Maintaining Trust:
Visa Inc. Payment Security Strategy

Ellen Richey
2010 Payments Conference
Chicago Federal Reserve
Global Electronic Payments

Protecting the payment system is a shared responsibility among participants

16,100 financial institutions

62 billion total transactions*

$4.4 trillion in total volume*

Source: Visa Inc data for 12 months ended December 2009
Cyber Security… Not Just a Card Problem

All Data Loss Events

- Card Breach Events
- Incidents
- Records
- Card Accounts

Global Payment Card Compromises

- 37% US and 63% Non-US
- 44% brick and mortar and 52% e-commerce merchants

Source: Public Data Loss Statistics Tracked by Datalossdb

Source: Visa Client Reports
Controlling Fraud Through Innovation

Innovations on all fronts including:
- Risk tools
- Standards and oversight
- Education and partnership

Source: Visa TC40 Fraud Reporting (as of March 2010)
Major Security Initiatives

Global PCI Compliance

Level 1 Merchants: 87%
Level 2 Merchants: 79%

Global Chip Deployment
Data Thieves Relentless

- Reduce stored card data
- Drive PCI among U.S. large merchants
- Number of U.S. compromises decreasing
- Implement EMV chip
2010: The Security Challenge

Fraudsters have evolved their business models and migrated between channels, products and geographies.

Criminals continue to adapt and challenge the system:

- The number of compromise incidents involving cardholder information has grown globally.
- Stakeholder costs are increasing.
- Security tops consumer concerns.
- Regulatory attention and intervention on the rise.

Visitors to a Brazil bank’s web site were redirected to a counterfeit site designed to steal customer credentials.

Carpark scam keeps banks busy. Customer told 100,000 credit cards need to be replaced.

The Menace in the Machines – Cyber-Scams On the Uptick In Downtown
M.P. McQueen
29 January 2009

Falling economy pushing cybercrimes up
May 21, 2009

The Washington Post

The New Zealand Herald
Payment System Risk Strategy

Maintain Trust in Visa Payments

- **PROTECT**
  - Stop thieves from stealing vulnerable data

- **RESPOND**
  - Mitigate impact of threats and attacks

- **PREVENT**
  - Eliminate re-usable data

Partner with Clients & Stakeholders
**Protect the System**

Lead the industry in protecting vulnerable payment data

<table>
<thead>
<tr>
<th>Standards</th>
<th>Education</th>
<th>Tools</th>
<th>Oversight</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Data Security</td>
<td>- Training and Consulting</td>
<td>- Device and service testing</td>
<td>- Incentive Programs</td>
</tr>
<tr>
<td>- Application and Device Security</td>
<td>- Implementation guidance</td>
<td>- Analytics and Reporting</td>
<td>- Requirements and Mandates</td>
</tr>
<tr>
<td>- Encryption</td>
<td>- Best Practices and Guidelines</td>
<td>- Alerts and Bulletins</td>
<td>- Partnerships and Compliance</td>
</tr>
</tbody>
</table>

**Opportunity:** Shrink the “Card Data Environment” to reduce stakeholder cost and risk
**Respond to Threats**

Minimize the impact of threats on stakeholders through early identification and advanced event management

<table>
<thead>
<tr>
<th>Identify</th>
<th>Analyze</th>
<th>Mitigate</th>
</tr>
</thead>
</table>
| - Consumer Alerts  
- Fraud ID systems | - Point of Compromise Tools | - Proactive Alerts  
- Authorization Solutions |
| Programs & Processes | | |
| - Cyber Intelligence & Investigations  
- Fraud Control Programs | - Zero Liability  
- Incident Response | |
| Information & Partnerships | | |
| - Intelligence Sharing  
- Risk Councils | - Performance Benchmarking | - Risk Services  
- Public/Private Partnerships |

**Opportunity:** Identify attacks earlier to shut down fraud faster  
Empower consumers to protect themselves from fraud
**Prevent Attacks**

Reduce the incentive for criminals to steal data by eliminating re-usable data from the system

- **Authenticate Participants**
  - Signature/PIN
  - Passwords
  - Challenge – Response
  - One time pass-codes

- **Authenticate Devices**
  - CVV/CVV2
  - dCVV
  - IP Validation
  - Smart Cards
  - Tokenization
  - Trusted PC

Only the legitimate customer can initiate a transaction

Data can only be used for the original transaction

**Static Data** ➔ **Dynamic Data**

**Opportunity:** Make transaction data useless by moving to dynamic authentication technologies
20/20 Vision
The Future of Payments Security

1. **Dynamic Authentication**: to take the majority of stakeholders out of harm's way

2. **Powerful Security**: among stakeholders who retain vulnerable data

3. **Intelligent Response**: to identify threats, shut down fraud, and minimize the impact of attacks

4. **Solutions that Engage Consumers**: to protect themselves from fraud

5. **Innovation, Leadership & Collaboration**: partnering with stakeholders to maintain trust in electronic payments