SAR Monitoring:
Program Management, Fine Tuning, and System Maximization

John Wagner (Moderator)
Director,
BSA/AML Compliance
Office of the Comptroller of the Currency

William D. Ward, CAMS
Executive Vice President
Union Bank

S. Marshall Martin, Esq.
Enterprise Risk Executive & Co-General Counsel
City National Bank

Deborah King
Senior Vice-President
RBS Citizens Bank

Suspicious Activity Monitoring Program

Program Management & Governance

William D. Ward, CAMS
Executive Vice President
Chief BSA/ OFAC & Security Officer
Union Bank – San Francisco, CA
### Three Pillars of a Program

<table>
<thead>
<tr>
<th>Program Management</th>
<th>Technology</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>AML Software</td>
<td>Surveillance</td>
</tr>
<tr>
<td>Policy (Monitoring Strategy)</td>
<td>Case Management</td>
<td>Investigations</td>
</tr>
<tr>
<td>Accountability</td>
<td>Data management</td>
<td>SAR Filing</td>
</tr>
<tr>
<td>Risk Nexus</td>
<td>Tuning</td>
<td>Alert / Case Management</td>
</tr>
<tr>
<td>Reporting / KPI</td>
<td>Analytics</td>
<td>Law Enforcement Liaison</td>
</tr>
<tr>
<td>Program Principles</td>
<td>Test Environment</td>
<td>Escalation / Adverse Action</td>
</tr>
</tbody>
</table>

*The above descriptors are not all encompassing. Each pillar may contain other components of the BSA program.*

### Governance

**Internal & External walls to the program**

- **Board or Executive Approval (AML Risk Tolerance)**
- **BOD or Board Risk Committee**
- **BSA Officer Approval**
- **Self Testing & Quality Control**
- **MIS Reporting**
- **Key Performance Indicators** (efficacy, timeliness, quality & sustainability)
- **CALIBRATE AGAINST AML RISK TOLERANCE**
- **AML Oversight Committee**

*12th Annual FIBA AML Compliance Conference*
BSA Policy: SAR Program

- Policy / Program should address the Suspicious Activity Monitoring & Investigations Strategy
- Policy / Program should identify structure around the AML monitoring strategy (AMBR5)
- Policy / Program should identify the need to tailor monitoring commensurate with risk (Risk Assessments)
- Monitoring policy should reference AML risk tolerance

Monitoring Strategy

- Establishes monitoring standards
- Administers the business rule change management process (production, retirement, tuning, etc)
- Establishes standards on the monitoring process procedures and results
- Provides for tools to accomplish function
Accountability: Who does what?

RESPONSIBLE BSA UNIT

RESPONSIBILITIES

• Perform Risk Assessment
• Integrate risk assessment program with HR population risks identified in MLRC
• Modify as needed per input from FFIEC, Authoritative Issuances, Exam & Audit findings

BSA/AML PROGRAM OFFICE

• Identify source data
• Develop systems & tools necessary to monitor
• Implement, test and validate monitoring effectiveness

TECHNOLOGY IMPLEMENTATION

• Perform on-going monitoring against full transaction universe
• Conduct investigations of suspect activity
• File SAR as appropriate
• Provide results back to A&I

LIFECYCLE STAGE

MONITORING STRATEGY

EXECUTION

ANALYTICS & INFORMATICS

BSA/AML/OFAC OPERATIONS

12th Annual FIBA AML Compliance Conference

Risks Drivers

Lower Risk/Stronger Controls (Perhaps Over-controlled)  Higher Risk/Stronger Controls (Appropriately Controlled)

Lower Risk/Weaker Controls (Appropriately Controlled)  Higher Risk/Weaker Controls (Action Needed)

Private Banking
• Correspondent Banking
• Retail Banking
• Embassy Banking
• Mortgage Lending
• Credit Cards
• Trade Finance
• Capital Markets
**Enterprise Business Security & Intelligence**

**Financial Intelligence Unit – IU SARs**

4th Quarter 2011

**Suspicious Activity Life Cycle Report**

From Alert Inception Date to SAR Filing Date

**Total SARs Filed 4th Quarter: 1098**

<table>
<thead>
<tr>
<th>Day Age</th>
<th>1-10</th>
<th>11-20</th>
<th>21-30</th>
<th>31-40</th>
<th>41-50</th>
<th>51-60</th>
<th>61-70</th>
<th>71-80</th>
<th>81-90</th>
<th>90-99</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCT</td>
<td>55</td>
<td>101</td>
<td>53</td>
<td>38</td>
<td>29</td>
<td>20</td>
<td>14</td>
<td>12</td>
<td>11</td>
<td>3</td>
<td>233</td>
</tr>
<tr>
<td>OCT Cum</td>
<td>16,615</td>
<td>26,145</td>
<td>29,285</td>
<td>31,985</td>
<td>34,405</td>
<td>36,225</td>
<td>37,345</td>
<td>38,065</td>
<td>38,785</td>
<td>39,095</td>
<td>60,600</td>
</tr>
<tr>
<td>NOV</td>
<td>110</td>
<td>60</td>
<td>92</td>
<td>52</td>
<td>48</td>
<td>18</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td>418</td>
</tr>
<tr>
<td>NOV Cum</td>
<td>17,715</td>
<td>26,725</td>
<td>29,105</td>
<td>31,105</td>
<td>34,025</td>
<td>36,250</td>
<td>37,445</td>
<td>38,265</td>
<td>38,985</td>
<td>39,305</td>
<td>49,700</td>
</tr>
<tr>
<td>DEC</td>
<td>86</td>
<td>57</td>
<td>36</td>
<td>26</td>
<td>22</td>
<td>14</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td>378</td>
</tr>
<tr>
<td>DEC Cum</td>
<td>19,351</td>
<td>28,282</td>
<td>30,648</td>
<td>32,762</td>
<td>35,782</td>
<td>38,040</td>
<td>39,195</td>
<td>40,025</td>
<td>40,655</td>
<td>41,005</td>
<td>53,390</td>
</tr>
<tr>
<td>Q4 Cum</td>
<td>295</td>
<td>172</td>
<td>111</td>
<td>74</td>
<td>69</td>
<td>46</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td>1,098</td>
</tr>
</tbody>
</table>

**New Case – SAR & SAR 90s by Life Cycle Age**

SARs Aged From Date of Determination

**Federal Regulations requires that a SAR be filed no later than 30 calendar days from the date of the initial detection of facts that constitutes a basis for filing. If no suspect can be identified the time period is extended to 60 days.**

**Alert Sources**

- AML-R: 1,320
- eQAR: 934
- BLU Cash: 1,222
- BLU Wire/Velocity: 110
- SOMI: 344
- WIBIS: 951
- RDC: 1,020
- UCA: 0

**Surveillance Unit**

- Alerts Raised: 5,901
- Total Alerts Auto-Routed: 634
- Alerts Worked: 5,898

**Sustainability: 99.95%**

Alerts Referred: 1,846
Non-Referred: 4,052

**Investigations Unit**

- New Cases Open: 2,731
- Cases Closed: 2,795

**Final Disposition**

- SAR: 1,098
- NO SAR: 1,697

**RDC Type:**

- Delta: 495
- Portfolio: 476
- Enrichment: 49

**Manual Input**

- Delta: 205
- Portfolio: 387
- Enrichment: 415
- Delta: 14
- Portfolio: 32

**Final Disposition**

- SAR: 261
- NO SAR: 132

NOTE 1: Not all alerts referred result in a case to the IU due to consolidation.

NOTE 2: SAR total is increased by 12 due to a SAR counted in the SRC.
Program Guiding Principles

1. Define Process
2. Sound Decisions
3. Decisions Supported
4. Consistently Applied
5. Repeatable & Sustainable

Effective BSA/AML Suspicious Activity Mentoring Program

12th Annual FIBA AML Compliance Conference

Technology & SAR Monitoring
(A Community Bank Perspective)

Date: February 23, 2012

Prepared By:
S. Marshall Martin, Esq.
Enterprise Risk Executive & Co-General Counsel
Agenda

I. Technology & Suspicious Activity Monitoring, where do we begin?
II. Surveillance & Transaction Monitoring
III. Tuning / Filtering / Threshold Setting
IV. Validation
V. Closing Thoughts

1. Technology & Suspicious Activity Monitoring, where do we begin?

Identification of Unusual Activity (alerting channels, Focus will be Technology)
Alert Analysis & Investigation
SAR Decision Making
SAR Completion & Filing

Taken from FFIEC Manual, Appendix S.

12th Annual FIBA AML Compliance Conference
I. Technology & Suspicious Activity Monitoring, where do we begin? (Cont.)

II. Surveillance & Transaction Monitoring

- Do you really need a system? (Risk Assessment / Analytics)
- Selection of vendor (due diligence)
- Functionality outside of alerts (e.g., case management)
- Other considerations:
  - Risk Scoring
  - Support
  - Filling capabilities (SAR / CTR)
  - Image capture
  - Consolidated alerts vs. individual alerts
- Out of the box rules (nightmare begins)
- Gaps in vendor systems (ad hoc reports / models?)
III. Tuning / Filtering / Threshold Setting

- Tuning, optimization, …….. (often akin to a “bad word”)
- Applies equally to surveillance / transaction monitoring and reports / models
- Goal: effectiveness / efficiency of alerts
- Identify successes and failures in monitoring systems
- Leverage risk scoring and risk assessment
- Focus should be on residual risk not inherent
- Should be analytics driven & fully documented

III. Tuning / Filtering / Threshold Setting (Cont.)

Distribution Analysis - Business Deposit Customers

- Average = 150
- Std.Dev = 450
- Count = 8933
- Min = 0
- Max = 12000

12th Annual FIBA AML Compliance Conference
IV. Validation

An effective AML monitoring system(s) requires implementation of a robust validation program!!

Key Elements of Validation Program

- FFIEC BSA/AML Exam Manual expectation
- Data integrity: inputs (transaction codes) & system output (test them)
- Ongoing monitoring / assessment process (timing)
  - Are the alerts effective (great resource impact, efficiency)
  - Reasonableness of thresholds / rules (risk profile / assessment)
- Improve system accuracy & close gaps
- Document
- Audit (internal / external) should confirm

Bottom-line: A robust validation program is necessary to insure your monitoring system is effective & efficient!

VI. Closing Thoughts

- Tight environment for human resources
- Focus must be on improving efficiency / effectiveness of alerting systems
- Stop doing what is not working or is inefficient
- Senior management and board support will be critical for your efforts
- Independently test (self assess / validate / audit)
- Data analytics should dictate & drive efforts (documentation / support)
- IT (data) support will be critical to your success
SAR Monitoring: Program Management, Fine Tuning, and System Maximization

Deborah King
SVP, Head, Financial Intelligence Unit
RBS Citizens

FIU Best Practices

• Know your Audience
  – Provide actionable intelligence to law enforcement
  – Ensure that your institution meets regulatory expectations
  – Protect your institution’s assets and customers from those individuals looking to exploit its products and services
  – Demonstrate to the Board and Senior Management that your Program meets all requirements

• Know your Environment
  – Keep current on emerging trends and regulatory initiatives
  – Review media reports
  – Make it easy for business lines to refer suspicious activity to you
  – Understand and actively participate in the roll-out of new products and services
  – Understand the impact of your institution’s expanding market (new geographies, product, and customers as a result of mergers and acquisitions and expansion)
Best Practices

• Know your Investigators
  – Hire investigators with the required skill set
    • Critical thinking
    • Writing proficiency
    • Ability to see the big picture
    • Variety of backgrounds: Law Enforcement, Banking, Law
  – Centralize all AML investigations within the FIU
  – Use a Team Approach with a shared workflow.
  – Cross-train team members to perform all roles (alert, case, QC), and rotate the Investigators between the roles.
  – Provide meaningful training to keep the Investigators engaged
    • Live group meetings with law enforcement
    • Webinars/Seminars on topics of interest
    • Regular department meetings

12th Annual FIBA AML Compliance Conference

Best Practices

• Know your Systems
  – Leverage your institution’s best available client and transaction data sources
  – Constantly monitor the performance of your system
    • Analyze the conversion rates of alert to case to SAR
    • Make adjustments to rules, scenarios, and parameters as needed
  – Strive for the perfect balance between high yield detection and false positive containment

• Know your Customers
  – Analyze activity at the customer level, rather than the individual account level
  – Utilize Peer Group analysis
  – Ensure that business lines understand the importance of obtaining accurate customer information
  – Review subpoenas received by your institution

12th Annual FIBA AML Compliance Conference
Best Practices

- Know your Data
  - Identify and correct any data challenges that affect the integrity of transactions, such as the ability to identify only “true” cash
  - Obtain data sufficient to stratify your customer base by type, so that you can create and leverage accurate expected activity profiles
  - Perform analysis on your repository of alerts (open and closed)
  - Obtain and analyze data from other areas of the Bank (CTRs, Wires, ACH)
  - Be tuned in to new data sources as they become available