EMV Chip Cards
Not as Scary as it Used to be

Brian Hamilton
Senior Director – Risk and Authentication Products
Visa Inc.

October 26, 2016
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.
Agenda

Fraud Landscape

EMV Update

EMV Quick Chip

Questions
Fraud landscape today

Counterfeit fraud represents 69% of card-present fraud and is growing

**Total fraud by type**
- **Counterfeit**: 42%
- **Card not present**: 42%
- **Lost/stolen**: 11%
- **Other**: 5%

**Card-present fraud**
- **Lost/stolen**: 15%
- **Counterfeit**: 16%
- **Other**: 16%
- **Counterfeit**: 69%

EMV chip will significantly reduce card-present **counterfeit fraud**

Source: Visa Fraud Reporting System (FRS); Reporting window YE 2015; U.S. issued / U.S. acquired Visa debit and credit – debit includes interlink
Fighting fraud from every angle

**EMV**
- Creates a unique cryptogram for each transaction
- Not a silver bullet

**VCAS**
- Dynamic, risk-based authentication
- Reduces friction at the POS

**Tokenization**
- Replaces PAN with unique digital alias
- If payment token is used as the PAN*, it will be identified as stolen and rejected

**PIN**
- Fraudster must know PIN for card to work
- Static data set

**Biometrics**
- Enhances cardholder verification
- Reduces friction at the POS

Source: Visa Fraud Performance Benchmarking. Reporting window YE 2015. Remaining percentage fall under “Other” fraud types. U.S. Fraud by Type (% = share of total)

*Primary Account Number
How does EMV chip technology work?

Because the cryptogram changes with every transaction, even if the card data is stolen, the information can’t be used to create counterfeit cards because the cryptogram would have already “expired”
Visa U.S. EMV chip roadmap

- In August 2011, Visa led the industry by setting a plan to move the U.S. to EMV chip technology
- Successful globally, liability shifts have been the primary tool used to encourage both issuers and merchants to adopt EMV chip technology

<table>
<thead>
<tr>
<th>Date</th>
<th>Acquirer EMV Chip</th>
<th>ATM Processing</th>
<th>POS Liability Shift</th>
<th>AFD* Liability Shift</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2013</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>April 2015</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>October 2015</td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>October 2017</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

*AFD = automated fuel dispenser

<table>
<thead>
<tr>
<th>Card</th>
<th>Terminal</th>
<th>Liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mag stripe only</td>
<td>Mag stripe only</td>
<td>Issuer</td>
</tr>
<tr>
<td>Mag stripe only</td>
<td>Mag stripe only</td>
<td>Issuer</td>
</tr>
<tr>
<td>Mag stripe only</td>
<td>EMV chip</td>
<td>Issuer</td>
</tr>
<tr>
<td>EMV chip</td>
<td>Mag stripe only</td>
<td>Acquirer</td>
</tr>
<tr>
<td>EMV chip</td>
<td>EMV chip</td>
<td>Issuer</td>
</tr>
</tbody>
</table>
U.S. EMV chip migration status as of Sept. 2016

52% of US cards now have chips that resulted to 82% of payment volume

**Adoption**
- **176.0M**
  - US issued EMV Visa credit cards
  - 94% PV
- **196.9M**
  - US issued EMV Visa debit cards
  - 68% PV
- **1.64M**
  - US EMV Visa acceptors
  - 39% PV

**Usage¹**
- **32.2%**
  - US credit card chip on chip transaction
  - 40.8% by PV
- **16.1%**
  - US debit card chip on chip transaction
  - 23.0% by PV

**Fallback²**
- **2.1%**
  - US EMV credit card fallback rate
  - 2.0% by PV
- **3.6%**
  - US EMV debit card fallback rate
  - 3.5% by PV

*Sources: Current cards based on MARS data through September 30, 2016.*

¹Visa branded chip cards processed as chip transactions.
²Magstripe transactions using a Visa branded chip card in a chip terminal.
Merchant Chip-on-Chip Transaction Rates

Key Merchant Categories Have Made Significant Strides*

- Electronics: 79%
- Drug Stores/Pharmacy: 62%
- Home Improvement: 57%
- Food/Grocery: 50%
- Discount Stores: 49%
- Department Stores: 49%

*Source: VisaNet Data for August 2016
Chip Card Issuance by State

Penetration of Chip Cards

- 70%+
- 60-69%
- 50-59%
- 40-49%

Source: VisaNet Data as of September 30, 2016. Chip card transactions at Mag Stripe or EMV terminals (based on 201 service code)

EMV Migration - Not as Scary as it Used to Be
U.S. EMV Chip Migration Status

Counterfeit Fraud Continues to Decrease

For merchants who have completed the chip upgrade, counterfeit fraud dollars dropped 54% in June compared to a year earlier.

Source: https://usa.visa.com/visa-everywhere/security/chip-technology.html
EMV Testing and Certification Update

- **Visa announced EMV chip roadmap in 2011** to give the industry time to plan and adopt EMV on their own timeframe
- Visa has been working with acquirers, processors, and point of sale providers on programs aimed at increasing the speed of certifications
- Visa has **streamlined testing requirements** for chip terminals that can reduce certification timeframes by as much as 50 percent
  - Published a revised set of “minimum” test scripts in Dec 2015
    - Reduced the number of test scripts by over 50%, from 35 to 14
    - Acquirers can self-certify and complete testing in less than an hour
- Many merchants are dependent on Value Added Resellers (VARs) to develop and implement their terminal software
  - VARs can pre-certify their software solutions using 3rd parties to **reduce the testing that the acquirer/processors need to do by up to 80%**
  - Visa **provides hands-on support** to VARs who need technical information, education, consulting, and training. A dedicated team of experts are available to provide direct support.
EMV Chargebacks

In June, Visa announced the following changes to our chargeback policies

– **Minimum Chargeback Amount**
  Effective 22 July 2016 through April 2018, a **$25 minimum amount** will be required for allowable counterfeit chargebacks on U.S. domestic card present transactions

– **Maximum Chargebacks per Account**
  Effective from October 2016 through April 2018, a **maximum of 10 counterfeit fraud chargebacks will be allowed per account** in 120-day period for U.S. domestic card present transactions
Visa Quick Chip for EMV® speeds up checkout times on chip transactions at the point of sale and optimizes the consumer experience while providing the same level of EMV security, including the cryptogram.

EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries.
With Quick Chip, merchants and their customers benefit from a faster EMV check out experience.
Reduce development & testing time by up to 85%.
Introducing Quick Chip

1. Insert the card face up, chip end first

2. Remove card when prompted. Processing should take about 2 seconds or less.

3. Follow prompts on screen to finalize transaction
Counterfeit fraud mitigation best practices
Point-of-sale merchants who are not EMV-chip enabled

Read and compare verification

Be on the lookout for highly suspicious transactions

- High-value purchases such as prepaid cards, electronics, jewelry or large amounts of merchandise
- Use common sense
- Know what behavior is normal for your business
Visit www.visachip.com
Online destination for merchants, acquirers, issuers, service providers and consumers

EMV Migration Forum
• www.emv-connection.com
• gochipcard.com

Testing Documentation
• Visa Inc. U.S. EMV Chip Terminal Testing Requirements
• Visa Minimum U.S. Online Only Terminal Configuration and Quick Chip
• Visa Chip Bytes and more.....
Questions?
Upcoming Events & Resources

• **Upcoming Webinars** – [www.visa.com/cisp](http://www.visa.com/cisp)
  —November 16, 2016 – Top 10 Signs your Payment Network is Breached

• **Visa Data Security Website** – [www.visa.com/cisp](http://www.visa.com/cisp)
  —Alerts, Bulletins
  —Best Practices, White Papers
  —Webinars

• **PCI Security Standards Council Website** – [www.pcissc.org](http://www.pcissc.org)
  —Data Security Standards – PCI DSS, PA-DSS, PTS
  —Programs – ASV, ISA, PA-QSA, PFI, PTS, QSA, QIR, PCIP, and P2PE
  —Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more...