Addressing Financial Crime Compliance Challenges: Shared Utilities

ACAMS, Chicago

Sept 2018
Trends, Insights and Solutions

Chetan Cariappa
Senior Manager, Financial Crime Compliance
SWIFT

The global provider of secure financial messaging services
SWIFT in figures

- 32.8 million: FIN messages peak day (2017)
- 7.1 billion: FIN messages per year (2017)
- 8.4%: Increase in FIN traffic (2017)
- 11,000+: SWIFT users
- 200+: Countries and territories

32.8 million
FIN messages peak day (2017)

7.1 billion
FIN messages per year (2017)

8.4%
Increase in FIN traffic (2017)

11,000+
SWIFT users

200+
Countries and territories
Banks  Fund Managers
Central Counterparties  Clearing & Settlement Systems
Corporates  Broker-Dealers  ICSDs
Central Banks  Global Custodians
CSDs  Stock Exchanges
Depositories  Trade Repositories
Today’s Compliance Challenges

Cyber Security
- Top 5 priority at the Board level
- Increased sophistication
- Business continuity

Regulatory Expectations
- Manage change through good governance
- Strong compliance culture
- Data management
- GDPR readiness

The Cost of Compliance
- Budgets continue to increase
- Skilled resources and training
- New Regulation
- Tools & processes

Increasing personal liability
- Increase of accountability regimes globally
- Individual accountability of senior managers
- Increasing standards of conduct & oversight

Impact of Technology
- Mobile payments
- Interoperability
- Real Time Payment Systems
- DLT

Effects on the Global Community
- Rationalization of correspondent relationships
- Financial Inclusion
- North American dominance is changing
The Shared Utility approach

Collaboration
- Ideas
- Best practices
- Technology

Benefits
- Time & Resources
- Cost
- Standards

Barriers
- Trust
- Regulators
- Critical Mass

Use Cases
- KYC
- Cyber Security
- Fraud
KYC Market Challenges

**Challenges**

- Increasing cost of doing business (KYC CDD/EDD) = de-risking
- Increase in AML/KYC fines ($>3 billion/2 years)
- Increasingly complex, bilateral, repetitive KYC process

**Bilateral-Decentralized Model**

**Centralized – Utility Model**
SWIFT Customer Security Programme

Supporting customers in three mutually reinforcing areas

You Secure and Protect
SWIFT Tools
Customer Security Controls Framework

Your Counterparts Prevent and Detect
Transaction Pattern Detection – RMA, DVR and Payment Controls

Your Community Share and Prepare
Intelligence Sharing
SWIFT ISAC Portal
Tackling Payment Fraud

Your Counterparts: Primary Focus
Insider fraud where back-office compromise allows fraudulent payments to be sent.

Your Counterparts: Secondary Focus
Wire fraud on corporate / retail accounts or account movements to launder fraudulent funds.

Payment Controls
In-network fraud detection and prevention
Sanctions Compliance

Christopher Johnson
Senior Manager, Financial Crime Compliance
Sanctions Compliance – Meeting the Evolving Regulatory Challenge

- **Regulation**
  - Simple
  - Segmented
  - Complex

- **Enforcement**
  - Sporadic
  - Significant Fines
  - Huge Fines & Close Surveillance

- **Policy**
  - Ad hoc
  - Regionalised
  - Centralized

- **Controls**
  - Manual
  - Black Box
  - Sophisticated

- **Assurance**
  - Absent
  - Ad hoc testing, 2nd Level Controls
  - Model Validation, Comprehensive Coverage

**Time**
Compliance Assurance - Survey

• How often does your organization regularly (at least once a year) test the AML and Sanctions systems?

• How many of you believe your institution has an understanding of how these systems operate?

• When was the last time a parameter change was made?

• Do you understand the impact of threshold or model changes?
## Sanctions Compliance – The Challenges

<table>
<thead>
<tr>
<th>Sanctions Compliance</th>
<th>Verifiable Assurance</th>
<th>Resource Efficiency</th>
</tr>
</thead>
</table>
| • Is my Watchlist Filtering effective?  
• Can I make it more effective? | • Can I prove it?  
• Can I demonstrate that I understand it? | • Is my Watchlist Filtering efficient?  
• Can I make it more Efficient? |
Sanctions Compliance – Balancing Priorities

Effectiveness – Testing
- Meeting Regulatory Demands
- Provide assurance that your filter works
- Measure system’s fuzzy matching performance
- Assess coverage of sanctions lists
- Align screening system to your risk appetite

Efficiency – Tuning
- Managing Cost and Resources
  - Reduce false positives through iterative testing
  - Build optimisation tests into your processes
- Understand parameter changes
- Manage and tune rules and “good-guy” lists
Operational Lifecycle - Best Practice Testing

- Investigations
  - Specific focused tests to verify and dig deeper on issues discovered

- Assurance
  - Periodic
  - Continuous
  - BAU Tests
  - Policy Alignment

- Continuous Improvement
  - Effectiveness and Efficiency Tuning
  - Model Understanding

- Regression
  - Change Assurance
  - Release Management
Tuning Projects – Basic Principles

• Iterative Approach
• Constrained Change between Iterations
• Efficient and Flexible Iteration
• Rigorous Recording and Documentation
• Consistent Test Environment

• The following dimensions should be considered to ensure sufficient coverage of tests can be performed within the required timeframes
  – Number of test iterations
  – Number of configuration changes per iteration
  – Number of test files
  – Sample size
Tuning Tests - Classification

Baseline Tests

• Typically broad in scope and provide a before and after comparison of a configuration change to ensure there is no detrimental impact on filter effectiveness
• Validates that a configuration change does not cause unexpected filter behaviour

Tuning Focus Tests

• Tests that focus on scenarios that will measure the success of the tuning, focusing on the areas of the filter being addressed
• Depending on the configuration change, these test cases could be a combination of historical problem cases, hand crafted tests or test cases meeting specific criteria

Impact Tests

• Tests that measure the overall impact on hit rates as a result of the configuration change
• Artificial data can be used to provide an indicator, but these tests should typically use a sample of real production data
Define Tuning Objectives
Identify Configuration Options
Define Tuning Focus Tests
Define Test Iteration
Tuning Focus Tests
Results Analysis
Baseline Testing
Impact Testing

Drill into Results
Regression testing

Compare new filter candidate with current filter version

- Review filter release notes
- Run tests with current filter
- Run tests with candidate filter
- Compare & analyse

Scope of tests
- Hit Rate
- Exact matches
- Fuzzy matches
- Custom (probing the changes highlighted in release notes)

Decision

YES

NO
Threshold Analysis – Fuzzy Effectiveness and Customers Alerted
Peer Analysis – Comparison Example

<table>
<thead>
<tr>
<th>List</th>
<th>Details</th>
<th>Records</th>
<th>Misses</th>
<th>Effectiveness</th>
<th>Peer Analysis</th>
<th>Narrative</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFAC SDN</td>
<td>Company Primes &amp; Strong Aliases</td>
<td>5515</td>
<td>10</td>
<td>99.82%</td>
<td></td>
<td>76.9% of peers miss fewer than 10 records.</td>
</tr>
</tbody>
</table>

- No Misses: 31%
- <=10: 46%
- 10+: 23%
- Not Screened: 0%
The results show depth 1 performance for the filter for *individual* entities for each derivation. Results allow comparative analysis between derivations and relative to peer ranges.
# Common Filter Issues Identified Through Testing

<table>
<thead>
<tr>
<th>Sanctions Lists Quality</th>
<th>Screening Policy</th>
<th>Message Types</th>
<th>Filter Weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Outdated lists</td>
<td>• List scope incorrect or not aligned with bank policy</td>
<td>• Inconsistent screening performance across message types</td>
<td>• Poor fuzzy matching performance</td>
</tr>
<tr>
<td>• Missing entry types</td>
<td>• Inconsistent implementation across filters</td>
<td>• Message or file elements not screened properly</td>
<td>• Line break, word order, sequences</td>
</tr>
<tr>
<td>• Missing entries</td>
<td>• Entity and alias types screened unnecessarily</td>
<td>• Overreliance on specific fields (e.g. address or country)</td>
<td>• Poor performance against particular entries (short or long names, aliases)</td>
</tr>
<tr>
<td>• Language variants not screened correctly</td>
<td></td>
<td></td>
<td>• Character set matching issues</td>
</tr>
<tr>
<td>• Deleted records still screened</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Sanctions Lists Quality**
- Outdated lists
- Missing entry types
- Missing entries
- Language variants not screened correctly
- Deleted records still screened

**Screening Policy**
- List scope incorrect or not aligned with bank policy
- Inconsistent implementation across filters
- Entity and alias types screened unnecessarily

**Message Types**
- Inconsistent screening performance across message types
- Message or file elements not screened properly
- Overreliance on specific fields (e.g. address or country)
SWIFT Sanctions Testing

Comprehensive Sanctions Quality Assurance

Ensuring Filter Effectiveness
- Quantify and Reduce Risk
- Model Validation and Fuzzy Effectiveness
- Coverage and List Validation

Managing Cost & Resources
- False Positive Reduction
- Filter Tuning and Optimisation
- Test Cycle Automation

Assurance, Insight and Understanding
- Captures risk appetite
- Fact based filter management
- Standard reports
- Community based approach