Agenda

1. The Data Security Landscape
2. Recent Trends
3. Visa’s Strategy
4. Working with the Public Sector
Complex Payment Landscape

- Direct Mail Marketers >1,000
- Reporting Vendors <50
- Call Center Vendors >1,000
- Fulfillment Vendors 100’s
- Chargeback Vendors <100
- Loyalty Vendors <100
- Archiving Vendors >100
- Mail/Couriers >100
- Other Vendors 1,000’s
- Risk Scoring Vendors >1,000
- Telecom Infrastructure Vendors 100’s
- POS Software Vendors ~1000
- POS Hardware Vendors <50
- Aggregator/Master Merchants 100’s
- Gateway Provider >1,000
- Other Networks <50
- Direct Mail Marketers
- Data Entry Vendors
- Call Center Vendors
- Collections Vendors 1,000’s
- Card Embossers <50
- Loyalty Vendors <100
- Archiving Vendors >100
- Mail/Couriers >100
- Other Vendors <100
- Statement Vendors <25
- Issuer Processors <25
- Bill Payment 1,000’s
- Other Financial Relationships 1,000’s
- Other Vendors
- Visa Inc. and Visa Europe

Numbers illustrative, US Market only
### Sophisticated and Organized Criminals

#### Estimated market value of compromised accounts*

<table>
<thead>
<tr>
<th>Type of Card</th>
<th>Data Type</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account number and CVV2</td>
<td>Classic track data</td>
<td>$1</td>
</tr>
<tr>
<td>Classic track data</td>
<td>Gold/Plat/Corp track data</td>
<td>$15</td>
</tr>
<tr>
<td>Gold/Plat/Corp track data</td>
<td>Semi-finished blank plastic</td>
<td>$30</td>
</tr>
<tr>
<td>Complete counterfeit Gold plastic</td>
<td>White-Plastic</td>
<td>$80 - $100</td>
</tr>
<tr>
<td>Track data and PIN</td>
<td>Finished</td>
<td>$250</td>
</tr>
<tr>
<td></td>
<td>Finished</td>
<td>$1,000**</td>
</tr>
</tbody>
</table>

---

*Source: The United States Secret Service

**Typically track data and PIN not for sale; profit share arrangement amongst criminals; estimated criminal profit per card
Cardholder Concerns About Card Use

Security and protection of personal information now tops consumer concerns… Despite concerns, Visa cardholders recognize they are protected from fraud.

- That you may become a victim of identity theft: 43%
- That your card may be used to make a fraudulent transaction: 16%
- You may be accumulating too much debt: 15%
- That your personal information may be stored by the merchant: 14%
- You might be charged a transaction fee: 3%
- The store doesn’t accept your card brand: 2%
- Your card may be declined: 1%
- None of these: 3%
- Don’t Know/Refused: 3%

Recent Trends

• The number of compromise incidents in the U.S. is rising
  – Trend suggests Level 4 merchants targeted
  – Level 1 merchant compromises subsiding

• Incidents outside the U.S. are also increasing

• But global fraud rates have remained stable since 2002
  – Visa and system participants have been more effective at combating fraud
  – Mix of fraud is changing
    • Lost and Stolen is on the decline
    • Counterfeit and Card-Not-Present are now category leaders
Visa’s strategy

Maintain Trust in Visa Payments

PREVENT
Keep Data Out of Criminal Hands

PROTECT
Prevent Thieves from Using Stolen Data

RESPOND
Monitor and Manage Incidents to Reduce Impact

Partner with Clients & Stakeholders
# Top System Vulnerabilities

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Remediation Efforts</th>
</tr>
</thead>
</table>
| **Storing prohibited data** *(Track, CVV2, PIN)* | *PCI DSS; PCI PA-DSS, PCI PED, PIN Security Requirements*
|                                       | Delete stored data; prevent future storage; replace vulnerable software              |
| **Out of date security / systems patches** | *PCI DSS, PCI PA-DSS*
|                                       | Establish policies, procedures and processes for maintaining and updating systems that handle sensitive data |
| **Inadequate perimeter security**      | *PCI DSS*
|                                       | Execute disciplined firewall policy management and network security; conduct routine penetration tests of all systems |
| **Weak wireless security**             | *PCI DSS*
|                                       | Utilize strong encryption to protect wireless environments                            |
| **SQL injection attacks**              | *PCI DSS*
|                                       | Conduct regular testing of susceptibility to SQL injection utilizing automated tools or manual techniques |
Working with the Public Sector

• **Public Officials:**
  – Consistent public policy to effectively and efficiently secure the payment system
  – Data security legislation with reasonable security requirements, risk-based notifications, and national uniform standards
  – Global law enforcement initiatives to prosecute criminal organizations

• **Visa:**
  – Education and training for public agencies, regulators, and law enforcement
  – Investigative support for law enforcement and other stakeholders
Final Thoughts on Security

Protecting the payment system is a shared responsibility for all payment system participants

Everyone has an important role to play:

- Issuers
- Acquirers
- Merchants
- Cardholders
- Processors
- Third Party Agents
- Public / Government Officials
- Law Enforcement