Case Study
Responding to a Sophisticated e-Commerce Fraud Attack

Mitch Muroff
Curaxian Inc.

Denise Aptekar
oDesk
Agenda

- Introductions
- The Case (Merchant, Best Practices)
- Typical Screening Methodology
- Circumvention Methods
- The Attack
- Our Approach & Results
- Cleaner Fraud: Implications & Solutions
Curaxian

- Consulting + Analytics: We help merchants find solutions to difficult fraud problems.
- Curaxian Analytics: SaaS based reporting, monitoring, and analytics.
- Plus:
  - Reduce authorization declines to increase order conversion and billing revenue
  - Reduce interchange downgrade costs.
oDesk

- Online marketplace for remote work projects
- 4M freelancers and 400K employers
- Work project is digital good
- Most transactions are international
- Guarantee funds to the freelancer
- Clients pay after receiving deliverable
The Case

- Fortune 500 global merchant.
- Selling tickets through online web site.
- Following all standard best practices.
- Discovered excessive chargeback levels.
- Could not find solutions in data.
- Requested audit and deep data analysis.
Typical Screening Methodology

› Identify high velocity correlated with risk (approval/decline, count/amount, by device, card, IP, email, etc.).

› Identify high risk geographic locations or inconsistencies.
  › Location of: IP address, card issuer, billing address, phone, etc.

› Validate data provided.
  › Address, CVN, name, phone, email.

› Most merchants have similar rules; criminals develop methods that can circumvent controls across many merchants.
Methods: Valid Card Data

- Merchants check billing address and CVN but fraudsters buy stolen cards on the black market with names, billing addresses & CVN

### For United States Of America Banks

<table>
<thead>
<tr>
<th>Bank Names</th>
<th>Balance</th>
<th>Price</th>
<th>Preview Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank Of America</td>
<td>Between 2k - 50k</td>
<td>400$</td>
<td>Download</td>
</tr>
<tr>
<td>Wells Fargo</td>
<td>Between 4k - 40k</td>
<td>300$</td>
<td>Download</td>
</tr>
<tr>
<td>Chase Bank</td>
<td>Between 2k - 30k</td>
<td>250$</td>
<td>Download</td>
</tr>
<tr>
<td>Citibank</td>
<td>Between 9k - 70k</td>
<td>300$</td>
<td>Download</td>
</tr>
<tr>
<td>Wachovia</td>
<td>Between 2k - 18k</td>
<td>275$</td>
<td>Download</td>
</tr>
</tbody>
</table>
Methods: Valid IP Address

- Merchants check type of IP address and look for IP addresses in high risk locations or far from cardholder location but fraudsters hide their real IP location.
Methods: Valid Email Address

- Merchants may limit accounts to 1 email and check for email from high risk areas but fraudsters have access to unlimited email accounts.
Methods: Valid Phone Number

- Merchants may verify that phone is located near cardholder but fraudsters can gain access to #s in any location
Methods: Designing The Attack

‣ Conduct R&D on a target site
‣ Gain access to source of funds, identities and exit methods
‣ Test accounts first before conducting real fraud
‣ Fast exits
‣ Social engineering
The Attack

- Every order had matching AVS and CVN.
- Names and addresses appeared to be valid.
- Every order had a phone number that appeared valid.
- Nearly all fraudulent orders had free email accounts, but most good orders did as well.
- There was no velocity against card, email, or IP.
- Chargeback rates were unacceptably high.
- No obvious rules could be developed to separate good from bad orders.
Our Approach

‣ 400 variables.

‣ Which combinations of variables are best?

‣ Reduced to 25 variables.

‣ 16,000 potential solutions.

‣ Almost 600% difference from worst to best.
Minimal Data @ Rules = Inefficiency

Most data is cobbled together by manual labor, if available at all: Higher false positive rates and labor costs.
More Data @ Rules = Efficiency

When more data is available to rules, they can catch more fraud at a lower cost (false positives & manual review).
62% Fraud Reduction: 1 variable.

<table>
<thead>
<tr>
<th>Cost</th>
<th>Fraud Reduction</th>
<th>Dimension 1</th>
<th>Dimension 2</th>
<th>Dimension 3</th>
<th>Dimension 4</th>
<th>Dimension 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.49</td>
<td>$1,320,367</td>
<td>IP Region Risk</td>
<td>Product/Service Bucket</td>
<td>Item Count Risk Bucket</td>
<td>Email Domain Risk Group</td>
<td>Card Brand</td>
</tr>
<tr>
<td>0.49</td>
<td>$1,213,603</td>
<td>IP Region Risk</td>
<td>Product/Service Bucket</td>
<td>Item Count Risk Bucket</td>
<td>Email Domain Risk Group</td>
<td>Order Date/Time Bucket</td>
</tr>
<tr>
<td>0.47</td>
<td>$1,182,253</td>
<td>IP Region Risk</td>
<td>Product/Service Bucket</td>
<td>Email Domain Risk Group</td>
<td>Order Date/Time Bucket</td>
<td>Card Brand</td>
</tr>
<tr>
<td>0.49</td>
<td>$1,166,897</td>
<td>IP Region Risk</td>
<td>Product/Service Bucket</td>
<td>Item Count Risk Bucket</td>
<td>Email Domain Risk Group</td>
<td>IP Proxy</td>
</tr>
<tr>
<td>0.49</td>
<td>$1,133,723</td>
<td>IP Region Risk</td>
<td>Product/Service Bucket</td>
<td>Item Count Risk Bucket</td>
<td>IP Type</td>
<td>Order Date/Time Bucket</td>
</tr>
<tr>
<td>0.48</td>
<td>$1,115,112</td>
<td>IP Region Risk</td>
<td>Geo-Location Consistency</td>
<td>Product/Service Bucket</td>
<td>Email Domain Risk Group</td>
<td>Card Brand</td>
</tr>
<tr>
<td>0.49</td>
<td>$1,108,703</td>
<td>IP Region Risk</td>
<td>Geo-Location Consistency</td>
<td>Product/Service Bucket</td>
<td>IP Type</td>
<td>Card Brand</td>
</tr>
<tr>
<td>0.49</td>
<td>$1,107,995</td>
<td>IP Region Risk</td>
<td>Product/Service Bucket</td>
<td>Email Domain Risk Group</td>
<td>Geo-Location Distance</td>
<td>Card Brand</td>
</tr>
<tr>
<td>0.49</td>
<td>$1,094,669</td>
<td>IP Region Risk</td>
<td>Product/Service Bucket</td>
<td>Geo-Location Consistency</td>
<td>Email Domain Risk Group</td>
<td>Card Brand</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cost</th>
<th>Fraud Reduction</th>
<th>Dimension 1</th>
<th>Dimension 2</th>
<th>Dimension 3</th>
<th>Dimension 4</th>
<th>Dimension 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.49</td>
<td>$2,140,908</td>
<td>Usage Data Bucket</td>
<td>IP Region Risk</td>
<td>IP Type</td>
<td>Card Brand</td>
<td>Product/Service Bucket</td>
</tr>
<tr>
<td>0.49</td>
<td>$2,090,128</td>
<td>Usage Data Bucket</td>
<td>IP Region Risk</td>
<td>Geo-Location Consistency</td>
<td>IP Type</td>
<td>Product/Service Bucket</td>
</tr>
<tr>
<td>0.49</td>
<td>$2,082,988</td>
<td>Usage Data Bucket</td>
<td>IP Region Risk</td>
<td>Item Count Risk Bucket</td>
<td>Email Domain Risk Group</td>
<td>Product/Service Bucket</td>
</tr>
<tr>
<td>0.49</td>
<td>$2,064,067</td>
<td>Usage Data Bucket</td>
<td>IP Region Risk</td>
<td>Item Count Risk Bucket</td>
<td>Email Domain Risk Group</td>
<td>Product/Service Bucket</td>
</tr>
<tr>
<td>0.49</td>
<td>$2,045,665</td>
<td>Usage Data Bucket</td>
<td>IP Region Risk</td>
<td>IP Proxy</td>
<td>Card Brand</td>
<td>Product/Service Bucket</td>
</tr>
<tr>
<td>0.49</td>
<td>$2,034,348</td>
<td>Usage Data Bucket</td>
<td>IP Region Risk</td>
<td>Email Domain Risk Group</td>
<td>IP Type</td>
<td>Product/Service Bucket</td>
</tr>
<tr>
<td>0.49</td>
<td>$2,033,195</td>
<td>Usage Data Bucket</td>
<td>IP Region Risk</td>
<td>Geo-Location Consistency</td>
<td>IP Type</td>
<td>Product/Service Bucket</td>
</tr>
<tr>
<td>0.49</td>
<td>$2,025,677</td>
<td>Usage Data Bucket</td>
<td>IP Region Risk</td>
<td>Phone Velocity</td>
<td>Email Domain Risk Group</td>
<td>Product/Service Bucket</td>
</tr>
<tr>
<td>0.48</td>
<td>$2,022,095</td>
<td>Usage Data Bucket</td>
<td>IP Region Risk</td>
<td>Item Count Risk Bucket</td>
<td>Card Brand</td>
<td>Product/Service Bucket</td>
</tr>
</tbody>
</table>

Association for Financial Professionals
Solution: Data Mastery

Key is to measure the right things and find the combinations that yield optimal results.

<table>
<thead>
<tr>
<th>Usage Data Bucket</th>
<th>IP Region Risk</th>
<th>Phone Velocity</th>
<th>Email Domain RG</th>
<th>Product Bucket</th>
</tr>
</thead>
<tbody>
<tr>
<td>15%</td>
<td>20%</td>
<td>7%</td>
<td>20%</td>
<td>17%</td>
</tr>
<tr>
<td>0.10%</td>
<td>0.13%</td>
<td>0.17%</td>
<td>0.53%</td>
<td>0.30%</td>
</tr>
<tr>
<td>0.26%</td>
<td>0.77%</td>
<td>1.50%</td>
<td>1.00%</td>
<td>0.97%</td>
</tr>
<tr>
<td>0.51%</td>
<td>0.47%</td>
<td>0.71%</td>
<td>0.96%</td>
<td>0.44%</td>
</tr>
<tr>
<td>1.09%</td>
<td>5.69%</td>
<td>2.93%</td>
<td>0.97%</td>
<td>3.49%</td>
</tr>
<tr>
<td>2.16%</td>
<td>2.89%</td>
<td>5.23%</td>
<td>3.29%</td>
<td>3.88%</td>
</tr>
<tr>
<td>2.62%</td>
<td>3.78%</td>
<td>4.38%</td>
<td>3.37%</td>
<td>4.22%</td>
</tr>
<tr>
<td>2.96%</td>
<td>5.34%</td>
<td>5.25%</td>
<td>2.67%</td>
<td>6.62%</td>
</tr>
<tr>
<td>6.49%</td>
<td>5.92%</td>
<td>4.33%</td>
<td>4.65%</td>
<td>10.68%</td>
</tr>
<tr>
<td>7.56%</td>
<td>10.70%</td>
<td>6.37%</td>
<td>3.79%</td>
<td>5.16%</td>
</tr>
<tr>
<td>8.52%</td>
<td>5.87%</td>
<td>7.93%</td>
<td>5.66%</td>
<td>4.19%</td>
</tr>
<tr>
<td>12.36%</td>
<td>22.71%</td>
<td>30.61%</td>
<td>20.86%</td>
<td>21.22%</td>
</tr>
<tr>
<td>12.58%</td>
<td>8.86%</td>
<td>10.89%</td>
<td>6.03%</td>
<td>6.09%</td>
</tr>
</tbody>
</table>

400 variables = trillions of combinations. Which lead to most powerful rules?

AFP® Annual Conference
Cleaner Fraud: Implications

- Criminals are constantly developing new attack vectors.
- Criminals seek to maximize ROI on those investments by applying new attack vectors within an industry and then across industries.
- Criminals are always seeking merchants with weakest defenses. Don’t be that merchant.
- Known “best practices” are becoming obsolete.
- An accelerating arms race.
Cleaner Fraud: Solutions

- Don’t trust that existing systems and processes will work in the future, just because they worked in the past.
- Develop early warning indicators and monitor them daily to detect new attacks that might be circumventing current controls.
  - Chargeback volumes and characteristics.
  - New-account signup velocity, characteristics, clusters.
  - Authorization declines, especially fraud related.
Cleaner Fraud: Solutions

‣ Strategies that are harder for criminals to circumvent.
‣ Use deeper data to inform risk decisions.
  ‣ Behavior before/after purchase transaction.
  ‣ Account source data.
‣ Join customer-provided data with third party data.
  ‣ IP, Machine, Phone, Name/Address, Social Network.
‣ Use analytics to refine fraud rules.
  ‣ Complex rules that are harder to evade.
  ‣ Fine tune manual review vs false positives vs fraud.
Contact

Curaxian

Mitch Muroff
CEO
Curaxian Inc.
mitch@curaxian.com

Denise Aptekar
Director, Trust & Safety
oDesk
daptekar@odesk.com

AFP® Annual Conference