9K: How Technology Can Address Current and Emerging Fraud Risks

Session Level: Intermediate

Tuesday, June 14 - 1:40-3:00 p.m.

This session will explore how organizations are addressing the operational and reputational risks associated with ACH (peer-to-peer) and Wire fraud, the priority being given to this type of fraud prevention over the next 1-3 years, and how information security operations should integrate with your fraud operations. Plus, expectations from your enterprise fraud vendor and how the rollout of mobile banking can and should impact your enterprise fraud strategy will also be discussed.
How Technology Can Address Current and Emerging Fraud Risks

Revathi Subramanian, Director, Research & Development
Manuel Da Silva, Fraud Management Consultant
Cameron Jones, Director, Financial Crimes Product Management
Challenges

• Customers want Convenience
• Devices Increase Payment Channel Choices
• Organizations View Technology in a Siloed Perspective
• Focus is on Traditional Fraud Attacks
Demographic traits:
- 97% of students own a computer
- 94% own a cell phone
- 76% of students use instant messaging (SMS) (~90% Europe/Asia)
- 92% multitask while IM’ing
- Spend at least 3.5 hours a day online

2007 Junco/Mastrodicasa study of high school students
Generation ‘Y’ Banking Insights

- **Online/Mobile Use**
  - 48% signed up for credit cards online
  - 36% applied for personal loans online
  - 80% use internet banking monthly

- **Cards/Accounts**
  - 36% have a debit card, savings or checking account
  - Daily payment method for expenses is debit card

- **Mobile Devices**
  - 32% check account balances
  - 15% receive and pay bills
Combating Financial Crimes

Trend is moving integration of data and analytics upstream in the fraud management process.

Proactive Prevention through Predictive Analytics
Multiple Analytical Approaches

Using a Hybrid Approach for Fraud Detection

<table>
<thead>
<tr>
<th>Enterprise Data</th>
<th>Suitable for known patterns</th>
<th>Suitable for unknown patterns</th>
<th>Suitable for complex patterns</th>
<th>Suitable for associative link patterns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customers</td>
<td>Rules</td>
<td>Anomaly Detection</td>
<td>Predictive Models</td>
<td>Social Network Analysis</td>
</tr>
<tr>
<td>Transactions</td>
<td>Rules to filter fraudulent transactions and behaviors</td>
<td>Detect individual and aggregated abnormal patterns</td>
<td>Predictive assessment against known fraud cases</td>
<td>Knowledge discovery through associative link analysis</td>
</tr>
<tr>
<td>Applications</td>
<td>Examples:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3rd Party Flags</td>
<td>Txns in different time zones within short period of time</td>
<td>Wire transactions on account exceed norm</td>
<td>Like wire transaction patterns</td>
<td>Association to known fraud</td>
</tr>
<tr>
<td>Call Center Logs</td>
<td>1st Txn outside US</td>
<td># unsecured loans on network exceed norm</td>
<td>Like account opening &amp; closure patterns</td>
<td>Identity manipulation</td>
</tr>
<tr>
<td></td>
<td>Cash cycling event</td>
<td>Accounts per address exceed norm</td>
<td>Like network growth rate (velocity)</td>
<td>Transactions to suspicious counterparties</td>
</tr>
</tbody>
</table>

Hybrid Approach

Proactively applies combination of all 4 approaches at account, customer, and network levels.
Potential for Accuracy Improvement

Results from POCs, POVs, and Projects

- Retail Bank Personal Accounts: 35% Scenario, 70% Scenario + Model
- Brokerage High Net Worth Accounts: 6.5% Scenario, 43% Scenario + Model
- E-Banking (Phishing): 1.3% Scenario, 25% Scenario + Model
- Watch List Compliance: 0.2% Scenario, 49% Scenario + Model
Neural Network Analytics
The Challenge – Enterprise Fraud

- Fraud got more sophisticated
  - Across multiple lines
  - Through different channels
- New Technologies
  - More channels are available to conduct variety of monetary or non-monetary activities
  - Constantly changing environment
- Demand in customer relationship management
  - Monitor the customer in silo fashion is insufficient
  - Need better understanding of the customer across the enterprise
ACH / Wire Transfer Fraud Analytics

- Most existing systems use rules
- Rule based systems have very high false positive rates - not feasible for taking action
- Commercial ACH and Wire fraud very rare
  - Very few cases to learn from
  - Fraud rates much lower than payment card fraud
- May not have many historical bad cases to train supervised models
  - Lacks patent pending semi-supervised or unsupervised modeling techniques that will be utilized for this problem
Typical Problem Characteristics

- Extremely large volumes of disparate data (numbers / text)
- Identify very rare events (needles in a haystack)
- Rare events constitute monetary / psychological high value
  (Credit card fraud, Tax under-filing, intrusion of highly secure networks)
- Solutions involve sophisticated analytical models, high performing software all rolled into one
Broad Classes of Problems

- **Supervised Learning:**
  - Target fully known
  - Learn from the examples and extrapolate
  - Credit card fraud, bankruptcy

- **Semi-Supervised Learning:**
  - Partial target known
  - Learn from the known targets as well as anomalous behavior to predict risk
  - Tax fraud, purchase card fraud good examples

- **Unsupervised Learning:**
  - Target unknown
  - Learn from anomalous behavior and isolate cases
  - Insurance fraud, network intrusion good examples
ACH/Wire
Strategic & Operational Risk
Why Fraudsters ‘love’ ACH/Wire

- Multiple ‘channels and products’ of intrusion.
  - Online, Phone, Direct deposits, Payroll, Procurement,
  - Automated Checks, Bill Payments, Social Security payments

- Common ACH/Wire fraud traits:
  - Employee collusion / Internal Fraud
  - Interception; (Seasonal targets emails i.e. ‘IRS-Unreported Income’) installs malicious Trojan software (‘Zeus/Zbot’ and ‘Backdoor.bot’)
  - Malware (Generic): MiTM / MiTB
  - Single Authentication Process
  - ‘Mules’/’Stay-at-home’ schemes to process funds - Structured and complex fraud group attacks

- Commercial v’s Consumer recovery periods:
  - Commercial targeting – High velocity (#) and high value($) of ACH/Wire hides small but significant incremental changes (low velocity/large $ value)
ACH / Wire Transfer Fraud Analytics (r)

- Most existing systems use rules. Subjective focus
- Rule based systems have very high false positive rates - not feasible for taking action
- Commercial ACH and Wire fraud very rare
  - Very few cases to learn from
  - Fraud rates much lower than payment card fraud
- May not have many historical bad cases to train supervised models
  - Lacks patent pending semi-supervised or unsupervised modeling techniques that will be utilized for this problem
How Pervasive is ACH/Wire Fraud

  - Most Cases; Accounts held at regional/local, credit unions.

- Apr-2011 – FBI Statement:
  - Mar-2010/Apr-2011, identified incidents where online banking credentials of small/medium U.S. businesses were compromised and used to initiate wire transfers to Chinese economic/trade companies. Total attempted fraud amounts to ~ $20 million.
  - Wire funds of $50K in large-part successful; funds withdrawn immediately.

- Zeus/Zbot:
  - Available to buy on internet (~$700-4000)
  - Proliferation: Machines in 196 countries/most significant
    - USA, Mexico, Saudi Arabia, Egypt and Turkey.
  - Altogether, 2,411 companies and organizations are said to have been affected. US ~3.6 million consumer PCs
  - Difficult to detect; Largest botnet on internet
### Strategic Responses to Reduce Fraud Risks

<table>
<thead>
<tr>
<th>Manage risk holistically, including fraud risk.</th>
<th>Manage fraud, security, compliance in coordinated fashion.</th>
<th>Improve data governance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leverage fraud information for new business opportunities.</td>
<td>Merge AML and fraud strategy, technology, processes.</td>
<td>Standardize security and business process with supply chain.</td>
</tr>
<tr>
<td>Adopt enterprise fraud management with LOB responsibility.</td>
<td>Manage valuation, liquidity, counterparty risk with eye to fraud.</td>
<td>Use risk-based, not standardized, approach to fraud.</td>
</tr>
<tr>
<td>Upgrade technology to comply with new regulations.</td>
<td>Source: TowerGroup</td>
<td></td>
</tr>
</tbody>
</table>
A Layered Security Framework

1. Proactive Monitoring

- Real-Time / Online Processing of ACH, ACH/Batch and Wire Transactions
- Manage within processing Time Windows
- Monitor both Debits and Credits into Account
- Monitor (‘household’, non-monetary type transactions)
- Allow for Real-Time Blocking/Hold Strategies – Managed by the Business Team
A Layered Security Framework

2. Authentication

- Utilize ‘2-Factor Type Authentication’ for log-in/access process – Different processes
- Malware Detection programs
- IP intelligence
- HTTP header / Secure browser
- Wireless / Virtual Tokens, etc.
A Layered Security Framework

3. Analytics / Behavioral Profiling

- Deploy Proven Model Methodologies to capture fraud more effectively – reduce false positive/increase detection rates

- Utilize Signatures as part of Entity Behavior – Single & Complex Structures (Account, Customer, Bank_id, Devise_id, Payee/Benefactor – Data driven

- Use Scores, Reason & Operational Codes to predict suspicious/fraud activity (make avail in Rules Logic)

- Maximize data values (incl. House-hold and Demographic data)

- Explore Link Analysis – Find ‘common’ patterns of fraud traits
A Layered Security Framework

4. Transaction Monitoring / Batch Fraud Monitoring

✓ Set Strategies based on Risk and Tolerance

✓ Prioritize based on ‘Hold’ and Time Sensitive Transactions

✓ Authenticate Suspicious Actions

✓ Manage Strategy and Champion/Challenge Environment

✓ Provide Holistic view of customer/account

✓ Empower analyst to action and reconcile investigations
A Layered Security Framework

3. Analytics / Behavioral Profiling

✓ Deploy Proven Model Methodologies to capture fraud more effectively – reduce false positive/increase detection rates

✓ Build Signatures as part of Entity Behavior – Single & Complex Structures (Account, Customer, Bank Details, Devise_Id, Payee/Benefactor)

✓ Use Scores, Reason & Operational Codes to predict suspicious/fraud activity (make avail in Rules Logic)

✓ Maximize data values (incl. House-hold and Demographic data)
A Layered Security Framework

5. Customer Education / Involvement

- Authenticate Suspicious Transactions
- Customer Education
- Preset Limits
- Interactive Alerts
- Increase Outbound Contact Medium (SMS, Email, Secure Message)
Conclusions

- Challenge ACH/Wire ‘Status Quo’ Fraud Detection
- Manage risk holistically
- Adopt proven Analytical methodologies to increase fraud rate detection
- Use a risk-based rather than standardized approach to fraud
- Upgrade technology to comply with new fraud requirements
- No Quick Wins - Layered Security
- Adopt enterprise fraud management with line-of-business responsibility