2015 Visa Payment Security Symposium
The Power of Partnership
AUGUST 12-13 | HYATT REGENCY | BURLINGAME, CA

2015 Visa Payment Security Symposium Webinar

Diana Greenhaw – Sr. Director, Global Data Security and Third Party Risk
Lester Chan – Director, North America Merchant Security

2015 Visa Payment Security Symposium

Forward-Looking Statements

The materials, presentations and discussions during this meeting 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 “will,” new,” "continue," "could," “accelerate,” 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 plans and goals regarding authentication, risk and fraud, the effect of developments in regulatory environment, and other developments in electronic payments.

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 because of a variety of factors, including the following:

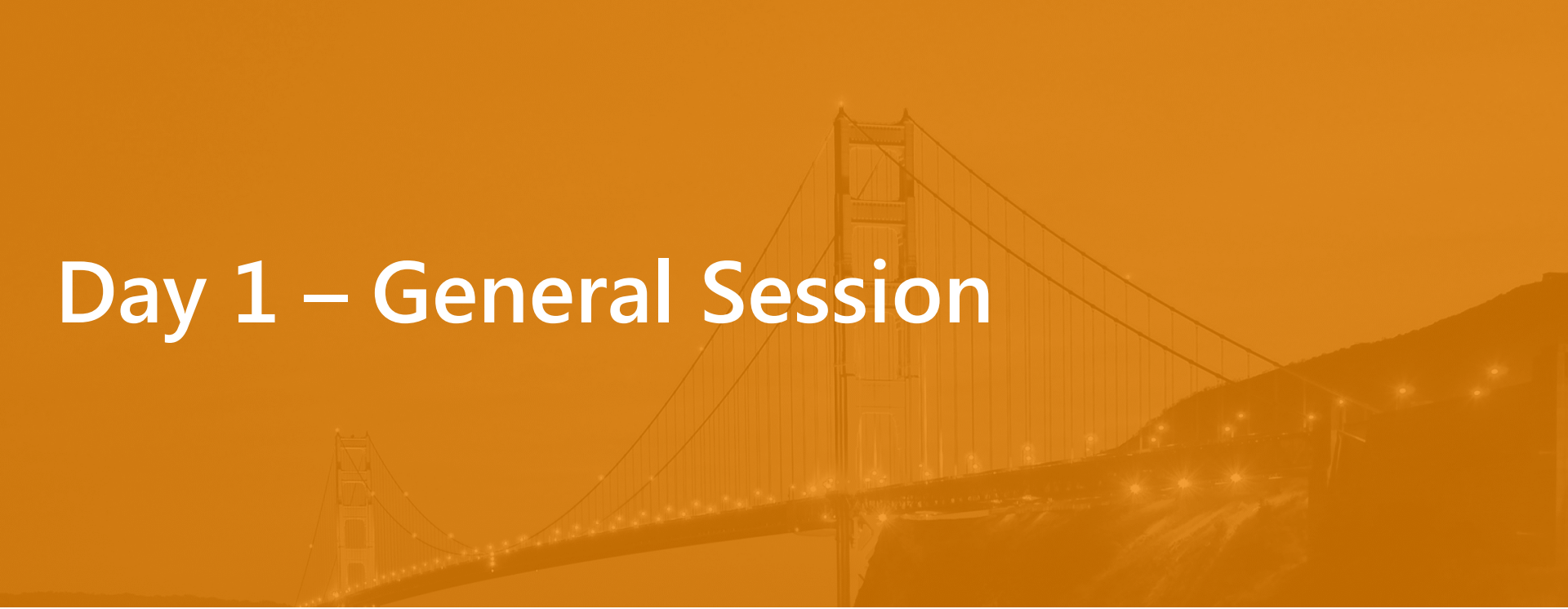
- the impact of regulation, including its effect on issuer and retailer practices and product categories, and the adoption of similar and related laws and regulations elsewhere;
- developments in current or future disputes
- macroeconomic and industry factors such as: global economic, political, health and other conditions; competitive pressure on customer pricing and in the payments industry generally; material changes in our customers' performance compared to our estimates; and disintermediation from the payments value stream through government actions or bilateral agreements;
- 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; increased fraudulent and other illegal activity involving our cards; failure to maintain interoperability between our and Visa Europe's authorization and clearing and settlement systems; loss of organizational effectiveness or key employees; and
- the other factors discussed under the heading "Risk Factors" herein and 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.

Notice of Disclaimer

The information, recommendations or “best practices” contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or “best practices” may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance.

Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.



Day 1 – General Session

Diana Greenhaw – Sr. Director, Global Data Security and Third Party Risk

VISA

2015 Visa Payment Security Symposium

Event Summary

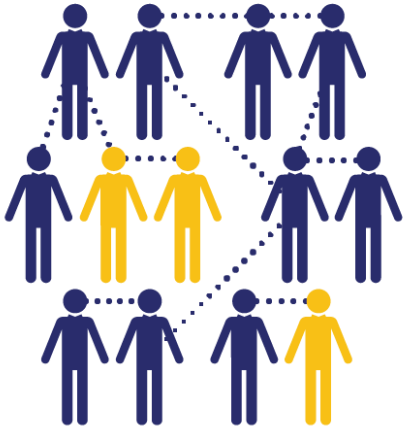
- Almost 400 participants from processors, third party agents, acquirers, merchants and event sponsors
- More than 40 industry expert panelists and speakers, including:
  - Ellen Richey, Vice Chairman – Risk and Public Policy, Visa Inc.
  - Mahesh Aditya, Chief Risk Officer, Visa Inc.
  - Jim McCarthy, Executive Vice President – Innovation and Strategic Partnerships, Visa Inc.
- Nine sponsors

Bluefin Payment Systems · Coalfire · ControlCase Compliance as a Service · FireEye · Modirum · securityMETRICS · SISA Payment Security Specialists · VirtuCrypt · VISA Data Secure Platform

2015 Visa Payment Security Symposium

The Power of Partnership: Securing the Future of Commerce Together

- Partners play a strategic role in securing the payment system
- Increasing involvement of non-traditional stakeholders and emerging technology organizations in payments
- Critical to maintain trust while extending payment environment and incorporating innovation



No one can do it alone!

After the Compromise: Lessons Learned

- Communication – at all levels – is key to successful incident management and resolution
- Organizations must understand the difference between the annual PCI DSS validation exercise and maintaining ongoing enterprise-wide data security
- Information sharing on cyber threats and compromise trends are critical to effective data protection
- You do not want to go through a compromise!

Heartland Payment Systems

globalpayments

Managing Risk with Secure Technology

- The future of payment system security is data devaluation
- Several technologies include inherent security features:
  - EMV Chip
  - Point-to-Point Encryption
  - Tokenization
- Organizations must use the solution that works best for their environment and understand how the technologies work together to create layers of security
- As emerging technologies continue to enter the payment environment, a key to success is the balance of innovation, convenience and security

2015 Visa Payment Security Symposium

U.S. EMV Migration Update

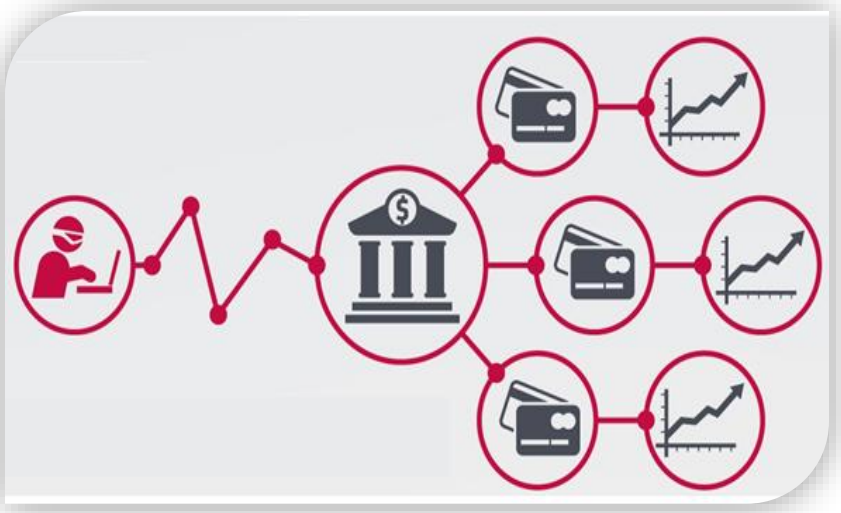
- U.S. EMV counterfeit liability shift – October 2015
- Liability shift date is not the finish line, but a starting point
- Multi-layered security approach provides best protection payment system stakeholders and downstream customers

- 117 Million EMV Chip Cards Issued
  - 78.1 Million Credit Cards
  - 39 Million Debit Cards
- 247,000 Activated EMV Terminals

Sources: Current cards based on MARS data through June 30, 2015; credit / debit card forecast per Aite Report – EMV: Lessons Learned and the U.S. Outlook (June 2014); activated terminal forecast per Payment Security Taskforce Acquirer projections press release (October 2014) ¹Forecast based on information currently available to Visa. Actual results may vary significantly.

Cyber Security Threats and Mitigation Strategies

- Security Metrics performed a "live" hacking demonstration illustrating how quickly hackers can access insecure systems to obtain cardholder data
- Criminals are shifting their attack methods and targets – the path of least resistance may not be where you think it is
- Information sharing between industry participants and law enforcement agencies will be key to combatting this type of crime



Data Security Regulatory Activity is Increasing

- In 2013, President Obama issued an Executive order directing the federal government to take steps to protect the nation's critical infrastructure from cyber threats
- In 2015, the FFIEC issued its cybersecurity assessment tool to aid financial institutions in evaluating their cyber risk and risk management capabilities
- The focus in the Senate has been on the "Cybersecurity Information Sharing Act of 2015"
- A number of individual states are amending security breach notice statutes
- State attorneys general continue to play a significant role on data security issues and breach incidents
  - Specifically, a large number are actively investigating various breach incidents that have occurred in the past two years

Day 2 – Breakout Sessions

Lester Chan – Director, North America Merchant Security

Malware POS Session Recap

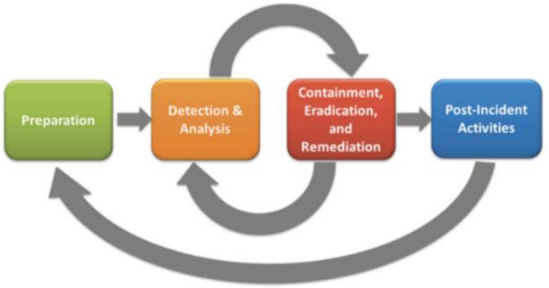
How POS Malware continues to proliferate and evolve with Palo Alto Networks

- Malware continues to be play a significant role in payment card breaches
- Four different malware type: file scraper, network sniffer, keylogger, and memory scraper
- Malware families are customized for different applications resulting in variants
- Coordinate with cyber threat intelligence to proactively monitor for malware
- Devalue payment card data and have a incident response plan
- Know and understand the warning signs and your environment

Incident Response Planning Session Recap

Incident response planning from Facebook

- Hire smart people and provide them tools to do their job
- Security incident plans should be small and flexible
- Sometimes only a limited amount of information is available
- Security incidents should be run and managed by people with experience
- Incident commander who is in charge and provide updates to management
- Red teams/blue teams are useful and don't limit their access



Incident Response Life Cycle

Network Segmentation & Zero Trust Session Recap

Benefits of next-gen firewalls and the Zero Trust principle with Palo Alto Networks

- Today's networks are extremely challenging with various devices and data
- Controlling the conversations and conversants make it easier to control security through policy
- Payment card data and devices such as iPads can easily be controlled on the network using next-gen firewalls
- Adding a Zero Trust policy can help organizations secure internal and external network connections

Securing the Payment Value Chain Session Recap

Discussing the hyperconnected value chain

- As the payment industry continues to evolve, the payment value chain is becoming more and more decentralized and it is no longer a simple 4 party model
- Hyper connectivity can increase complexity of managing risks and it is critical to ensure that all parties are accountable
- Breaches involving integrators and resellers are increasing
  - PCI SSC Qualified Integrator and Reseller (QIR) program provides training on secure POS system installation
  - MercuryPay recently partnered with Visa, Retail Solutions Providers Association (RSPA), and PCI Security Standards Council (PCI SSC) to offer training to its providers
- The industry must work together to educate small merchants and offer them simple and affordable solutions

Global Brand Protection – Global Acquirer Risk

Managing Online Pharmaceutical and Nutraceutical Merchants

- Acquirers must attain the pharmacy's valid and verified licenses for each jurisdiction where the merchant offers to ship prescription medication
- Be wary of merchants with wholesale pharmacy licenses
- Interpol will be heavily focused on preventing the illegal sale of medical devices
- It has become increasingly simple to create websites that look legitimate

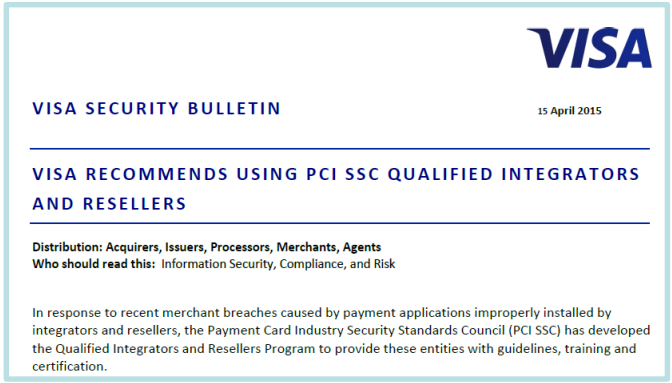
Acquirer Operational Risk Reviews

- Have a control environment in place to validate compliance with Global Acquirer Risk Standards (GARS)
- Ensure proper oversight of Agents
- When it comes to questionable merchants: Remediate or Terminate, DO NOT facilitate.

2015 Visa Payment Security Symposium

Third Party Agent Program Updates

- Criminals are sophisticated, but they are using the same attack vectors
- Post EMV, criminals may target aggregation points or entities with large amounts of data such as payment facilitators, processors, and gateways
- The Visa Registry of Service Providers (Global Registry) includes entities who meet Visa program rules and are PCI DSS validated, as applicable



VISA

VISA SECURITY BULLETIN 15 April 2015

VISA RECOMMENDS USING PCI SSC QUALIFIED INTEGRATORS AND RESELLERS

Distribution: Acquirers, Issuers, Processors, Merchants, Agents
Who should read this: Information Security, Compliance, and Risk

In response to recent merchant breaches caused by payment applications improperly installed by integrators and resellers, the Payment Card Industry Security Standards Council (PCI SSC) has developed the Qualified Integrators and Resellers Program to provide these entities with guidelines, training and certification.

Upcoming Events and Resources

Upcoming Webinars – Under Merchant Resources/Training on www.visa.com

- The Importance of Containment and Remediation of Compromised Payment Processing Environments, September 2, 2015

Visa Online Merchant Tool Kit provides helpful information to make a seamless EMV transition

- Streamline your chip migration – www.VisaChip.com/businesstoolkit

Visa Data Security Website – www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

PCI Security Standards Council Website – www.pcissc.org

- Data Security Standards, QIR Listing
- Fact Sheets –Mobile Payments Acceptance, Tokenization, and many more…