Table of Contents

Introduction ..................................................... 1
Get Ready for the New Wave of Cybercrime ..................... 1
The Industry Is Taking Action ................................... 3

Limitations of Traditional Fraud and AML Approaches ........ 3
The Necessary Analytic Rigor Is Lacking ......................... 3
Fraud and AML Are Managed in Silos .......................... 4
Investigation Tools and Processes Are Not as Efficient as They
Could Be .................................................................. 5

Five Must-Have Capabilities for Fighting Financial Crime .... 5
1. A Holistic, Behavior-Based View of ‘Normal’ .................. 6
2. Cross-Channel Visibility ....................................... 6
3. Alert Management of Fraud and Anti-Money Laundering Events . 7
4. Central Case Management ..................................... 8
5. Entity Linking ...................................................... 8

The SAS® Financial Crimes Suite ................................. 9
The Benefits of Integrating Fraud and AML Programs .......... 11

This white paper was written by David Stewart, CAMS, Director, Financial Crimes Practice for Banking at SAS. As Director, Stewart leads strategy development, drives product management and provides key marketing counsel for SAS anti-money laundering and fraud management solutions worldwide. In addition to working closely with financial services institutions and regulatory agencies, Stewart collaborates with SAS R&D and implementation teams to deliver industry best practices for financial crimes solutions. Previously, Stewart served as a SAS Business Manager for one of the world’s largest financial institutions. He managed a team responsible for implementing enterprise-scale projects devoted to customer relationship management and AML initiatives. In addition, Stewart has held various relationship management responsibilities for financial services customers over the past 16 years.
Introduction

Meyer Lansky is not exactly a household name, and he has been gone for nearly 30 years, but his influence is felt every day. Lansky is credited as the father of modern money laundering.

After Al Capone went to prison, Lansky realized he needed to hide the sources of his money. He laundered an estimated $1 billion from his casino empire through accounts and businesses in Switzerland, Hong Kong, South America and the Caribbean.

By all accounts, he pioneered the offshore model well. Lansky was never convicted, and when he died in 1983, he was worth an estimated $100 million or more. Nobody really knows.

Impressive as it is, that’s pocket change in today’s fraud and money laundering world. A single fraud hit can strip an institution of more money than Lansky ever possessed. Just ask one of the largest banks in Europe, which lost more than $7 billion when a rogue employee executed a series of elaborate, fictitious transactions.

“Cyber-thieves have cost US companies and their banks more than $15 billion in the past five years,” wrote Joseph Menn of Financial Times, quoting an FDIC study. Card fraud costs the US card payments industry about $8.6 billion annually, with the bulk of the losses falling on card issuers. The FBI estimates that corporate account takeovers cost US companies as much as $1 billion in 2011 alone.

The sheer magnitude of the losses is one clue that financial criminals are growing ever more sophisticated, more organized, and more capable of exploiting vulnerabilities in new electronic channels. The losses hurt a bank’s reputation and bottom line, but there’s also the issue of social good. How many of the illicit transactions are financing organized crime, drug smuggling, human trafficking, kleptocracy or terrorism?

Get Ready for the New Wave of Cybercrime

“We are witnessing a plethora of new, high-tech value transfer systems that can be abused to launder money and finance terror,” said former US Treasury Special Agent John A. Cassara, an industry adviser to SAS. The Financial Action Task Force (FATF), the global anti-money laundering policymaking body, calls them “new payment methods,” or NPMs.

Examples include digital precious metals, Internet payment services, prepaid calling and credit cards, and mobile payments or “M-Payments.” Although the technology and terminology are changing rapidly, generally speaking, M-Payments are acknowledged to mean the use of a cellphone to credit, send, receive or transfer money or digital value.

US consumers have been cautious – citing concerns over mobile phone privacy and security – but M-Payments could grow rapidly on such apps as Google Wallet, a mobile payment system that allows users to store debit cards, credit cards, loyalty cards, gift cards and more on their mobile phones.

---

3 “Corporate Account Takeover – Traditional Protection Strategies Not Enough; Multi-Dimensional, Preemptive Strategies Needed,” ACH Alert, 2011
“Today only 1.5 billion people have direct access to financial services, but there are more than 5 billion cellphones,” Cassara noted. “By 2020, experts predict more than 50 billion connected devices. … In the US, M-Payments are projected to gross $214 billion by 2015, including transactions involving mobile bill payments and carrier billing transactions.”

US consumers have been cautious in adopting mobile banking, but M-Payments could grow rapidly on such apps as Google Wallet, a mobile payment system that allows users to store debit cards, credit cards, loyalty cards, gift cards and more on their mobile phones.

“Assuredly, criminals and criminal organizations will be attracted to this new financial and communications medium,” said Cassara.

Cybercrime threats continue to loom large. In a 2012 study conducted by Javelin Strategy & Research, risk and fraud executives noted an increase in man-in-the-middle, man-in-the-browser and other malware attacks. The risks are pervasive, expanding with greater online presence. Javelin’s consumer data shows that more than 10 percent of the identity fraud victims who knew how their information was stolen reported that it was taken when simply making purchases online; another 9 percent reported that their information was stolen through the computer due to stolen password or keystroke capture.4

Figure 1: Electronic channels open up multiple opportunities for identity theft – valuable information for both fraudsters and money launderers.

4 Current State of E-channel Fraud Trends: Online Banking, Mobile Banking and Card Fraud, Javelin Strategy & Research, August 2012
The Industry Is Taking Action

Under pressure to protect itself from regulatory fines, financial loss and loss of reputation, the financial industry is taking action. It is responding to regulators’ expectations to put new controls and reporting in place. It is building out fraud programs and anti-money laundering (AML) programs in its various organizational units. It is replacing manual processes with automated solutions, or replacing outdated solutions with new ones.

By 2013, banks and businesses will spend $4.3 billion on information technologies to help them fight back, according to Chartis Research. The global market for AML software alone has reached US$450 million and is expected to expand at a compound annual growth rate of 9 percent, reaching $690 million in 2015.

But is it enough? Could all this investment deliver better returns than it does?

Limitations of Traditional Fraud and AML Approaches

The Necessary Analytic Rigor Is Lacking

Fraud detection systems have traditionally relied mostly on business rules. Rules are good for identifying new incidents of lessons already learned, but rules alone have their limitations:

• **Business rules create a lot of noise.**
  Legitimate customers constantly do things that look suspicious: deposit a check for more than the average amount, submit a claim, change an address, add a bill pay recipient to online banking. Any of these activities could trigger false positives that take time to triage and result in operational inefficiency – while annoying or even humiliating good customers.

• **Business rules become common knowledge to the fraudsters.**
  Either by trial and error – or by infiltrating the organization – business rules become known. This leads to greater organizational risk, which leads to constant tweaking of rule parameters and thresholds, which leads to more operational inefficiency.

• **Managing business rules is an imperfect balancing act.**
  Loosen the controls too much, and you overwhelm investigators with too many low-quality alerts. Tighten the controls too much, and you miss incidents that fall just under the radar.

• **Business rules capture hindsight, not foresight.**
  They don’t know how to catch emerging patterns of fraud and money laundering. They also can miss crimes that are concealed in complex layering of transactions across channels, products and accounts.

“**In our increasingly interconnected global village, criminal elements will assuredly take advantage of innovative developments in mobile banking, commerce and communications to further criminal endeavors and launder illicit funds.**”

John A. Cassara
Former US Treasury Special Agent

---

Ultimately, a suspicious activity is not necessarily the one that exceeds a business rule but rather the one that is out of bounds in relative context. For example, it could be a change in loan payment frequency from monthly to annual to hide a lapping scheme. It could be some activity that appears normal but is abnormal for that particular customer or when viewed in broader context across accounts, entities and time.

A deeper view is required – one gained by applying scenarios and risk factors to transactions, then applying additional processes to the alerts that are generated – such as suppression, risk scoring and routing. With analytical insight determining which alerts should be prioritized, investigators can focus their efforts where they will have the most value, rather than on chasing all simple alerts.

**Fraud and AML Are Managed in Silos**

In the last 25 or 30 years, the banking industry has approached financial crimes, particularly fraud, in a fragmented and reactive manner. As new products, channels, and access points have been introduced, niche fraud systems have been created to meet demand. As a result, banks operate with a patchwork of systems and tools, even within a channel or product group.

Furthermore, most large banks have multiple fraud groups – a check fraud group, an ACH fraud group, a wire fraud group, a credit card group, and so on. These groups tend to work in silos, so they don’t have a holistic view of risk across the organization – often a necessary prerequisite to detect complicated patterns of fraud.

Similarly, fraud and AML programs have developed separately within financial institutions as distinct programs addressing different issues. The industry has traditionally viewed compliance (AML) and fraud as separate disciplines – one focused on avoiding fines and the other on averting loss.

Financial institutions have made substantial investments in both areas but done little to capitalize on the natural synergies between them. For instance:

- Most illicit activities span channels, products, entities and lines of business.
- Many fraud schemes have a money-laundering aspect to them, because the ill-gotten gains have to get into the financial system somehow. Conversely, many money laundering schemes have a fraud aspect to them.
- Fraud and AML programs run detection processes on similar data sets, such as records of account openings and transactions.
- Both fraud and AML programs work with the same law enforcement or regulatory agencies and generate Suspicious Activity Reports (SARs). The Financial Crimes Enforcement Network (FinCEN) of the US Treasury reports a 50-50 split of SARs for one and the other, dispelling the perception that regulators are only concerned with money laundering.
- Fraud and AML investigators tap into the same information for investigations and often independently work the same cases.
"Financial criminals do not operate in silos the way that large financial institutions organize their anti-money-laundering (AML) and fraud prevention programs," wrote John Byrne and Chris Swecker in ABABankingJournal online. "While many small- to mid-size banks have effectively integrated fraud and AML programs, many large financial institutions continue to house AML and fraud in separate ‘silos.’ … Change is essential to keep pace with the threats and to reduce risk and cost."

**Investigation Tools and Processes Are Not as Efficient as They Could Be**

When fraud and AML departments are segregated and compartmentalized – with insufficient oversight at the enterprise level – there is little information sharing and much duplication of effort. Process inconsistency leads to inefficient or incomplete investigations that in turn misrepresent true risk exposure, reduce recoveries and could lead to greater regulatory scrutiny.

As a result of inefficiencies, financial investigative units may struggle to staff adequately, so some threats may go unaddressed. If the institution had a better way to manage alerts generated from separate fraud and AML systems, investigators could prioritize and focus their resources on those events that represent the greatest threats to the institution.

**Five Must-Have Capabilities for Fighting Financial Crime**

Silo approaches, limited use of analytics, separate and redundant case management systems – these limitations are the industry's legacy, but not its future. The technology is available today to launch a unified defense against financial crime, with five essential capabilities:

- **A holistic, behavior-based view of “normal,”** to more accurately detect suspicious behavior.
- **Cross-channel visibility,** to detect complex patterns of behavior that may involve multiple layers across channels, products and accounts.
- **Alert management of fraud and AML events,** to automate decisions and score risk before the investigation process.
- **Integration of anti-fraud and anti-money laundering,** to improve efficiency and effectiveness in fighting financial crime while reducing the cost and effort.
- **Central case management,** to provide a shared repository and workflow tool for both fraud and AML investigations that fosters greater collaboration and information sharing among those teams.
- **Entity linking,** to identify collusion or fictitious accounts by quickly visualizing relationships that cannot be detected through traditional methods.

---

1. A Holistic, Behavior-Based View of ‘Normal’

Accurately detecting fraud and money laundering requires not just knowing whether an activity or event has met a certain business rule, but whether that trigger is meaningful. For example, it’s not enough to say, “We’ll flag transactions of \( x \) type over \( y \) dollar amount.” There are plenty of good customers making transaction \( x \) over \( y \) dollar amount, and the bad guys quickly figure out \( x \) and \( y \) and find workarounds.

True detection relies on understanding behavior in broader context, as well as being able to detect new patterns. Analytics is required to properly group customers and accounts that should behave similarly. A hybrid approach supplements rules by applying multiple flavors of analytics, such as:

- **Predictive modeling.** Neural networks, decision trees, generalized linear models, econometric models and gradient boosting can unearth new cases and patterns based on the previous disposition of alerts and cases.
- **Text mining.** Extract meaningful information from vast stores of unstructured (text) data, such as reports, staff notes, social media and websites.
- **Anomaly detection.** Techniques such as mean, standard deviation, percentiles, univariate and multivariate regression, clustering, sequence analysis and peer group analysis can be applied to identify abnormal patterns in the data.
- **Automated business rules.** Transactions can be filtered on sophisticated rules that reflect behavioral patterns/factors associated with suspicious behavior. For example, automated rules could flag transactions made by the same customer in multiple time zones in a short period of time.
- **Database searches.** Supplement detection and investigation processes with data from internal and external sources, such as from Lexis Nexis, CIS, DowJones, Websearch, Dunn/Bradstreet and OFAC.
- **Social network analysis.** Identify links between people and businesses that could reveal organized crime activities.

A hybrid approach that augments business rules with analytics delivers much higher quality alerts, so investigators’ time is used more productively, and customers are not inconvenienced with false positives.

2. Cross-Channel Visibility

From a customer perspective, banks are seen as a single brand that operates across multiple channels (ATMs, branch offices, online, call centers, mobile, etc.). From a bank’s perspective, customers are seen as diverse entities based on product – mortgage, credit card, consumer banking, small business, home equity, etc.

Criminals know this fact all too well. They know bank fraud systems rarely monitor customer behavior across multiple accounts, channels and systems. That vulnerability paves the way for hiding fraud and money laundering activities in cross-channel transactions.
SAS recently commissioned a research firm to conduct a study on mobile banking security. Of the 12 banks in the study – 12 of the largest banks in North America – none had a good key performance indicator, key risk indicator or other quantitative measure of cross-channel fraud.

That’s troubling, because cross-channel visibility is essential to quantify the exposure presented by more sophisticated attacks. Transactions that look innocent at face value could be exposed as suspicious when correlated with activities in other areas. Only with an enterprise view that integrates departments, products and channels can a financial institution get a clear picture of a customer’s risk profile and the institution’s overall exposure.

It is imperative to source cross-channel data to the detection process in order to have a clear view of behavior across channels and relationships. This is particularly true in real-time or intraday detection to thwart zero-day fraud attacks where criminals use a number of different channels to withdraw funds.

3. Alert Management of Fraud and Anti-Money Laundering Events

The current separation of fraud and AML programs is more a matter of culture and business impact than reason. Investigation units want a more consistent process for managing alerts per the unique business requirements of fraud and AML units:

- Fraud operators need to take action on specific accounts or transactions to protect customers, which often requires frequent changes to strategies in the face of rapid attacks.
- AML departments have specific alert handling requirements based on the types of cases involved, complexity or the need to contact law enforcement.

Regardless of the type of behavior, most institutions want to escalate events that trigger multiple factors or are the subject of multiple investigations.

“As a result of the financial crisis, many financial institutions seek greater efficiencies in their fraud and AML functions ‘to do more with less,’” wrote Byrne and Swecker. “The issue of merging fraud and AML functions is a matter of maximizing the bank’s return on investment in both areas. Many industry experts believe that the efficiencies, cost savings, loss reductions and increased recoveries to be gained by integration will increase shareholder value at a time when protecting the bottom line has never been more heavily scrutinized.”

This integration doesn’t have to be a complete merger of organizational units. It’s more about establishing a view across those areas and common ground for information sharing and collaboration. A solid foundation for this integration is a consistent process for applying logic to events – one that collects, consolidates, processes and automates alerts from existing silo-based detection systems and enriches them for further investigation and disposition.
The degree to which the functions are coupled is up to each institution. Ideally, an integrated platform enables the sharing of data at multiple points in the detection and decision life cycle.

4. Central Case Management

“That largest area of concern is internally related to the lack of a robust enterprise case management system. … The greatest area for immediate action appeared to be in the area of centralizing the fraud management function.”

That’s the word from an Aite study published a few years ago but just as relevant today.7 A centralized, shared platform can automate and streamline the business process for investigating cases in real time and near-real time. A strong case management solution is one that enables investigators to:

• **Create multiple workflows for various case types** – such as fraud, physical security and AML – to automatically route cases to the right individuals or groups. You can also designate certain action items as prerequisites before the case can proceed to the next step in the workflow.

• **Receive alerts from monitoring systems** and import existing records and historical information from originating systems to help prevent rekeying errors and reduce the volume of duplicate data.

• **Review work items sent electronically** to the system before creating a case or linking the incident to a case.

• **Easily store documents with a case**, including any digital media that may need to be retained for future viewing. With all pertinent materials archived together by case, all necessary documentation is retained for audit purposes, and investigators can review previous subjects more efficiently and effectively.

• **Prepare batch files for uploading** to complete regulatory reporting requirements, such as for SARs and CTRs, as well as any other formal internal or external documentation or reporting requirements.

A centralized case management platform makes it easier to coordinate and collaborate on alerts and investigations, as well as share leads, information and best practices between the fraud and AML teams.

5. Entity Linking

Institutions that are serious about combating financial crimes are adding entity link analysis (also called social network analysis) to their arsenals. Network analysis helps investigators detect and prevent criminal activity by:

• Identifying patterns of behavior that only appear as suspicious when viewed across a community of related accounts or entities.

• Discovering the networks associated with an identified suspicious account, entity or individual to determine if a case is an isolated behavior or part of a criminal conspiracy.

• Aggregating the potential exposure of both known frauds and existing credit limits.

---

For example, the SAS Advanced Analytics Lab created an application that enables an automobile insurance provider to better identify fraudulent claims. The system identifies staged accidents or false claims by spotting suspicious patterns or overlaps, such as cases where an individual is the insured party in one case and a passenger in another, or where the insured party and claimant have the same phone number, or where there is repetitive use of the same body shops and medical professionals.

The unique network visualization interface helps investigators see these connections more clearly, so they can uncover previously unknown relationships and direct their investigations accordingly. In addition to detection and risk scoring, investigation teams can review visualizations of relationships that include individuals flagged by existing rules, anomaly detection or predictive modeling. Investigators have fast access to customer details and all related parties and networks, resulting in quicker case assessments and better dossier production.

The SAS® Financial Crimes Suite

SAS provides an end-to-end technology infrastructure for detecting, preventing and managing financial crimes (fraud and AML) across business lines. This framework includes components for data management, detection and alert generation, alert management and case management, along with category-specific workflow, content management and advanced analytics, including social network analysis.

With a modular approach, customers can adopt an enterprise approach to controlling financial crimes, while incrementally deploying targeted capabilities, such as packages for:

- Anti-money laundering.
- Enterprise case management.
- Currency transaction reporting.
- Customer due diligence.
- Sanctions monitoring.
- Predictive alert analytics.
- Fraud detection.

Data is gathered and mapped from all product lines, organizational units and geographic regions of the organization. Authorized users access the various modules from a consistent user interface. Dashboard reporting gives at-a-glance views of key performance indicators relevant to analysts, investigators or managers.

This unified framework enables financial institutions to:

- Gather and share relevant data from across the organization.
- Analyze this data to connect the dots and spot attacks early in their life cycles.
- Plan and execute focused countermeasures to protect customers.

Network analysis goes beyond transaction and customer views to analyze activities and relationships within a network of related entities, such as customers who share demographic data or transactions.

Through network analysis, investigators can easily see whether customers, accounts or other entities are associated in ways could indicate criminal activity.

The financial savings of consolidating two or more components, thereby eliminating redundancy and inefficiencies can be significant, depending on the size of the organization. These savings can more than offset the expenses of consolidation and procurement of the necessary technology.

John Byrne, CAMS, and Chris Swecker
ABABankingJournal, Feb. 12, 2012
Commonwealth Bank of Australia chose a single-platform approach to address all financial crime, including various types of fraud and money laundering. John Geurts, Executive General Manager for Group Security and Chief Security Officer, explained why his organization took a unified approach to fraud and AML:

"We adopted a platform approach because we needed a holistic view of fraud and financial crime that was independent of product, channel or geography. We were also looking to achieve an economy of scale, reducing data storage costs, enabling reuse across the group. In addition, we needed the flexibility to add new products, services and channels to the platform at a far lower incremental cost than installing another customized fraud detection system."

Within months of implementing the SAS platform, the Commonwealth Bank detected twice the level of check fraud compared to its previous system, saw a 95 percent increase in check fraud detection efficiency, and had a 60 percent improvement in Internet banking fraud alert volumes.

Aite positioned SAS as the leader in its June 2011 Global Anti-Money Laundering 2011 Competitive Landscape report. Chartis Research reports that SAS solutions “feature strong capabilities in the important areas of analytics, business intelligence, case management and data management” – and highlights advanced analytics, configurability, data management and reporting/dashboards as key differentiators.8

---


---

Figure 2: SAS provides an integrated platform for monitoring, managing and reporting financial crimes with enterprise perspective and information sharing.
The Benefits of Integrating Fraud and AML Programs

Many financial services firms are already moving in this direction. An Ernst & Young survey of 250 respondents from financial services, law enforcement and regulatory agencies around the world showed positive progress. More than half of financial services firms represented in the survey (52 percent) had already integrated some aspects of their anti-money laundering and anti-fraud functions.⁹

The benefits are compelling:

- **Avoid duplication of resources and processes.**
  “Consolidating AML and fraud-related technical and procurement support under the same manager may limit deployment of redundant or incompatible technology, prevent technology silos, and rationalize existing applications and software,” wrote Byrne and Swecker. “Of secondary importance is the elimination of redundant layers of management, investigators, support components and technology. Reorganizing staff, processes and technology involves significant cost savings.”

- **Gain a more accurate view of financial crime activity.**
  With a more holistic view across channels, products and business entities, the institution has an entirely different vantage point from which to assess risk and detect suspicious activity, as well as understand how well fraud programs are working at an enterprise level.

- **Improve investigator efficiency.**
  A converged system delivers more accurate alerts, objectively automates the scoring of events, and offers a shared platform to view all relevant data to speed time to decision. Investigators can find more criminal activity faster, with less cost and effort. For example, in one pilot project SAS did for a large US county department of social services, the system had an 83 percent hit rate detecting providers engaging in fraud and a 40 percent hit rate identifying fraud among participants – which yielded $31 million in annual benefits payment savings and a $3 million savings in investigator efficiency.

- **Enhance the institution’s reputation with all stakeholders.**
  By integrating its financial crime management efforts and gaining an enterprisewide view, the institution affirms its commitment to compliance and strong risk management, earning the trust of regulators, shareholders and customers.

It’s not a bad signal to send to potential hackers, fraudsters and money launderers either. The industry is arming itself, gearing up, addressing vulnerabilities, joining forces and taking advantage of high-powered analytics and high-performance computing. It’s a new era, more hostile to anyone trying to be a modern-day Meyer Lansky.

---

⁹ Survey, Linking anti-fraud and anti-money laundering programs – unrealized opportunity or unnecessary complexity? Association of Certified Anti-Money Laundering Specialists and Ernst & Young, December 2010
About SAS

SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions, SAS helps customers at more than 60,000 sites improve performance and deliver value by making better decisions faster. Since 1976 SAS has been giving customers around the world THE POWER TO KNOW®. For more information on SAS® Business Analytics software and services, visit sas.com.