FIRST 2017 Technical Colloquium

Dec 6, 2017

The State of Point Of Sale (POS) Security

Glen Jones
Sr. Director, Visa Threat Intelligence

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.

Agenda

- Payment Ecosystem Breach Trends
- Current threats and breach trends
- Emerging threats to the payment ecosystem
- Effective threat management for payments
- Visa Threat Intelligence

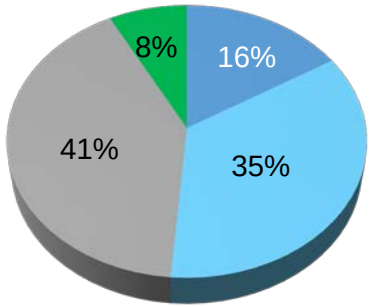
Payment Ecosystem & POS Breach Trends

Global Breach Trends - Overview

- The US and Europe represent the top two regions for data breaches
- Across all regions so far in 2017, we have seen about as many Visa accounts breached as all of 2016
- More breaches occur at e-commerce merchants, but the majority of stolen account data comes from Level 1 brick and mortar entities (~85%)
- 2017 saw a substantial increase in breached “Agents” (banks, processors)

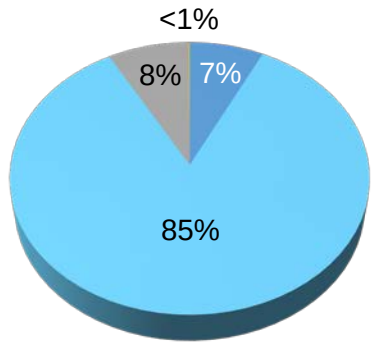
Global Breach Trends – By Channel and Entity Type

Total Breach **Alerts By Channel**



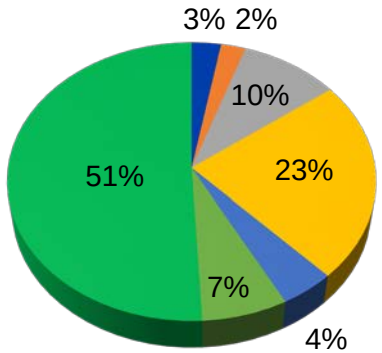
Agent Brick and Mortar Ecommerce Other

Total Breach **Accounts By Channel**



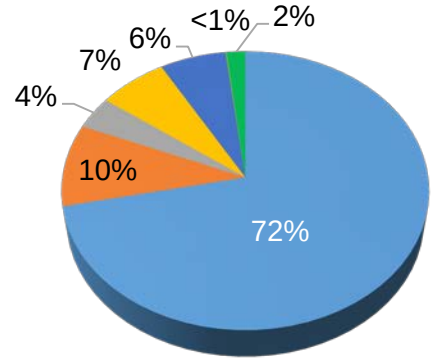
Agent Brick and Mortar Ecommerce Other

Total Breach **Alerts By Entity Type**



L1 L2 L3 L4 Agent Other EU

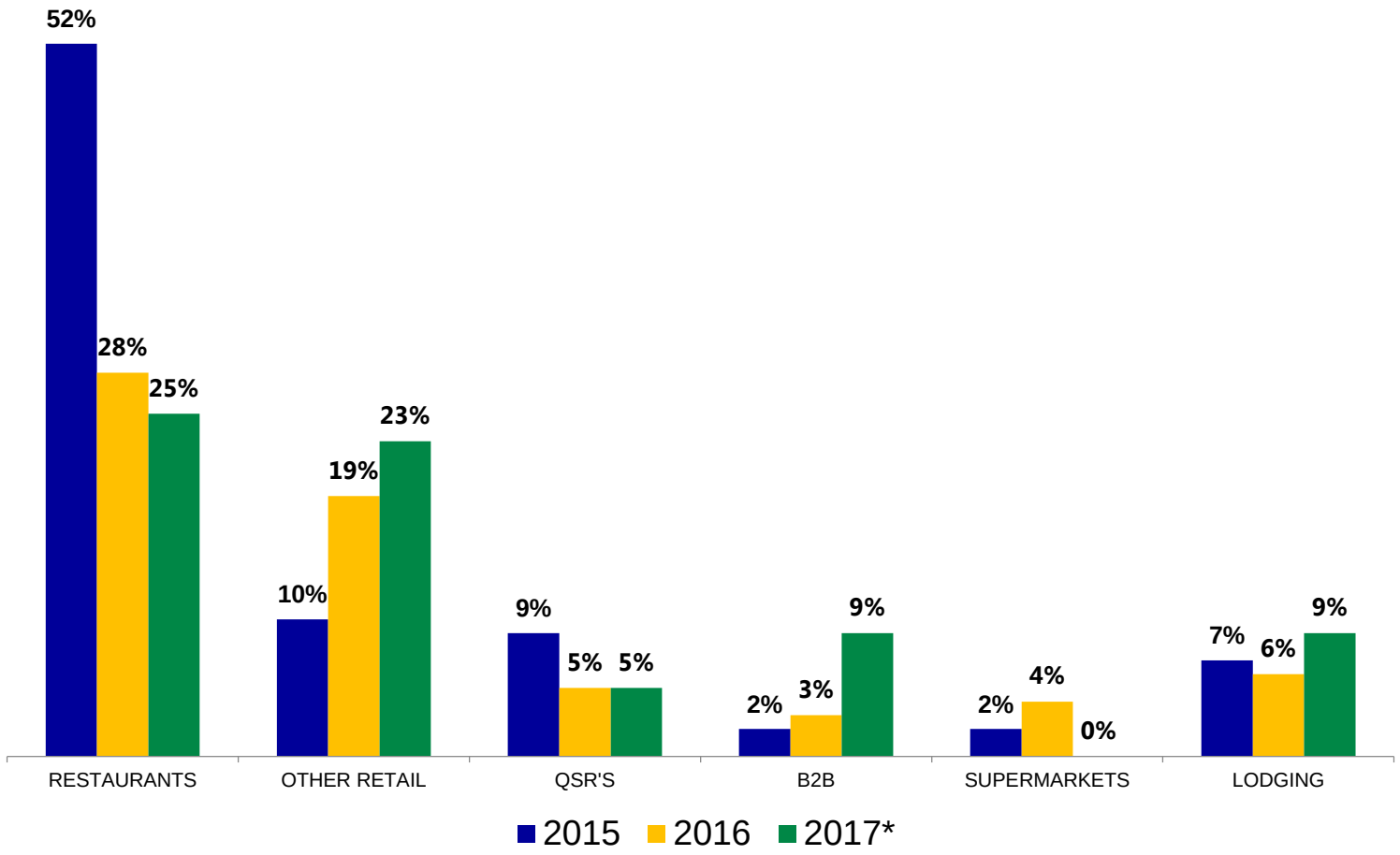
Total Breach **Accounts By Entity Type**



L1 L2 L3 L4 Agent Other EU

Global Breach Trends – By Merchant Type

- Restaurants, retailers and lodging (hotels) are the three leading market segments through the first six months of 2017
- Restaurant breaches continue a downward trend from prior years
- Retail breaches continue an upward trend, more than double from 2015
- There has been an increase of Business-to-Business (ecommerce channel) and as well as lodging breaches over the prior year



Evolved POS Malware

- Customized payment card-stealing malware
- Kaptoxa (BlackPOS), BlackPOSv2, Alina, Dexter, ModPOS, Backoff, FindPOS, RawPOS, Poseidon
- POS malware is not just RAM-scraping anymore:

  Screenshot-grabbing

  Keystroke logging

  Command-and-control

  Data exfiltration

  Self deletion (malware self-removal)
- POS malware becoming increasingly resistant to analysis

Emerging Point Of Sale 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)

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

Multi-Site “Land and Expand” Tactics

“With all the meteor activity in this system, it's going to be difficult to spot approaching ships”

- Attackers set up a hierarchy of breached merchants
- Conduct recon and launch attacks from legitimate merchants
- Exfiltrate payment card data through other merchants
- Attacker IPs and C2 servers are tough to spot, look like false positives

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?

Effectively Managing POS Threats

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

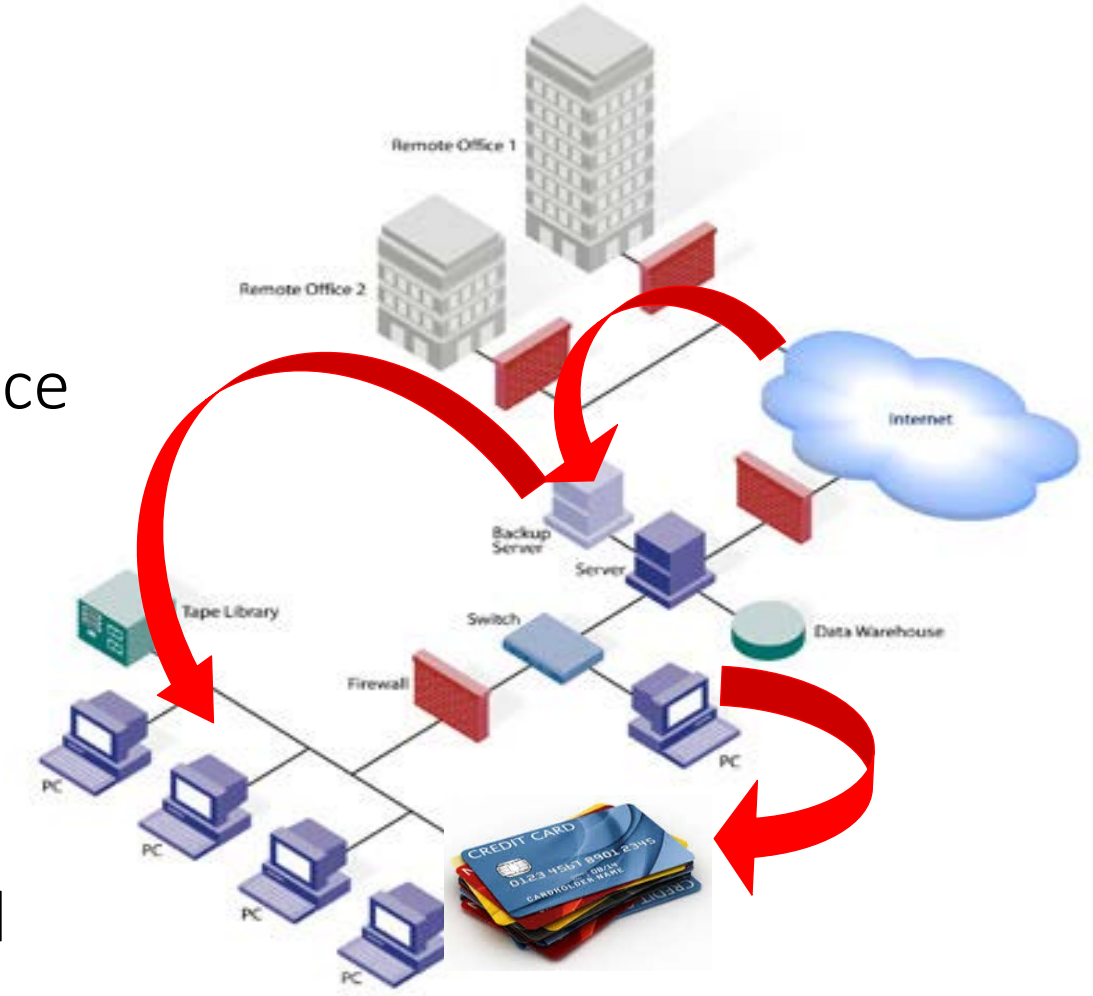
Actual forensic finding: "Investigation showed client's anti-virus system had been alerting *starting approximately 3 days after the breach* began but client was unaware or unresponsive to the alerts."

Effective Payment Threat Management

- 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

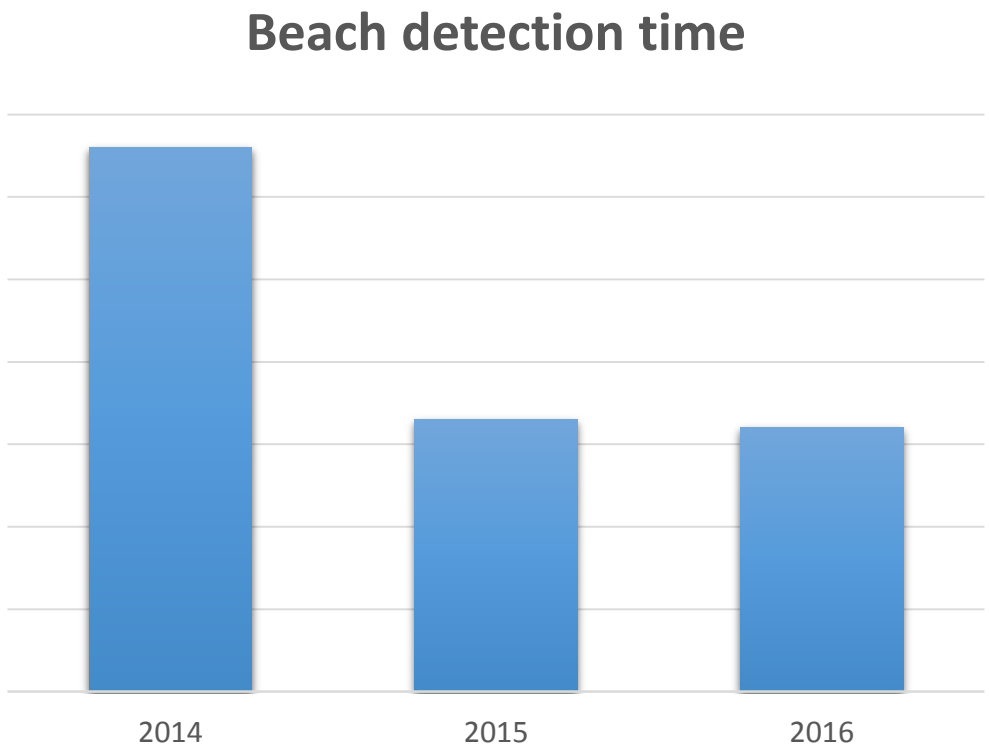
Intelligence Sharing and Indicators of Compromise

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

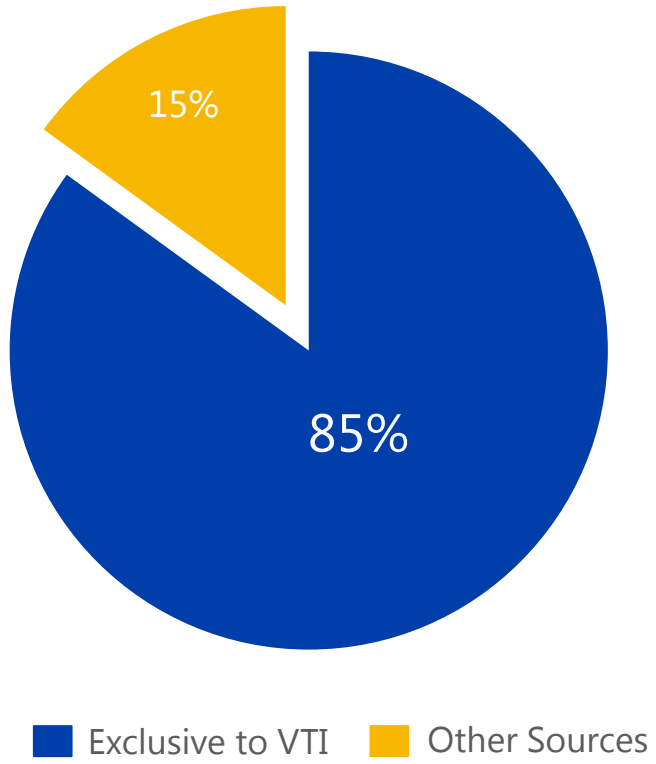


- Cut detection time in half from 2014
- Many detected compromises had little or no occurrence of fraud
- In many cases, Visa was the first to detect
- Intelligence for early detection now available throughout payment ecosystem

Why Visa for payment cybersecurity intelligence?

Visa Threat Intelligence Indicators of Compromise are not found in other leading threat intelligence tools[1]

Source of Forensic Indicators for Visa Threat Intelligence



[1] Visa. Based on a sample of Visa Threat Intelligence indicators compared to four commercial threat intelligence sources/vendors, 2016

Visa Threat Intelligence Integration Options

SIEM Integration: Correlation of IoC's with log data. Analysts create rules and alerting mechanisms to assist in breach identification, incident response and remediation.

Endpoint: Clients utilize the VTI API to configure endpoint monitoring for IoC's. This allows merchants to run endpoint scans for threat hunting on files and connections found in the VTI feed.

Firewall: IP addresses and domains from the IoC feed which are known to be malicious and unnecessary for daily operations can be blocked/quarantined/monitored at the firewall level to prevent connections and quickly detect malicious activity, helping to avoid breaches from occurring.

Third Party: Threat Intelligence Platforms, Simulated Breach Vendors, Operations Management

Vendor Integrations

SafeBreach
CISCO
ANOMALI
THREAT CONNECT
paloalto NETWORKS
THREATQ
Kroll
SIFT SECURITY
CENTRIPETAL NETWORKS
PERCH
STRATOZEN
sqrrl Target. Hunt. Disrupt.

Thank You

Questions?