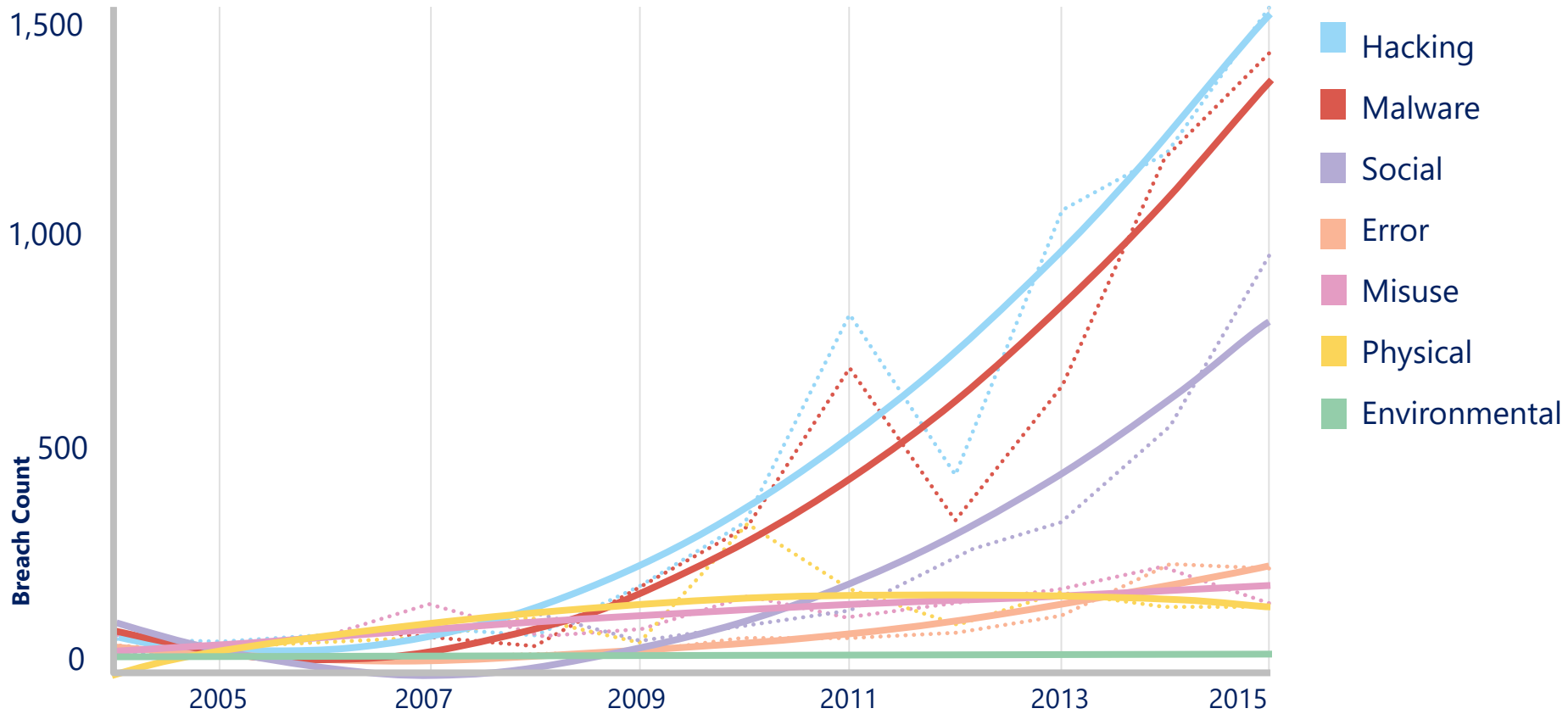eCommerce = 55%

2017*
Brick & Mortar = 11%
eCommerce = 87%

* YTD through September 2017

We Can Never Become Complacent

Number of Breaches Per Threat Action Category Over Time
(n=9,009)

Legend:
- Hacking
- Malware
- Social
- Error
- Misuse
- Physical
- Environmental

Breach Count (y-axis): 0, 500, 1,000, 1,500

x-axis: 2005, 2007, 2009, 2011, 2013, 2015

Source: 2016 Verizon Breach Report

Visa's Strategy for Payment Security

Data is Key to Addressing Threats

Protect Data

Safeguard payment data

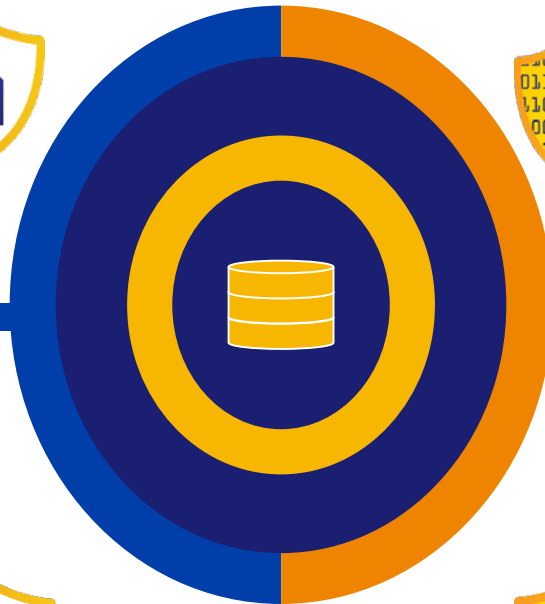**Harness Data**

Stop fraud before it occurs

Devalue Data

Render data useless

Empower Consumers

Engage cardholders in payment security

Merchant Levels & PCI DSS Compliance Validation Requirements

Level/Tier	Merchant Criteria	Minimum Validation Requirements
1	Processing over 6 million Visa transactions annually (all channels) or global merchants identified as Level 1 by any Visa region	• Annual Report on Compliance (ROC) by Qualified Security Assessor (QSA) or internal resources if signed by officer of the company • Quarterly network scan by Approved Scan Vendor (ASV) • Attestation of Compliance (AOC)
2	Processing 1 million to 6 million Visa transactions annually (all channels)	• Annual Self-Assessment Questionnaire (SAQ) • Quarterly network scan by ASV • AOC
3	Processing 20,000 to 999,999 Visa e-commerce transactions annually	• Annual SAQ • Quarterly network scan by ASV • AOC
4	Processing fewer than 20,000 Visa e-commerce transactions annually and all other merchants processing below 1 million Visa transactions annually	• Annual SAQ • Quarterly network scan by ASV

Small Merchant Security Basics

Simple Processes Providing Significant Security

	Change Default Passwords	Install Antivirus	Enable Remote Access Only When Necessary	Use Only PCI Certified QIRs	Use Only Visa Registered Service Providers
Ease of Implementation	Easy	Medium	Easy	Easy	Easy
Cost	None	Medium	None	None	None
Effectiveness	Medium	Medium	High	High	High

Merchant Risk

PCI SSC Small Merchant Security Taskforce

Purpose
- Communicate unique small business security challenges
- Simplify understanding of PCI DSS
- Provide educational materials that relate to small businesses

Participants
- Collaboration from dozens of small merchant owners and franchisees
- Co-chaired by Barclaycard and National Restaurant Association

Products
- Materials that are easy to understand
- Tips for improved security implementation
- Small merchant resources

PCI SSC – Small Merchant Taskforce

Providing infographics, diagrams and illustrations with easy-to-understand guidance on security

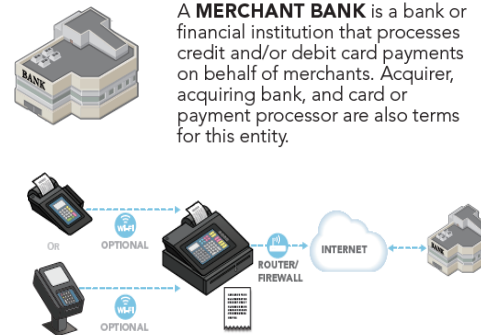### The impact of breaches to small businesses

$20,752

AVERAGE COST TO A SMALL BUSINESS DUE TO HACKING, UP FROM $8,600 IN 2013
(NSBA)

69% OF AMERICAN CONSUMERS WORRY ABOUT THEFT OF THEIR PAYMENT CARD DATA
(Gallup)

What's at risk? Understanding data on a payment card

TYPES OF DATA ON A PAYMENT CARD

Card security code (American Express)

Chip

PAN

Cardholder name

Expiration date

Magnetic stripe (Data on tracks 1 and 2)

Card security code (All other payment brands)

Common payment terms and types of POS terminals

A **MERCHANT BANK** is a bank or financial institution that processes credit and/or debit card payments on behalf of merchants. Acquirer, acquiring bank, and card or payment processor are also terms for this entity.

A **PAYMENT SYSTEM** encompasses the entire process for accepting card payments in a retail location (including stores/shops and e-commerce storefronts), and may include a payment terminal, an electronic cash register, other devices or systems connected to a payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), servers with e-commerce components such as payment pages, and the connections out to the merchant bank.

Different risk for different environments and payment systems

COMPLEX ENVIRONMENT · SIMPLE ENVIRONMENT

HARDER TO REDUCE RISK · EASIER TO REDUCE RISK

DIAL-UP PAYMENT TERMINAL · PHONE LINE · BANK

Simple payment system for in-shop purchases

Merchant Risk

Technology Innovation Program

- In 2012, Visa announced the Technology Innovation Program (TIP) to recognize merchants that invest in secure technology

- Program eliminates the annual PCI DSS validation exercise for qualifying merchants

Merchant Qualification Criteria

At least 75% of merchant's Visa transactions originate from EMV chip-enabled devices

Implementation of PCI-validated point-to-point encryption solution

Action Items
Quick Wins

- Subscribe to RSS feed for automatic Data Security updates

- Leverage the data security resources on visa.com

- Create – and practice – an after-hours response escalation plan

Closing Thoughts

- The digital future is happening now – it's rapidly changing the payment experience offering nearly limitless growth potential for payments

- The rise of artificial intelligence is making cyber criminals more effective – Visa is using this same technology to defend and protect against the attacks

- Key to success is to continue to **innovate and collaborate** in line with Visa's Security Strategy

Protect Data	Devalue Data	Harness Data	Empower Consumers

Data Security Resources

Visa Data Security Websites
North America and LAC: www.visa.com/cisp
AP and CEMEA: www.visa.com/staysecureAPCEMEA

Data Security Questions
North America and LAC – cisp@visa.com
AP and CEMEA – vpssais@visa.com and pciagents@visa.com

Visa Global Registry of Service Providers – www.visa.com/onthelist

Visa Business School – www.visabusinessschool.com

PCI Security Standards Council Website – www.pcissc.org
What to do if compromised