An Oracle White Paper
October 2009

An Integrated Approach to Fighting Financial Crime: Leveraging Investments in AML and Fraud Solutions
Executive Overview

Today’s complex financial crime schemes pose increasing business and reputational risks to financial services firms. Financial crime costs an estimated $20 billion in losses annually, and the operational costs of compliance are growing substantially year after year. That’s why the need to limit losses and reduce the costs of compliance is a matter of urgent concern for the financial services industry.

Introduction

Traditionally, the industry has viewed compliance and financial crime as two separate areas. While substantial investments have been made in anti-money laundering (AML) compliance and fraud prevention, these two areas are typically managed in a silo’d fashion – an approach that is no longer sufficient to address evolving risk management and regulatory requirements. Compliance and risk officers now see that better integration of fraud management and AML compliance is the direction they must take to fully understand the complete impact of financial crime on their institutions, improve their return on risk and compliance investments, enhance the institution’s reputation with investors and shareholders and cultivate trust with customers and business partners.

This whitepaper outlines ideas to help optimize an institution’s approach to financial crime and compliance management by leveraging the synergies and return on investment (ROI) that can be gained from addressing AML compliance and fraud prevention in tandem, thereby helping achieve a more unified view of financial crime and risks across the enterprise.
THE CASE FOR CENTRALIZED FINANCIAL CRIME & COMPLIANCE MANAGEMENT

Due to regulatory and reputational pressures, financial services firms are focusing more than ever on implementing effective Governance, Risk and Compliance (GRC) programs. GRC is viewed as critical to rectifying organizational weaknesses that lead to significant operational risk, losses, or regulatory censure or fines, as well as helping avoid such problems. A key challenge, however, is how to bridge specific areas of risk and compliance into a unified and enterprise-wide approach.

Taking an enterprise approach to financial crime is an area where a firm can get the most “bang for its buck”. Fraud and money laundering are considered key operational risks to financial institutions’ profitability and reputation. Implementing effective fraud and AML detection, prevention, and security systems has become a critical part of a firm’s ability to control operational risk.

Financial institutions have made substantial investments in AML compliance and fraud prevention measures. Typically, these solutions, systems or reporting mechanisms have been implemented in a silo’d fashion, specific to line of business or channel. The result is significant exposure, since most fraud schemes (and many money laundering schemes) cross channels, products, and even lines of business. The "umbrella" for financial crime extends more broadly, beyond only AML or fraud, and requires an enterprise-wide approach to monitoring, detection and prevention.

KEY BENEFITS OF A CENTRALIZED FINANCIAL CRIME & COMPLIANCE MANAGEMENT

Following are key benefits of taking a more integrated approach to AML compliance and fraud prevention efforts:

Understand the Full Impact of Financial Crime on Your Institution

An integrated approach to AML compliance and fraud prevention provides a more holistic view across lines of business, channels and products. It creates an extra “layer” to review high-risk customers, channels and products, and helps you better understand how anti-fraud and AML efforts apply to the totality of the institution’s operational risk assessment.

Improve Your Return on Risk and Compliance Investments

Financial institutions are being asked to do more with the same or fewer resources. Combining and centralizing your compliance and fraud analytical teams can provide synergies, cost savings and efficiencies – in terms of both systems and people - for your transaction monitoring programs. Alert and case analysis and investigations leverage many of the same skill sets and data to address both compliance and operational risk. If properly staffed, a centralized unit provides highly skilled analysts and investigators that complement your transaction monitoring teams, resulting in more efficient and effective investigations, loss mitigation, and reporting.
Enhance Your Institution’s Reputation & Cultivate Customer Trust

Security and trust are paramount in the minds of customers today. Taking a more integrated and effective approach to financial crime management reinforces your institution’s commitment to compliance and risk management.

KEY CHALLENGES OF A CENTRALIZED FINANCIAL CRIME & COMPLIANCE MANAGEMENT

While the benefits are substantial, taking an integrated approach to AML compliance and fraud prevention requires focus, commitment, and hard work. Key challenges include:

Moving Beyond a Silo’d Approach to AML and Anti-Fraud Programs
AML compliance is typically organized by business and/or jurisdiction, and sometimes centralized at the enterprise level, however, the systems, solutions and technologies used may vary by line of business or regulatory jurisdiction. Fraud management and prevention programs are typically even more segmented than this with point solutions deployed for specific types of fraud, such as check or deposit fraud, or for specific channels or products, such as credit cards or ATM transactions.

Leveraging or Integrating Various Data Warehouses or Data Marts
Each installation of a point AML or Fraud system may have involved the creation of a specific data base or data mart to support that system. Multiply this by the many point and source systems you rely on for both AML and fraud prevention, and you quickly realize the enormity of the work required to better integrate these data sources.

Rationalizing the Use of Different Watch Lists and Risk Assessment Mechanisms
Both AML and fraud prevention efforts require the use of various watch lists. While there is some overlap in the lists used, there may also be specific lists that are developed, maintained, and leveraged differently from system to system. Also, the risk scoring of entities or accounts on these watch lists can differ.

Recognizing and accommodating the differences in focus and investigatory workflows
For AML compliance, regulatory reporting requirements are the main driver. Case investigations and evidence to support reporting or non-reporting are typically developed over time. In the area of fraud prevention, however, the objective is to detect (or even prevent) fraud schemes as early as possible to mitigate losses and reduce their impact on the customers. Alert and case investigations must be completed quickly, often with incomplete information. In addition, real-time monitoring, alerting and interdiction capabilities are critical to fraud prevention.
AREAS OF SYNERGY BETWEEN AML COMPLIANCE & FRAUD PREVENTION

With the benefits and challenges acknowledged, let’s take a closer look at some areas of synergy between AML compliance and fraud prevention that can be leveraged to rapidly and easily achieve an integrated approach to financial crime and compliance management.

Figure 1. Areas of Synergy Between AML and Fraud

Data

There is a high correlation of data used in both AML compliance and fraud prevention efforts. For example, the same products or transaction types, such as wires, electronic / ACH payments, and stored value products, are typically considered high risk and monitored more closely. Also, the same channels, such as online and remote access points, are considered to be at higher risk for both money laundering and fraud. AML and anti-fraud efforts also leverage the same account and customer information, as well as similar peer group definitions, in helping to detect potentially suspicious activities. There may also be some overlap in the use of certain watch lists, such as lists of entities on which SAR's have been filed, other known high risk entities, and so forth.
Detection Scenarios & Risk Models

Certain scenarios or detection models may be used for both AML and fraud detection. Many AML scenarios may also be indicative of fraudulent behaviors, and vice versa. AML scenarios can be repurposed for Fraud detection by adding fraud-specific parameters for detection and risk scoring.

Also, the high degree of commonality of data requirements across AML and Fraud scenarios can reduce costs and time to on-board new scenarios, or re-purpose existent AML scenarios for fraud detection.

KYC Program (CIP/CDD)

Know Your Customer (KYC) programs are primarily a Bank Secrecy Act (BSA) requirement, but KYC and enhanced due diligence procedures can serve as an important fraud tool as well.

The Customer Identification Program (CIP) performs identification and authentication of new customers opening accounts at the institution. The background information obtained on the customer is used to establish a risk score or rating for that customer. The Customer Due Diligence Program (CDD) documents the customer's expected activity, in terms of transaction volumes and product and channel use.

This expected activity can be used in anticipatory and peer group profiling to monitor for deviations from expected activity that could be deemed suspicious or concerning. Both of these programs together provide coverage for many of the FACT Act Red Flags and contribute to the prevention of identity theft and account takeover schemes.

Alert & Event Correlation

Alert correlation is the intelligent aggregation and correlation of related entities and alerts; even alerts generated from disparate point AML or fraud solutions. Scenarios or risk models, along with alert correlation, provide a critical layer of intelligence to help in the fight against financial crime. Alert correlation combines AML alerts or exceptions with fraud point solution outputs, plus contextual data on the accounts or entities involved in those alerts. The result is more targeted and actionable fraud & AML alerts and cases.

This approach provides an enterprise view of alerts across existent AML and fraud silos, and allows you to leverage your firm’s existent AML and point fraud solution investments.

Alert and Case Investigation

Fraud and AML units working side by side in the same location facilitates cooperation (virtual teams can also work). A centralized monitoring approach facilitates easier hand-off of alerts, cases and investigations, as well as greater sharing of leads and information between the AML and fraud teams. It also supports load balancing across teams to meet the changing business/regulatory needs. For example, you can perform an annual or semi-annual audit of AML and fraud analytical and investigative teams, and assess individual unit performance. This can determine whether one unit has
significantly more activity. Cross-training and shifting of investigative staff can mitigate the risk of inadequate coverage.

Of course, your case management system must be able to support such an integrated approach, while still providing the specific workflows required by your AML and fraud analysts to be optimally effective and productive.

People

A centralized or more integrated monitoring approach can also provide significant benefits in your training and retention efforts. Cross training between different types of fraud or AML alert triage or case investigations helps to develop well rounded analysts and investigators. It facilitates load balancing across individual units. Even more importantly, it serves as an important retention tool, because you are able to provide more opportunities for learning and advancement.

Some financial institutions have established Financial Intelligence Units (FIU’s) or Financial Crime Units (FCU’s) to centralize and better coordinate their efforts against financial crime. Such centers become a valuable source of knowledge about the financial crime being attempted or perpetrated against the institution and its customers.

![Centralized Financial Crime & Compliance Platform](image)

Figure 2. Oracle Financial Services Financial Crime and Compliance Platform
REGULATORY CONSIDERATIONS

Once the majority of financial institutions moved to more robust and automated transaction monitoring systems to support AML compliance and suspicious activity reporting, regulators began to focus on how well the institutions have been leveraging their systems. A better targeted and more efficient AML monitoring system and program results in fewer defensive filings of SAR's and higher quality reports to law enforcement.

At the same time, regulators began to require increasingly tougher fraud prevention measures, especially in the areas of identity theft and account takeover. An emerging expectation is the integration of sophisticated analytics with fraud management – gaining more of an enterprise-wide view of fraud, even of those complex fraud schemes that tend to cross lines of businesses and products, and result in the most significant losses. Simply relying on point fraud solutions that focus on a specific product or channel is no longer sufficient.

One additional point: Loan losses, particularly on mortgages, have been and continue to burden the financial services industry and the government. Given the massive government intervention in the financial services industry, regulators want the AML department to support the fraud department in better detecting fraud.

CONCLUSION: ENSURE THE BROADEST POSSIBLE VIEW OF FINANCIAL CRIME

Financial institutions will continue to be called upon to do more with less. Especially in relation to regulatory compliance, but even more relevant within fraud management, where return on investment and impact to the bottom line can be directly calculated. Coupled with an increasing incidence of financial crime and the growing complexity of fraud and money laundering schemes, the result is a clear necessity to upgrade systems, streamline processes and improve efficiencies.

Additionally, as we continue through a time of upheaval and reduced earnings within the financial services industry, institutions must be even more focused on customer acquisition and retention. A reputation for strong compliance, security and risk management becomes a competitive differentiator and helps cultivate customer trust and confidence. Taking a more integrated approach to financial crime and compliance management helps ensure the broadest possible view of financial crime, improves return on risk and compliance investments and enhances the institution’s reputation.