What's Next?

The Evolution of Risk in Retail

VISA

Forward-looking statements and disclaimer

This presentation may contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms “objective,” “goal,” “strategy,” “opportunities,” “continue," “can,” "will,“ and other similar references to the future. Examples of such forward-looking statements may include, but are not limited to, statements we make about our corporate strategy and product goals, plans, and objectives. By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance, and (iii) are subject to risks, uncertainties, assumptions, and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements for a variety of reasons, including macroeconomic and industry factors such as currency exchange rates, global economic, political, health and other conditions, competitive pressure on customer pricing and in the payments industry generally, and material changes in our customers' performance compared to our estimates; systemic developments such as disruption of our transaction processing systems or the inability to process transactions efficiently, account data breaches involving card data stored by us or third parties, and increased fraudulent and other illegal activity involving our cards; and other factors discussed under the heading "Risk Factors” in our most recent Annual Report on Form 10-K and our most recent Quarterly Reports on Form 10-Q. You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement because of new information or future developments or otherwise.

Studies, survey results, research, recommendations, and opportunity assessments are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory, or other advice. Recommendations and opportunities should be independently evaluated in light of your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of any studies, survey results, research, recommendations, opportunity assessments, or other information, including errors of any kind, or any assumptions or conclusions you might draw from their use. Except where statistically significant differences are specifically noted, survey results should be considered directional only.

Topics

- Payment ecosystem risk landscape
- Current threats and breach trends
- Emerging threats to the payment ecosystem
- Effective threat management for payments

Current Payment Data Breach Trends

Payment System Risk Landscape

Data Security

- Frequency of data breaches is increasing
- Small merchant breaches account for the majority of 'known' compromised accounts
- Emphasis on cyber intelligence information sharing is growing

Fraud Trends

- Fraud levels and accounts are increasing
- Fraud is concentrated in markets/channels that rely on static authentication data
- CNP fraud is disproportionately high

New Players in the Eco-system

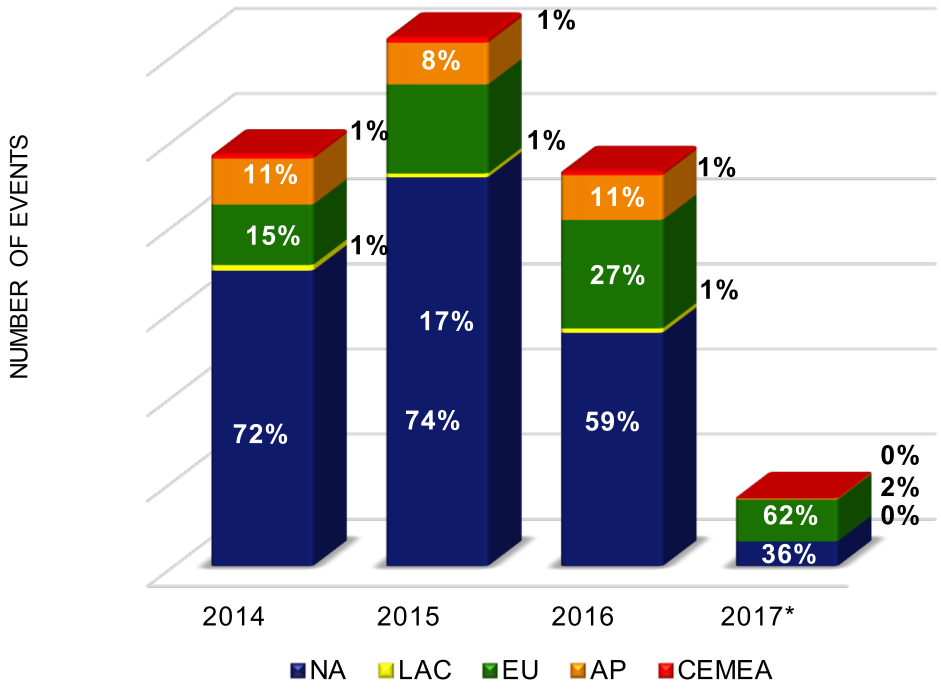
- Proliferation of third party agents and nontraditional players is increasing security risks
- New payment innovation is introducing new risks

Regulatory Attention

- Governments and regulators are paying more attention to fraud and data security
- Opportunities for public-private collaboration on payment security are expanding

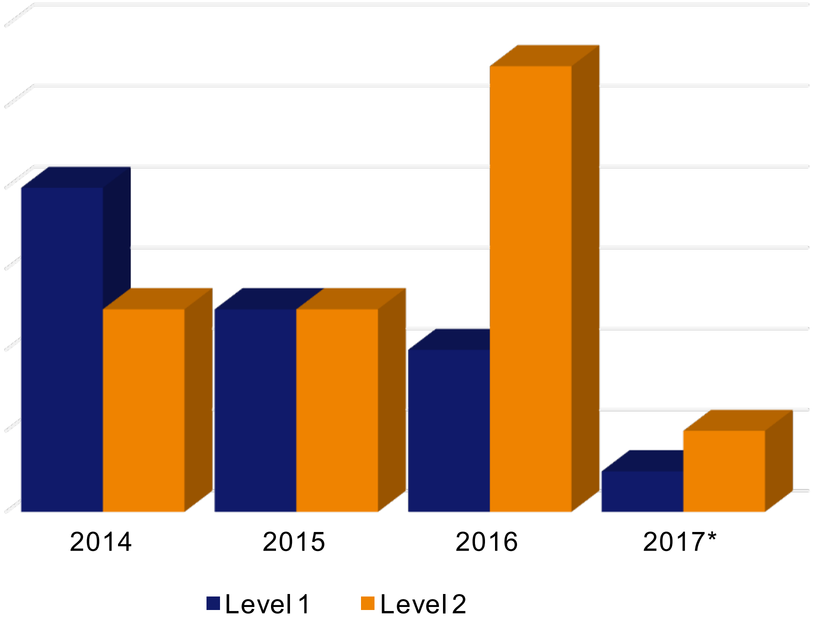
Global Breach Trends – By Merchant Region, Size

Global CAMS Alerts by Region



- As a proportion of the total number of breach events, Level 4 merchants (less than 1mm trans per year) remain the vast majority of compromise cases
- 2016 marks a shift in proportion of compromises between North America and the rest of the world

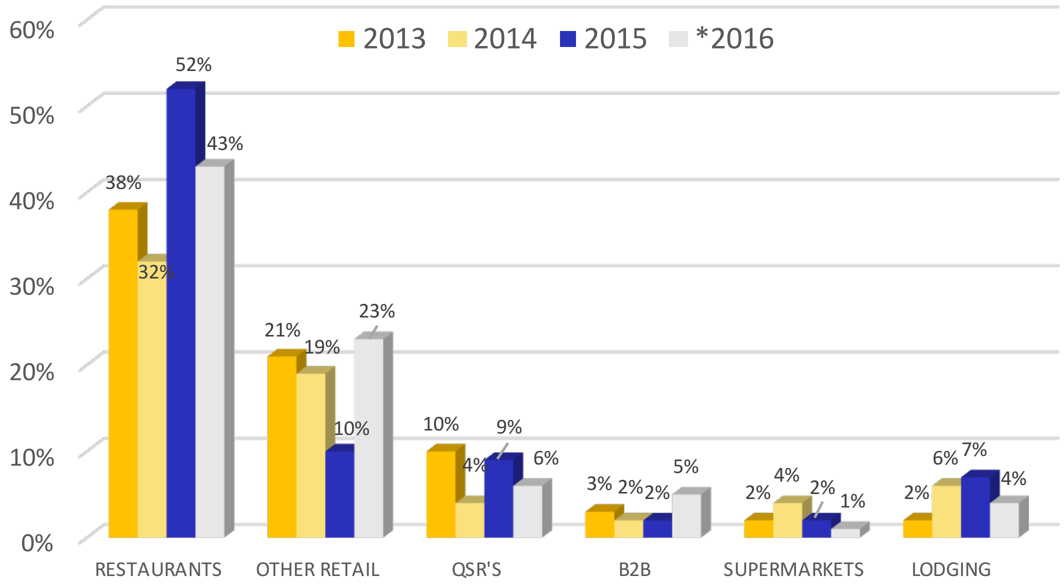
Merchant Investigations

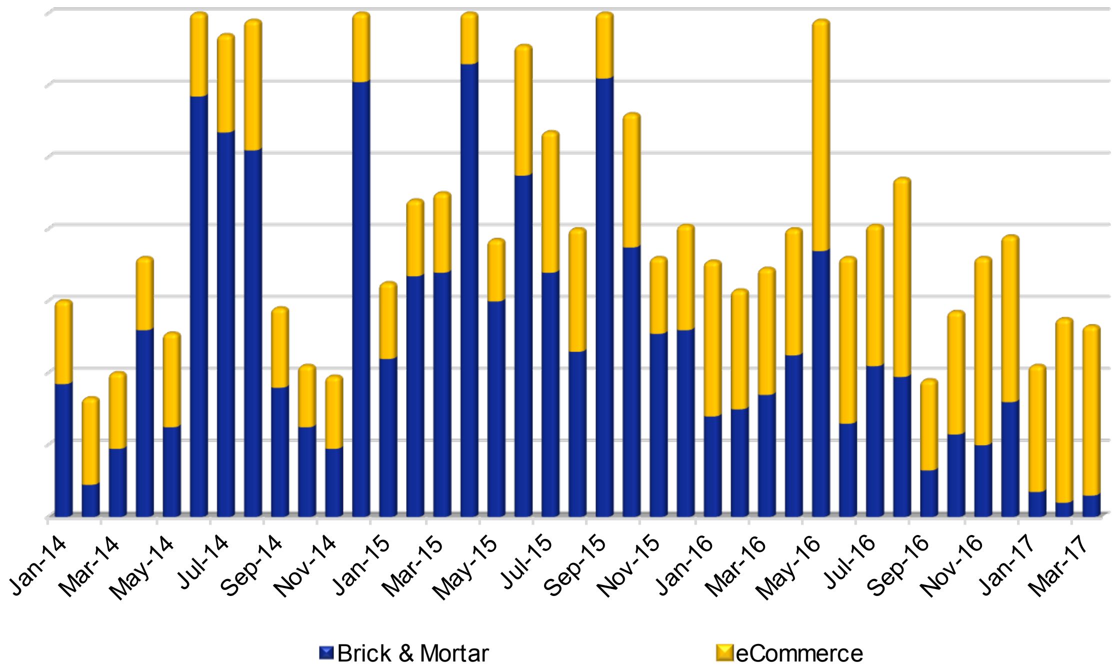


- Level 1 = >6 mm trans per year
- Level 2 = 1mm-6mm trans per year

*YTD through March 2017

Global Breach Trends – By Merchant Type





- Restaurant, "Other Retail" are consistently the top breached merchant types
- Insecure remote access makes restaurants a top target for cybercriminals
- Significant shift in breaches of brick and mortar vs. ecommerce merchants

Payment Data Breach Trends - Summary

VISA

Card Present

- Counterfeit still a major concern
- For EMV-enabled merchants, fraud is down
- Fewer large merchant breaches
- Most breaches (by %) involve unprotected smaller merchants
- Fewer breaches detected by conventional methods
- Repeat compromises and “re-breaches”

Card Not Present

- Increase in CNP merchant compromises
- Vulnerable web commerce applications being exploited
- Fraudulent applications trending up
- Account takeovers trending up
- CNP data contributing to other fraud types

Emerging Payment Ecosystem Threats

EMV Effect on Merchant Breaches

- Starting to shift away from big retailers to merchants without advanced security
- Criminals are targeting remaining mag stripe data, and in different ways
- Many vulnerable merchants out there
- Breaches involving card-not-present data are on the rise
- Big data gone bad (combining stolen data from multiple breaches)
- EMV driving criminals to attack other data

Multi-stage Attacks & Targeting Business Partners

- Attacking Point Of Sale “Integrators” to reach large numbers of smaller merchants
- Underground sites selling enterprise access, like xDedic, popping up
- Huge underground market in authentication credentials (single-factor remote access)
- Breached merchants as pivot points
- Data exfiltration through breached merchants

Cybercrime, Inc.

Cybercrime Markets

- Hacking services
- 0-day vulnerabilities
- Exploit kits
- POS malware development
- Botnet rentals
- Merchant remote access
- On-the-spot data validation
- Customer support
- Money back guarantees

Changes in Payment Data Monetization

- Getting harder to identify the breach with conventional methods (fraud & Common Points of Purchase)
- Data mixing (old with new, data across breaches)
- Localized counterfeiting
- Selling cardholder profiles along with the card number (ZIP, address, CVV2, phone)
- Criminals can hold data for up to 6 months, some even longer

Hiding in Plain Sight, Deception and Anti-forensics

- Tactics, tools used to avoid detection
- No malware
- PowerShell exploits
- Sneaky exfiltration methods
- Data encryption with asymmetric keys
- Log deletion
- Timestomping

Forced “Fallback” Transactions

- “Fallback” described
- What would it take to disable the chip card reader and force a less secure transaction (swipe)?
- Attack would need to be successful on multiple devices (100s/1000s)
- Requires very advanced malware & a detailed understanding of POS devices
- What if the Windows system controlling POS devices had this as an option?

Protecting The Data Is Foundational
Our Work Is Never Done

Data Protection

Data Devaluation

Responsible Innovation

Fraud Prevention

Effective Payment Threat Management

Root Cause - Ineffective Threat Intelligence

- Incident response process only existed on paper
- Slow/no reaction to obvious threats
- Threat intelligence with no forethought or focus
- Intelligence and IR teams drowned in information overload
- False sense of security or single points of failure
- Attacks end up succeeding anyway, right under their noses

Actual forensic finding: "Investigation showed client’s anti-virus system had been alerting starting approximately 3 days after the breach began but client was unaware or unresponsive to the alerts."

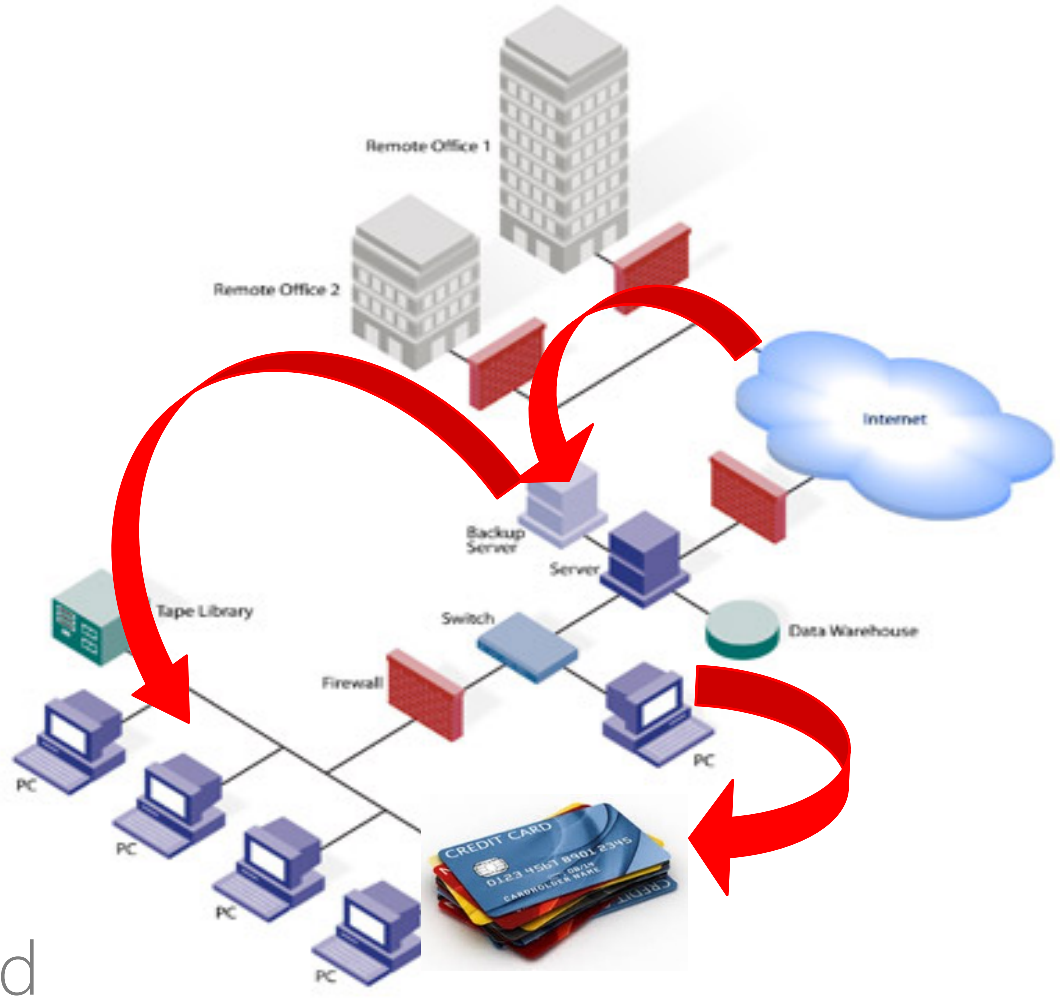
Effective Payment Threat Management

VISA

- Put yourself in a position to identify the breach before the fraud occurs
- Knowing and practicing incident response with TTPs
- Adapting defenses and response over time
- Include threat intelligence for relevant threats

Common Merchant Breach Scenario

- Attacker spear phishes employee
- Steals VPN login credentials
- Performs internal network reconnaissance
- Attacker elevates privileges
- Attacker gains access to AD Domain
- Attacker distributes POS malware
- Aggregates and exfiltrates payment card data



Components of a Working Cyber Defense

Intelligence-driven cybersecurity

- Collect, prioritize and share cyber intelligence
- Internal and external intelligence (what you observe and what others observe)
- Process to prioritize events
- Process to respond quickly
- Continually adapt defenses based on observed threats (and successful attacks)
- Practice incident response with a focus on evolving threats

Intelligence Sharing and Indicators of Compromise

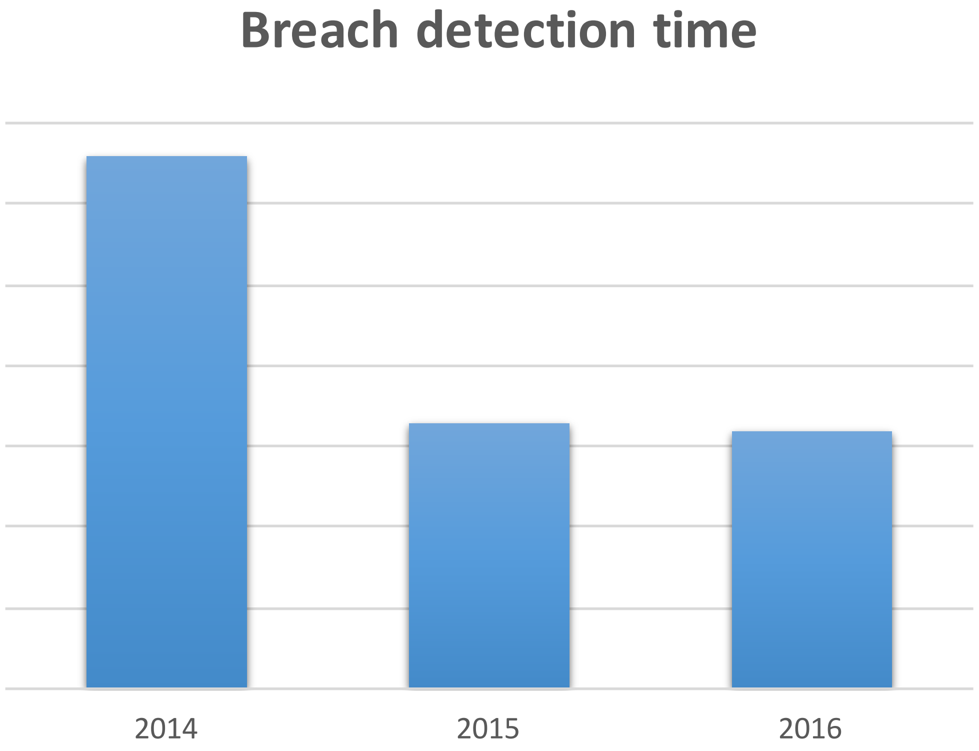
VISA

How important are IOCs to your business?

- Higher fidelity intelligence
- Operationalizing cyber intel and automation
- More reliable for earlier breach detection
- Reduce payment card fraud and the overall impact of a breach
- Streamline incident management
- Enables proactive cyber defense
- Aging of IOCs, what Visa sees

Visa's Results With Intel-led Breach Detection

Incorporating IOCs into breach detection reduced detection time



- Cut detection time in half from 2014
- Many detected compromises had little or no occurrence of fraud
- In many cases, Visa was the first to detect
- Intelligence for early detection now available throughout payment ecosystem