Optimising Your Transaction Monitoring System

Jeroen Dekker
Senior Product Manager
Risk & Compliance

European Client Conference
What we’ll share today is based on:

- More than 10 years experience
- With over 900 implementations
- In over 70 countries
- With small and large institutions
- With different business lines (retail, private, business, insurance, investments, prepaid)

Payments Processing Services
Customer & Channel Management
Insights & Optimization
Risk & Compliance

Financial Risk Management
Financial Performance Management
Financial Control Solutions
Financial Crime Risk Management

Fraud AML
(Terrorist Financing, Sanctions, Corruption, Market Conduct)

Transaction Monitoring
(Detection, Investigation, Reporting)
Agenda

- Role of transaction monitoring
- Project recommendations
- Compliance approaches

- **Case Study:** Turning too many alerts into a strategy

- Scenario tuning concepts and tips
- Wrap-up
Role of Transaction Monitoring

- Catch the bad guys

- Watch the good guys

- Do what makes sense (Get it right or else)

Member States shall require that the institutions and persons covered by this Directive pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

(d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transac-

measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. The institutions and persons covered by this Directive shall be able to demonstrate to the competent authorities mentioned in Article 37, including self-regulatory bodies, that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.
When (not) to Generate Alerts

Monitor every customer and all behavior

High-risk behavior

Accounts or Transactions for Sanctioned entities

High-risk customer

Low-risk behavior

Simplified Due Diligence for “No-risk” customer or behavior?

Low-risk customer should do something very strange to be alerted

High-risk customer should be alerted if behavior is only slightly off

© 2012 Fiserv, Inc. or its affiliates.
Project Recommendations

- Take time for data quality
- Test before you go live
- Start with small set of scenarios
- Grow and refine over time
- Invest in periodical tuning
Compliance Approaches

- Load data on Day 1+X
- Embrace Alerts from other sources
- Document your evolving thinking
- The Risk-Based Approach is everywhere!
- Investigate Customers, not Alerts
Case Study:
Turning too many alerts into a strategy

- European regional bank
- Group scenarios and local scenarios
- Resource constraints on data, tuning, investigation
- Problem: too many alerts to handle
Case Study:
Turning too many alerts into a strategy

• Always investigate High-Risk Scenarios and Alerts (and do so first)
• Assemble Medium-/Low-Risk Alerts per Customer
• Rank by Alert count, work your way down
• Outcome: efficient, effective and a defensible risk-based approach
## Scenario Tuning – Where to Improve

### Table: Scenario Alerts and Hit Rates

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Alerts</th>
<th>A / C rate</th>
<th>Cases</th>
<th>C / R rate</th>
<th>Reports</th>
<th>A / R rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Cash by Retail Customers</td>
<td>50</td>
<td>10%</td>
<td>5</td>
<td>80%</td>
<td>4</td>
<td>8%</td>
</tr>
<tr>
<td>Unusual Cash by Business Customers</td>
<td>16</td>
<td>75%</td>
<td>12</td>
<td>33%</td>
<td>4</td>
<td>25%</td>
</tr>
<tr>
<td>Cash Peer Group Deviation</td>
<td>100</td>
<td>40%</td>
<td>40</td>
<td>50%</td>
<td>20</td>
<td>20%</td>
</tr>
</tbody>
</table>

- **First review workload**
- **Heavy investigation workload**
- **What you’ve found**

© 2012 Fiserv, Inc. or its affiliates.

European Client Conference
Scenario Tuning – How to Improve

- What do the false positive Alerts have in common?
- What do the false positive Cases have in common?
- What do the Reports (confirmed suspicions) have in common?

First candidates:
Transaction Types, Account Types, Industry Codes, Countries, Age of the Account or Relationship
Finding the Right Balance

Finding the right balance (scenario coverage and thresholds)

False Negatives

Very efficient

0

Very effective

False Positives
Finding the Right Balance

Improving the equation(s) by refining scenarios

© 2012 Fiserv, Inc. or its affiliates.
Basic Scenario Tuning Strategies

- Increase thresholds / adding filters for badly performing scenarios
  - Can I get rid of many alerts with an acceptable loss in hits? (and can I then define a second scenario to effectively catch the lost hits?)

- Lower thresholds / removing filters for well-performing scenarios
  - Can I catch a lot more with an acceptable increase in false positives? (and can I then add new filters to minimize those false positives?)

- Add new scenarios for new or more granular risks
- Turn off scenarios that don’t produce or are no longer valid
Detection Strategy – Attack from All Sides!

- How the customer behaved in the past
- How customers like him behave
- How the customer said he would behave
- Known laundering patterns
Historic / Actual Behavior

- Limit alerts for single large transactions
- Think about seasonal effects
- Use Alert history (and outcome)
How Customers Like Him Behave

Using Peer Grouping Against False Positives

• The customer’s behavior has changed – but it’s still within range of the peer group’s normal behavior
• The customer’s behavior has changed – but so has that of everyone in the peer group!
Peer Grouping – Some Lessons Learned

• Occupation (data quality)
• Industry Code (company size)
• Age and Zip Code
• Statistical validity
Expected Behavior

Especially useful for Private/Business customers

• What’s “a lot”?  
• Will you use cash?  
• Domestic or international?  
• If international, which countries?  
• Many small or few large transactions?  
• Coming in or going out?

How the customer said he would behave
Known Laundering Patterns

- Don’t blindly copy industry / regulator / vendor red flags
- Use your knowledge of your geographies, customers, industries
Avoid Repeat Alerts

- Threshold will still be broken tomorrow
- Exclude specific customers from specific scenarios
- Use Alert history (and outcome)
- Avoid repeat investigations: add new alerts to cases in progress
Use Good Old Rules to Filter

Original Scenario

Focus

Exclude

Exclude some more

Original Scenario

Only incoming transfers

No government customers

No savings accounts
Segmentation – Break Down and Refine

- Alert all wire transfers to foreign countries above $50,000
  - Alert all wire transfers to low-risk countries above $100,000
  - Alert all wire transfers to medium-risk countries above $50,000
  - Alert all wire transfers to high-risk countries above $20,000
  - By low-risk customers above $50,000
  - By medium-risk customers above $20,000
  - By high-risk customers above $10,000
Wrap-Up

• Relate concepts to details
• Be thorough
• Be realistic
• Be pragmatic
• Keep shaving, mixing, refining
Connect With Us

Jeroen Dekker
jeroen.dekker@fiserv.com

© 2012 Fiserv, Inc. or its affiliates. Fiserv is a registered trademark. Other products referenced in this material may be trademarks or registered trademarks of their respective companies.