Guarding Against Card-Not-Present Fraud

Sylvia Auyeung – Merchant Risk
Nathan Wood – CyberSource
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.
Agenda

• CNP trends
• Key mobile trends
• How prevalent is mobile commerce?
• Is mCommerce riskier than eCommerce?
• What is the right fraud strategy for mCommerce transactions?
• How do you configure your solution to minimize mCommerce fraud?
• Q&A
The amount of data is enormous and growing

Email users send
204,166,667 messages

Google receives over
2,000,000 search queries

Facebook users share
684,478 posts

Twitter users send over
100,000 tweets

644,444 phishing emails sent

every minute.

What’s driving the massive data creation?

In 2015....

4.9 billion connected devices

In 2020....

25 billion connected devices

Source: Gartner
Why are we talking about Card Not Present (CNP)?

$3.5T
GLOBAL ECOMMERCE SALES WILL DOUBLE FROM 2015 TO 2019

$1.7T
Challenge: Optimize authorization and fraud management practices to maximize the growth of ecommerce and digital payments

Source: eMarketer July 2015, includes online and mobile ecommerce
Mobile Fraud

Convert more mCommerce orders with less fraud
68% of U.S. adults have a smartphone, up from 35% in 2011, and tablet computer ownership has edged up to 45% among adults.
Mobile made its presence known over the holidays

1 in 5 U.S. online holiday purchases made over mobile

44% of smartphone users said they made a purchase from their device, up from 41% a year ago

Source: 1 "Mobile accounts for nearly 1 in 5 online holiday purchases", Internet Retailer, January 8, 2016 http://bit.ly/1Pjygcm
2 "Survey Shows Rapid Growth in Online Shopping", Wall Street Journal, June 8, 2016 http://on.wsj.com/1PgQjod
Overall fraud loss by order channel

- Webstore: 0.8% in 2015
- Mobile commerce: 0.5% in 2015
- Telephone: 0.5% in 2015

Source: CyberSource Online Fraud Management Benchmark Report, 2016
Few merchants track mobile fraud

Source: CyberSource Online Fraud Management Benchmark Report, 2016
## Is mCommerce any riskier?

<table>
<thead>
<tr>
<th><strong>Customer/preventions</strong></th>
<th><strong>No</strong></th>
<th><strong>Yes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Omni present</td>
<td></td>
<td>• Easier to steal</td>
</tr>
<tr>
<td>• Personal identification number (PIN) lock prevents access and usage</td>
<td></td>
<td>• Customer apathy</td>
</tr>
<tr>
<td>• GPS to quickly locate and deactivate</td>
<td></td>
<td>• New threats: Rogue apps, malware, “smishing”</td>
</tr>
<tr>
<td>• Biometrics (Siri)</td>
<td></td>
<td>• Man-in-the-middle subverts SMS verification</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Merchant/mitigations</strong></th>
<th><strong>No</strong></th>
<th><strong>Yes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• New data elements to determine identity</td>
<td></td>
<td>• Variable internet protocol (IP) addresses and “diluted” digital fingerprint</td>
</tr>
<tr>
<td>• Mobile network security more secure than WiFi</td>
<td></td>
<td>• App “fatigue” and privacy considerations</td>
</tr>
<tr>
<td>• New validation methods (short message service (SMS))</td>
<td></td>
<td>• New customer behavior/norms/history</td>
</tr>
</tbody>
</table>
Device preferences throughout the day

Traditional fraud strategies need to be “tuned”

Device Shifting: Daily Trends
(Global Q3 2014)

Source: OOYALA Global Video Index, Q3 2014 http://bit.ly/1KxEVkb
What is a “mobile” transaction?

All devices are not created equal

**Percentage of volume by device type**

- iPad: 56.4%
- Android: 16.1%
- iPhone tablet PC: 19.2%
- Windows tablet: 0.8%

**Fraud “pressure” by device type (fraud chargebacks + cancels)**

- iPad: 3.2%

Source: Decision Manager, January – June 2015 Global credit card transactions for transactions where the device was identified
Global view of mobile rates

Mobile volume as a % of total

- North America: 40.3%
- Asia Pacific: 17.7%
- Europe: 12.5%
- South America: 12.4%
- Eastern Europe: 6.8%

Fraud “pressure” rates by revenue

- North America: 6.38%
- Europe: 4.57%
- Eastern Europe: 4.90%
- South America: 14.13%
- Asia Pacific: 3.98%

Source: Decision Manager, January – June 2015, mobile phones only, Global credit card transactions
Fraud management is a balancing act, including mobile

**Accurate detection**
- Reduce fraud rate
- Help minimize chargebacks

**Positive customer experience**
- Reduce false positives
- Increase acceptance rates
- Lower review rates

**Efficiency**
- Maximize automated decisioning
- Streamline review process
Managing mobile fraud on your platform

Order data
- Cross-channel activity
- Velocities
- Risk models
- IP geo-location
- Device fingerprint
- Third-party validations

Detection tools
- Operating system
- Device type
- GPS location (w/app)
- Universally unique identifier (UUID) (w/app)
- Phone number (w/app)

Fraud strategy
- Segmenting/profiling
- Rule creation
- Risk score evaluation
- Integrated case management

Order disposition
- Accept
- Reject

Reporting and analytics
- Mobile cancel rates
- Mobile fraud rates
- Custom reporting

Channels
- eCommerce
- Call center
- Kiosk
- POS
- Mobile

Detection tools
- Business rules
- Manual review

Fraud strategy
- Segmenting/profiling
- Rule creation
- Risk score evaluation
- Integrated case management

Order disposition
- Accept
- Reject

Reporting and analytics
- Mobile cancel rates
- Mobile fraud rates
- Custom reporting

CyberSource®
# Strategy #1 - Mobile Data

## Traditional Mobile Browser vs. “Apps”

<table>
<thead>
<tr>
<th><strong>Pros</strong></th>
<th><strong>Cons</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Browser</strong></td>
<td><strong>Variable IP geo-location (WiFi limited)</strong>&lt;br&gt;&lt;br&gt;- True device fingerprint (locked iOS)&lt;br&gt;&lt;br&gt;- Browser strings can be spoofed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Browser</strong></th>
<th><strong>Apps</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pros</strong></td>
<td><strong>Cons</strong></td>
</tr>
<tr>
<td><strong>Browser</strong></td>
<td><strong>Variable IP geo-location (WiFi limited)</strong>&lt;br&gt;&lt;br&gt;- True device fingerprint (locked iOS)&lt;br&gt;&lt;br&gt;- Browser strings can be spoofed</td>
</tr>
</tbody>
</table>
Strategy #2 - Identifying mobile device in your fraud management system

1. Select “mobile device” identifier

2. Create custom data
Strategy #3 - Tool usage

Merchants tracking mobile fraud

- Positive lists: 49%
- Device "fingerprinting": 46%
- Telephone number verification/reverse lookup: 40%
- Order velocity monitoring: 37%
- Customer order history: 37%
- Multi-merchant purchase velocity/identity morphing models: 31%
- Fraud scoring model – company specific: 29%
- IP geolocation information: 26%
- Postal address validation services: 23%
- Two factor phone authentication: 20%
- Shared negative lists – shared hotlists: 20%
- Credit history check: 20%
- Paid for public records services: 11%
- Social networking sites: 9%
- Biometric indicators: 9%

Strategy
- Multi-factor approach
- Mobile-specific
- Multi-channel

Source: CyberSource 2013 Annual Fraud Report
Strategy #4 - Mobile fraud strategy

1. Isolate mobile segment using profiles. These can be established by the device fingerprint or using merchant defined data fields.

2. Analyse, create and implement specific mobile fraud rules.

   Mobile fraud rules:
   A...
   B...
   C...

   All transactions
   mCommerce profile
   Non-mobile profiles
## Strategy #4 - Mobile fraud strategy

![Profile Selectors](image)

This section shows your profile selector rules, and the profile that will be used to evaluate the orders if the conditions are satisfied. The selector rules appear in the order that Decision Manager uses to evaluate them. If no selector rule is triggered or none is present, the default profile is used to evaluate the orders.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Rule Description</th>
<th>Order Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Mobile Orders</td>
<td>This rule will direct orders from mobile devices to our mobile...</td>
<td>Mobile Orders</td>
</tr>
<tr>
<td>2  High Risk Orders</td>
<td>This rule looks for known high risk orders, particularly those ...</td>
<td>High Risk Orders</td>
</tr>
<tr>
<td>3  My Sample Selector</td>
<td>My Sample Selector</td>
<td>Simple Rule Based Model</td>
</tr>
<tr>
<td>4  Select Decision Tree 1</td>
<td>Example of handling a profile like a decision tree</td>
<td>Simple Rule Based Model</td>
</tr>
<tr>
<td>5  Select a default profile</td>
<td>Select a default profile to evaluate orders that do not trigger an active profile selector rule.</td>
<td>Default Profile</td>
</tr>
</tbody>
</table>

### Active Selectors

### Passive Selectors

[Image of Profile Selectors]

Add Selector Rule  | Delete
Strategy #4 - Mobile fraud strategy

Rule Editor

Rule Definition
Name: Card x4 per hr > $200
Description: For mobile < 3 hrs to reject 3 time card usage to a max amt
Category: Mobile Specific

Rule Conditions
This rule is true if:
- all conditions below are true
- at least one condition below is true

Merchant-specific velocity is equal to Mobile 3x Card Per Hr

Add Condition
To add a condition, select an order element to evaluate, a comparison operator, and a comparison value. The order element selected determines the available comparison options.

Order Element:
- IMEI/CUID
- Phone Number
- Install ID
- Download ID
- Handset ID
## Summary comparison of profiles

### Profile performance comparison report

**Results:**  
Date: March 01, 2013 – March 31, 2013  
Merchant(s)

<table>
<thead>
<tr>
<th>Active profiles</th>
<th>Total transactions</th>
<th>Accepted</th>
<th>Rejected</th>
<th>Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call center</td>
<td>8,431</td>
<td>8,402</td>
<td>29</td>
<td>0</td>
</tr>
<tr>
<td>Electronic web public</td>
<td>13,459</td>
<td>13,075</td>
<td>384</td>
<td>0</td>
</tr>
<tr>
<td>Web Canada</td>
<td>19,77</td>
<td>1,509</td>
<td>468</td>
<td>0</td>
</tr>
<tr>
<td>Military</td>
<td>18</td>
<td>18</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mobile site</td>
<td>108</td>
<td>68</td>
<td>40</td>
<td>0</td>
</tr>
<tr>
<td>Web affiliate</td>
<td>13,878</td>
<td>13,824</td>
<td>54</td>
<td>0</td>
</tr>
</tbody>
</table>

All rights reserved CyberSource® 2016
### Profile performance comparison report

**Results:** Date: March 01, 2013 – March 31, 2013 | Merchant(s)

<table>
<thead>
<tr>
<th>Profiles</th>
<th>Active profiles</th>
<th>Transactions</th>
<th>Accepted</th>
<th>Force accepted</th>
<th>Rejected</th>
<th>Review</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Totals</td>
<td>39,845</td>
<td>24,532</td>
<td>14,338</td>
<td>975</td>
<td>0</td>
</tr>
<tr>
<td>Call center</td>
<td>8,431</td>
<td>4,810</td>
<td>12.07%</td>
<td>3,592</td>
<td>9.01%</td>
<td>29</td>
</tr>
<tr>
<td>Electronic web public</td>
<td>13,459</td>
<td>9,802</td>
<td>24.60%</td>
<td>3,273</td>
<td>8.21%</td>
<td>384</td>
</tr>
<tr>
<td>Web Canada</td>
<td>1,977</td>
<td>1,488</td>
<td>3.73%</td>
<td>21</td>
<td>0.05%</td>
<td>468</td>
</tr>
<tr>
<td>Military</td>
<td>18</td>
<td>15</td>
<td>0.04%</td>
<td>3</td>
<td>0.01%</td>
<td>0</td>
</tr>
<tr>
<td>▼Mobile Site</td>
<td>108</td>
<td>50</td>
<td>0.13%</td>
<td>18</td>
<td>0.05%</td>
<td>40</td>
</tr>
<tr>
<td>Rules</td>
<td>Transactions</td>
<td>Accepted</td>
<td>Force accepted</td>
<td>Rejected</td>
<td>Review</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AVS service is not available</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account issued outside of billing country</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCountry /=/ BIN Country: CA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accepted</th>
<th>Rejected</th>
<th>MAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>38,870</td>
<td>975</td>
<td>307</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accepted</th>
<th>Rejected</th>
<th>MAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>8,402</td>
<td>29</td>
<td>4</td>
</tr>
<tr>
<td>13,075</td>
<td>384</td>
<td>81</td>
</tr>
<tr>
<td>1,509</td>
<td>468</td>
<td>189</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accepted</th>
<th>Rejected</th>
<th>MAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>68</td>
<td>40</td>
<td>29</td>
</tr>
</tbody>
</table>

All rights reserved Copyright CyberSource® 2016
Mobile reporting
Ad hoc analysis
Strategy #5 – Fraud management tools

Device fingerprinting specialized for mobile

- Additional mobile data fields for rule building and reporting
- Support iOS and Android software development kits (SDKs)

**Data for authentication**
- IP address
- Browser fingerprint data
- Location ID
- Dynamic ID
- Persistent ID
- Device fingerprint
  - 1,000+ inputs

**Data for security and fraud**
- Root detection
- Crime ware detect
- Malware detect
- Location anomaly
- Device languages
Fraud management tools

Mobile risk models for greater accuracy

- Built specifically for mobile channel using historical transaction data
- Requires sufficient transaction information and "truth" data
- Will further segment into additional regions/verticals as warranted
Fraud management tools

Visual Link Analysis for Case Management

- Find common data linkages across transactions (including mobile device fingerprints)
- Drill down each linkage to transaction level detail
- Select multiple transactions with click through disposition from visual map
Summary

- Rapid mCommerce growth but also increasing mobile fraud “pressure”
- Supplement traditional fraud-prevention data points, tools, and rules for mobile
- Tune fraud strategies specifically for mCommerce
- Incorporate mobile as part of overall cross-channel monitoring
- Remain flexible and vigilant to anticipate fraud behavior
Upcoming Webinars – Training page on www.visa.com/cisp
• September 28, 2016: Effectively Managing Account Data Breaches

Visa Data Security Website – www.visa.com/cisp
• Alerts, Bulletins
• Best Practices, White Papers
• Webinar Presentations

PCI Security Standards Council Website – www.pcissc.org
• Data Security Standards – PCI DSS, PA-DSS, P2PE, and PTS
• Programs – QSA, ASV, PA-QSA, PFI, ISA, PCIP, and QIR
• Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more…
Questions?