2014 North America Payment Card Security & Technology Symposium

Securing Our Future Growth:
Then, Now and into the Future

Webinar
20 August 2014

Disclaimer

The information or recommendations 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 or programs 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.

2014 North America Payment Card Security and Technology Webinar

Agenda

Presenter: Glen Jones, Senior Director | Global Forensic Intelligence, Visa Inc.

- Understanding the Evolution of Malware
- Optimizing Card-Not-Present Fraud Prevention Strategies

Presenter: John Sheets, Senior Director | Risk Products, Visa Inc.

- Demystifying Tokenization
- Navigating U.S. EMV Implementation
- Managing Mobile Payments Risk

Presenter: Jessica Scheppmann, Counsel | Corporate Legal, Visa Inc.

- Approaching the Intersection of Cyber Security and Privacy

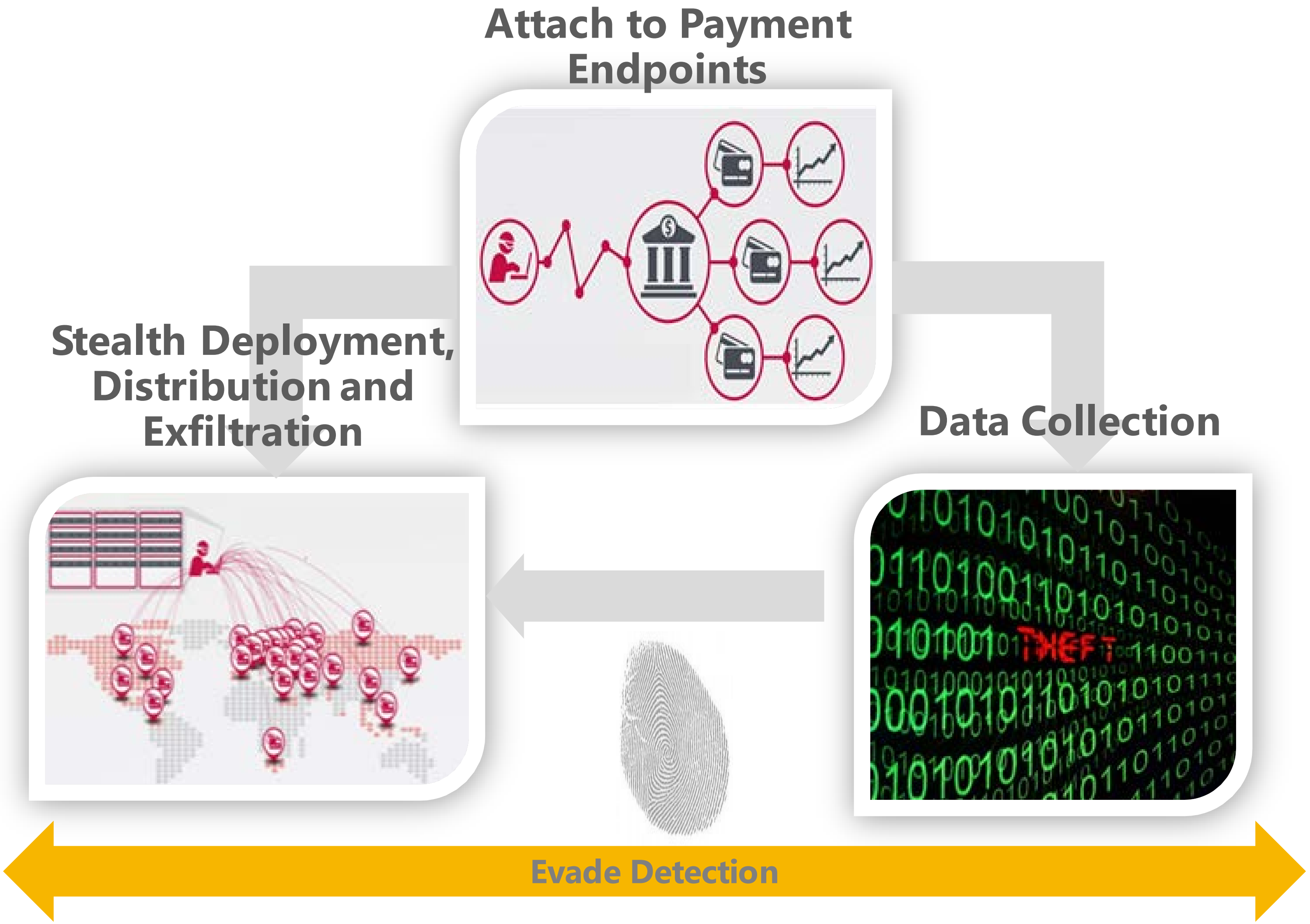
Understanding the Evolution of Malware

Optimizing Card-Not-Present Fraud Prevention Strategies

Glen Jones, Senior Director
Global Forensic Intelligence, Visa Inc.

Advanced Payment Card-Stealing Malware

Customized, Persistent



Attach to Payment Endpoints

Data Collection

Stealth Deployment, Distribution and Exfiltration

Evade Detection

Evolution of Malware Panel – Key Takeaways

1. POS malware has evolved from simple, commodity-variety to customized, very difficult-to-detect software

2. Detecting POS malware involves a combination of host and network monitoring

3. Detection cannot be done with tools alone, must include human action and polished processes

4. Intelligence-driven intrusion detection is more common in payment card cases

5. POS malware prevention involves application whitelisting, access restrictions, network-level controls

6. Private sector / law enforcement partnerships, like **Electronic Crimes Task Force**, play a big role in combating cybercrime

Card Not Present – Key Takeaways

1 With the continued growth of the CNP channel and US migration to EMV, CNP fraud is expected to increase before it stabilizes

2 While multiple authentication solutions are available and used by payments participants the key challenge for all stakeholders is to balance their fraud and security strategy with consumers' experience (minimal friction)

3 New technologies provide more insights into consumer behavior and spending patterns and this information exchange between issuers and merchants could open new opportunities in fighting CNP fraud

Demystifying Tokenization

Navigating U.S. EMV Implementation

Managing Mobile Payments Risk

John Sheets, Senior Director
Risk Products and Business Intelligence, Visa Inc.

Payment Token Definition

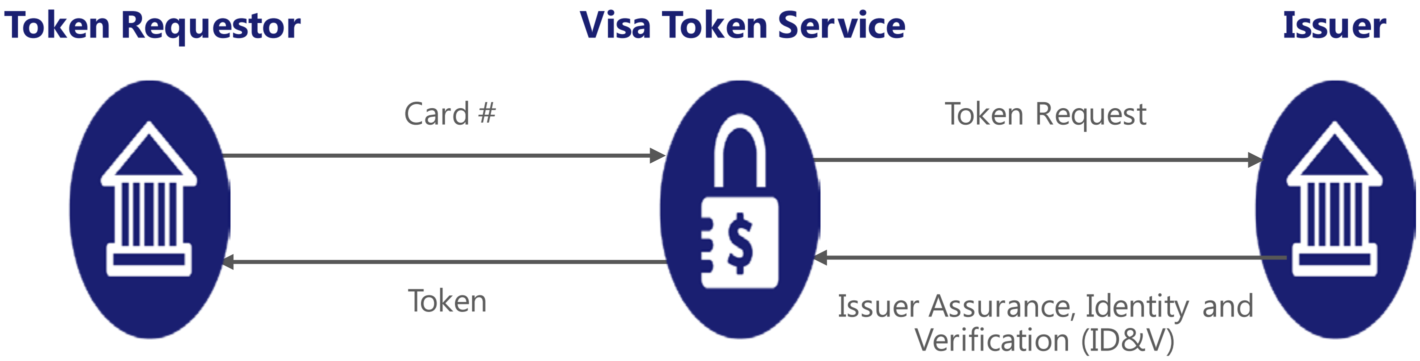
Tokenization involves the replacement of the card-account number with a "non-financial identifier" which may be used in its stead to initiate payment activity

Uses for Tokens

- Conduct payment transactions over online and mobile payment channels
- Provide a method for third-party payment enablement
  - Wallet
  - Near Field Communication (NFC)
  - Quick Response (QR) Codes
  - Other Emerging Technologies

Demystifying Tokenization - Payment Token Processing

1. Token Request Process



Token Requestor

Visa Token Service

Issuer

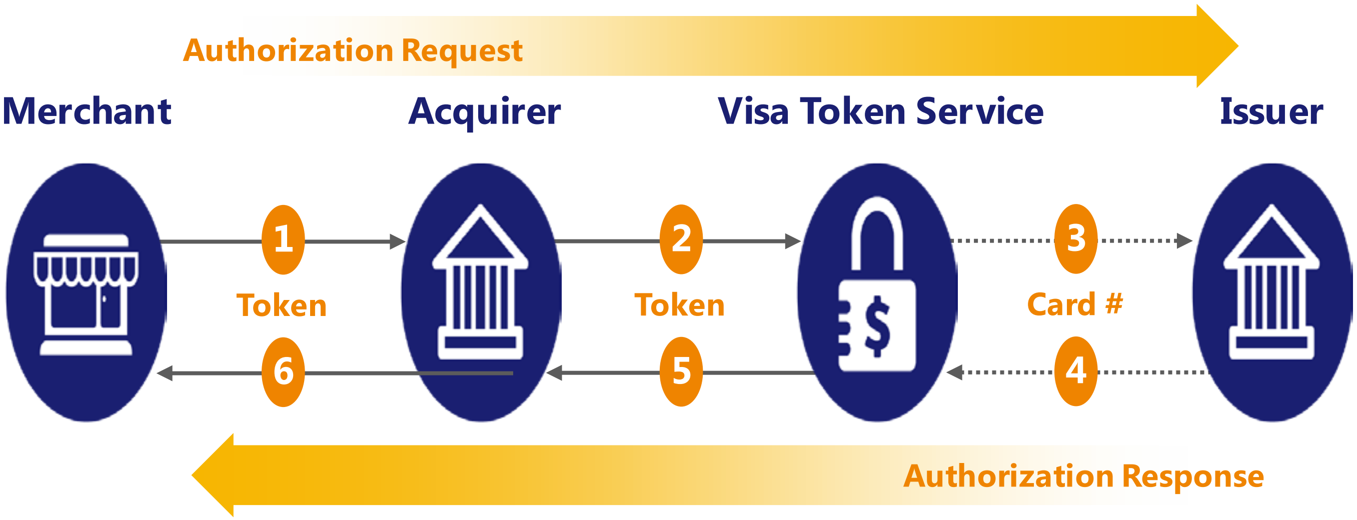
Card #

Token

Token Request

Issuer Assurance, Identity and Verification (ID&V)

2. Token Authorization Process



Authorization Request

Merchant

Acquirer

Visa Token Service

Issuer

1 Token

2 Token

3 Card #

4

5

6

Authorization Response

Demystifying Tokenization – Benefits for Ecosystem Participants

Common tokenization standard minimizes impact by ensuring compatibility with current payment technologies and enabling support for emerging payment innovations

Cardholder

- Card re-issuance not required if merchant database is compromised

Merchant/ Wallet Provider

- Increased data protection as sensitive card number (PAN) is not passed through the ecosystem
- A common approach to tokenization simplifies the process for merchants for contactless, online or emerging payments

Acquirer

- Reduced threat of sensitive cardholder data being compromised

Issuer

- Reduces overall cost of fraud by minimizing card re-issuance
- Reduced risk of subsequent fraud in the event of merchant data breach
- Issuers benefit from new and more secure ways to pay

Demystifying Tokenization – Key Activities

Industry Standard

- Donated to EMVCo by Visa
- A new EMVCo task force established to govern the standard going forward

VisaNet Processing

- November 2013 Technical Letter
- April 2014 Business Enhancements Release

Visa Payment Token Service

- Mid-2014 limited deployment anticipated in United States

Demystifying Tokenization – Key Takeaways

1. Tokenization has two main components: standard and service

2. Token replaces account number with a non-financial identifier

3. Issuers, acquirers/merchants, wallet providers and OEMs can be potential token requestors

4. A single PAN can have multiple tokens based on number of token requestors and channels

5. Limited deployment of Visa Token Service will start in later half of 2014

Navigating U.S. EMV Implementation – Key Takeaways

1. Chip is not a silver bullet – continue using a multi-layered approach to fraud management

2. As US EMV migration continues, there are already encouraging signs of progress in card issuance and terminal installation and at the industry level in addressing chip migration challenges that were impeding faster adoption.

3. There are solutions and test/certification processes already in market to facilitate EMV terminal deployments. Industry efforts are also underway to further streamline EMV terminalization so time to market for POS devices can be reduced.

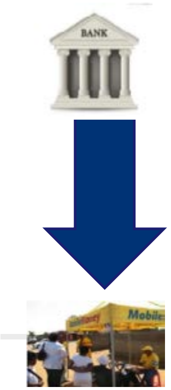
4. Chip implementations are more complex when compared against their magnetic-stripe counterparts. However, Online Only chip implementations are significantly less complex when compared to offline capable solutions.

5. Many industry stakeholders in the U.S. already have considerable EMV implementation experience

Managing Mobile Risk - Impact of Innovation

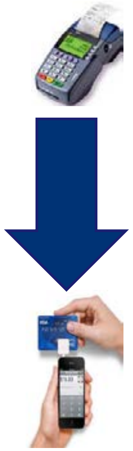
Enabling Payments

Everyone



- Network of agents
- Technological compatibility
- Low cost

Everywhere



- Enable new business models: Long-tail of merchants
- Multiple channels
- Multiple methods
- New business relationships

Every Channel

- Customized shopping preferences
- Frictionless checkout
- Trust and security
- Relevant real-time offers

Managing Mobile Risk - Key Takeaways

1

Use Existing Baselines and Strategies

All existing strategies, risk frameworks, process and procedures in place to address either fraud or data security risk applies for new technologies.

2

Focus on incremental changes

Identify the incremental changes brought about by the new technology and focus on addressing any incremental risks as a result of.

3

All Existing Domain Knowledge Still Works

As you review these incremental risks, understand that the fundamental principles and domain knowledge still works and applicable when assessing new technologies.

Approaching the Intersection of Cyber Security and Privacy

Jessica Scheppmann, Counsel
Corporate Legal, Visa Inc.

Cyber Security and Privacy

- Privacy – Based on societal norms that people are entitled to keep aspects of their lives and activities private.
- History –
  - Europe – In Europe and other countries that have followed its lead, privacy is considered a fundamental human right that requires entities to inform citizens when information is collected and obtain consent for any use.
  - United States – Historically, rather than implementing comprehensive legislation, the U.S. has regulated areas where misuse of information can cause the most harm, such as financial and health information, and information belonging to children.
- Today – New privacy regulation is just around the corner in the EU, and in the U.S., the White House, FTC, and the Supreme Court are all discussing how we must rethink privacy in light of technological innovation.

Cyber Security and Privacy - Discussions

- Which consumers are most focused on data security and privacy?

- What are consumers’ top concerns with respect to data security and privacy?

- Why should merchants care about consumer privacy?

Cyber Security and Privacy - Key Takeaways

1

The majority of consumers today are making buying decisions based on their perception of a merchant's commitment to data security. Maintaining trust is paramount to acquiring and preserving customer relationships.

2

Although there is no sign of a uniform U.S. federal law on the immediate horizon, U.S. regulators are increasingly focused on the following:

(a) notice and disclosure to consumers;

(b) ensuring that any entity collecting personal information is limiting data use only to those activities disclosed to consumers;

(c) or obtaining specific consent from users regarding the use of their confidential data.

Upcoming Events and Resources

PCI Security Standards Council (SSC) North America Community Meeting: http://community.pcisecuritystandards.org/2014/

- September 9 - 11, 2014
- Orlando, Florida
- Visa Acquirer Roundtable on September 9, 3 pm – 5 pm EST
  - For acquirers only
  - Email cisp@visa.com for more details and registration
- Visa to host "office hours" throughout the Community Meeting
  - Participating organizations are encouraged to take advantage of this unique opportunity to engage with Visa subject matter experts

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

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

Questions?