Top 9 Fraud Attacks and Winning Mitigating Strategies

Carl Tucker
Principal, Managed Risk Services
CyberSource

Tom Donlea
Managing Director of Americas
Merchant Risk Council

CyberSource®
the power of payment
Confidentiality Notice

By accepting this presentation and the information herein, you acknowledge that the information furnished to you is confidential, (the “Information”) and that your use of the information is limited to your business dealings with CyberSource Corporation, or its affiliated company, (“CyberSource”). You agree to keep the Information confidential and not to use the Information for any purpose other than in your business dealings with CyberSource. The Information may only be disseminated within your organization on a need-to-know basis to enable your participation in business dealings with CyberSource. Please be advised that the Information may constitute material nonpublic information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc., the parent company of CyberSource, while being aware of material nonpublic information would constitute a violation of applicable U.S. federal securities laws.

Forward-Looking Statements

Today’s presentations may contain, in addition to historical information, forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended.

These forward-looking statements are based on our current assumptions, expectations and projections about future events which reflect the best judgment of management and involve a number of risks and uncertainties that could cause actual results to differ materially from those suggested by our comments today. You should review and consider the information contained in Visa, CyberSource’s parent company, filings with the SEC regarding these risks and uncertainties.

CyberSource, a subsidiary of Visa Inc., disclaims any obligation to publicly update or revise any forward-looking statements or information provided during today’s presentation.
G2W Housekeeping

- Please use Questions area of your control panel.
- Questions at the end unless additive.
- Links will be provided as follow-up.
- Any unanswered questions will be shared with presenters.
MRC Program Objectives

Networking: “Connect members to other members and industry leaders to share information and best practices.”

Benchmarking: “Provide member access to industry-specific data and information used to measure operational functionality and efficiency.”

Education: “Develop and implement programming that assists with professional development, improves organizational operations and enhances long-term strategic growth.”

Advocacy: “Lead and facilitate efforts to effect positive change in the electronic payments industry.”
EVENTS

2012 Semi-Annual Platinum Meeting

October 1 - October 3, 2012
The Fairmont Olympic
Seattle, WA

Registration is now open for the Fall Platinum Meeting in Seattle, WA.

Click here to view the latest version of the agenda.

To view details of the Merchant Focus Group on Monday October 1, click here.

Only MRC Members are invited to attend this event. If you are not a current member, you may join by filling out the membership form on our site here. In order to ensure a diverse event, companies are limited on the number of delegates they can send.

Attendance is limited by your membership level.
Merchant Members - Unlimited
Elite Members: Limit 3
Signature Members: Limit 1

If you are unsure of your membership status, please contact.
CyberSource
The Universal Payment Management Platform

$190B

Fraud Management

Managed Risk Services

Complete Lifecycle Management

Global Payment Acceptance
Payment Security
Fraud Management
Analytics and Administration

Integrations and Developer Services
Professional Services

One platform | Multiple channels | Single integration

© 2012 CyberSource Corporation. All rights reserved.
MRC Survey of Merchants

- Survey sent to MRC members between August 1-8
- 81 respondents
Top 9 Fraud Attacks

9. Triangulation Schemes
9. Triangulation: Definition

- Fraudster
- eRetailer/Marketplace
- Auction Site
- Innocent Consumer

© 2012 CyberSource Corporation. All rights reserved.
9. Triangulation: Strategy

**Consumer Electronics**

**Situation**
- Customer complaints increasing

**Analysis**
- Customer complaints linked to chargebacks
- Same IP

**Solution**
- Velocity of IP and email accounts
- Product velocity

**Purchase History/ Velocity**
- One user making multiple purchases with multiple shipping locations
- One user purchasing the same or similar products multiple times

**Customer Activity**
- Age of the customer account
- Number of purchases compared to the age of customer account
- Ignoring product discounts or promotions

**Session Profile**
- Length of buying process
Top 9 Fraud Attacks

9. Triangulation Schemes

8. Phishing/Pharming/Whaling
8. Phishing/Pharming/Whaling: Definition

This message was sent with High importance.
From: Chase Online [sxydwq@emailonline.chase.com]
To:
Cc:
Subject: Account Suspended

******************************************************************************
THIS IS AN AUTOMATED EMAIL - PLEASE DO NOT REPLY.
******************************************************************************

We received a request from 75.15.165.131 to reset your password for your Bank Account at Chase. Your account has been suspended after too many failed login attempts have been made.

You may click on the link below to reactivate your account:


We appreciate your business and look forward to serving you again in the future.

Best regards,
2012 JPMorgan Chase & Co.
28255-0001

512 Encrypted String:
FZKJFBYLRPLHLSMPU0FJKBWTDPHZHRMBTREVD
8. Phishing/Pharming/Whaling: Definition

Targeted Brands Phished 1Q 2012

*Phishing Activity Trends Report 1Q 2012; antiphishing.org*
Top 9 Fraud Attacks

9. Triangulation Schemes

8. Phishing/Pharming/Whaling

7. Botnets
7. BotNet: Definition

Over 3 Million Zombie Botnets in 2011.
Symantec Internet Security Threat Report 2011

Mary Los Angeles
Bill Detroit
Merchant
George Miami
Fraudster Nigeria
7. Botnet: Strategy

Ticketing Company

Situation
• Organized crime attack

Analysis
• Identified true IP = Vietnam, associated with multiple purchases

Solution
• Device IP = Vietnam
• Same Device IP with multiple credit cards

Device Fingerprint
• Device associated with a Botnet
• Time zone difference from the IP to the Device
• Browser language consistency with device location
• Multiple tracking elements linked to same device?

Proxy Piercing
• Does FP = VPN
• Proxy identification: anonymous, hidden, transparent
Top 9 Fraud Attacks

9. Triangulation Schemes
8. Phishing/Pharming/Whaling
7. Botnets

6. Re-Shipping
6. Re-shipping: Definition

- Fraudster
- “Mules”
- eRetailer/Marketplace
Top 9 Fraud Attacks

9. Triangulation Schemes
8. Phishing/Pharming/Whaling
7. Botnets
6. Re-Shipping
5. Affiliate Fraud
5. Affiliate Fraud: Definition

1. Affiliate and merchant have relationship
2. Affiliate and merchant have NO relationship
Top 9 Fraud Attacks

9. Triangulation Schemes
8. Phishing/Pharming/Whaling
7. Botnets
6. Re-Shipping
5. Affiliate Fraud
4. Identity Theft
4. Identity Theft: Definition

232,000,000*

*Symantec Internet Security Threat Report 2011
## 4. Identity Theft: Definition

### Identity fraud

<table>
<thead>
<tr>
<th></th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incidence Rate</strong></td>
<td>6.0%</td>
<td>4.35%</td>
<td>4.9%</td>
</tr>
<tr>
<td><strong>Total Annual Cost $B</strong></td>
<td>$31</td>
<td>$20</td>
<td>$18</td>
</tr>
<tr>
<td><strong>Mean Fraud Amount</strong></td>
<td>$2,219</td>
<td>$1,911</td>
<td>$1,513</td>
</tr>
<tr>
<td><strong>Mean Misuse Time (days)</strong></td>
<td>85</td>
<td>78</td>
<td>55</td>
</tr>
</tbody>
</table>

*2012 Identity Fraud Report: Javelin Strategy & Research*
Top 9 Fraud Attacks

9. Triangulation Schemes
8. Phishing/Pharming/Whaling
7. Botnets
6. Re-Shipping
5. Affiliate Fraud
4. Identity Theft
3. Friendly Fraud
3. Friendly Fraud

Definition
• Individual behavior, not systematic but can be expensive
• Buyers remorse—can’t detect

Strategy
• Business processes
• Review process
Top 9 Fraud Attacks

9. Triangulation Schemes
8. Phishing/Pharming/Whaling
7. Botnets
6. Re-Shipping
5. Affiliate Fraud
4. Identity Theft
3. Friendly Fraud
2. Account Takeover
2. Account Takeover: Definition

Change Account Settings

Name: 
E-mail: 
Password: ************
Mobile Phone number: 
Edit  Edit  Edit  Add

Add an address

Full Name:
Address Line 1: Street address, P.O. box, company name, c/o
Address Line 2: Apartment, suite, unit, building, floor, etc.
City:
State/Province/Region:
Zip:
Country:
Phone Number:
Optional Delivery Preferences (What’s this?)
Address Type:
Security Access Code:

Save & Payment Method  Save & Continue

© 2012 CyberSource Corporation. All rights reserved.
2. Account Takeover: Strategy

Account Takeover Methods 2011

- Change the physical address
- Add their name as a registered user on the account
- Change the email address on an account
- Obtain a debit or credit card with their name
- Change the phone number
- Change the password to an online account
- Change the PIN on a card
- Obtain checks

% of Fraud Victims

*2012 Identity Fraud Report: Javelin Strategy & Research
2. Account Takeover: Strategy

General Goods

Situation
- Abuse by established customers

Analysis
- Different emails
- Descriptive emails
- Same ID
- Same password

Solution
- Same ID associated different email accounts
- Multiple users same password

Account Activity
- Age of account
- Purchase history
- Additional verification for any account information changes

Identity Authentication
- Require 2-factor authentication for new (customer) login devices
- If login device is from suspicious location
- Velocity of the user activity
- Check if device fingerprint associated with fraudulent activities
- Check if password is the same for multiple accounts
Top 9 Fraud Attacks

9. Triangulation Schemes
8. Phishing/Pharming/Whaling
7. Botnets
6. Re-Shipping
5. Affiliate Fraud
4. Identity Theft
3. Friendly Fraud
2. Account Takeover
1. Clean Fraud
1. Clean Fraud: Definition

Order appears good…

Standard Processing Services Checks…

Account Information Matches

Checking Merchant’s Own Order History Database…

No Negative Order History? (Name)...

Checking Outside Services…

IP Geolocation…

IP Address Matches Location

No Negative Order History? (Card Number)...

Card Verification Number Matches
1. Clean Fraud: Strategy

High End Luxury Goods

Situation
• Auto-accepts becoming fraud chargebacks

Analysis
• Different accounts = same ID
• Linked during order review
• Abnormal customer behavior

Solution
• Proactive order review
• Established customer process

1. Use device fingerprint to connect yourself to the fraudster
2. Separate the new customers from loyal ones
3. Lock down purchase delivery
4. Real time order review feedback
5. Analyze your system data to understand fraudster behavior
1. Clean Fraud: Strategy

Analyze Results

Expected Results

Good

Valid orders

Bad

Chargebacks

Good

Customer insults

Bad

Captured fraud

Actual Results
Questions?

Carl Tucker
Principal, Managed Risk Services
CyberSource
c Tucker@cybersource.com
Sales: 1-888-330-2300

Tom Donlea
Managing Director of Americas
Merchant Risk Council
tom@merchantriskcouncil.org