

Tackling Financial Crime – The BPM Perspective

Channeling financial crime proceeds for illegal activities may not be a new phenomenon, but it has recently soared to alarming proportions. The spread of such unlawful acts is wide enough to include a whole range of criminal activities involving human trafficking, drug trafficking, illegal dealing with sanctioned companies or individual and terrorist financing. This sudden spate of crime has forced governments and regulatory organizations worldwide to confront this menace with an iron fist in a coordinated manner.

While it is immensely difficult to determine the true impact of financial crime in monetary terms, businesses and tax payers are estimated to be hit by billions of dollars annually. The International Monetary Fund has estimated the scale of global money laundering to be equivalent to 2% to 5% of worldwide Gross Domestic Product (GDP). The UK customs authorities, in particular, estimate the annual proceeds from crime in the UK to be anywhere between £19 billion and £48 billion. An early 2009 Gartner report commented that about 7.5% of U.S. adults lost money as a result of financial fraud last year, mostly due to data breaches.¹

Estimated annual cost of some type of organized crime

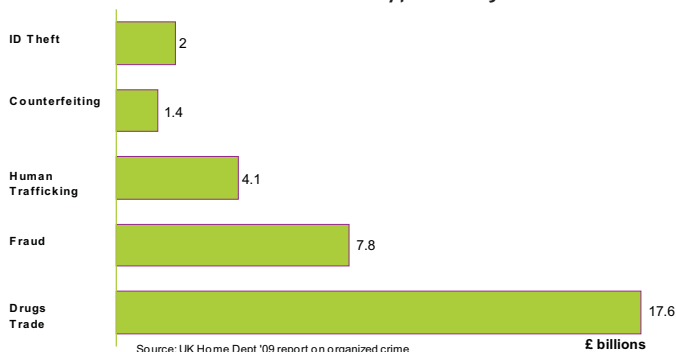


Exhibit 1

Regulatory Framework for Tackling Financial Crime

In wake of the stern measures advocated by regulatory authorities in the U.S., EU and UK to combat financial crime, the key compliance challenge for banks and financial organizations has been the lack of a standardized and consistent guideline arising from various regulatory regimes or suggested by different bodies overseeing multiple aspects of financial crime, with a mix of risk-based and zero tolerance approaches. To assist law enforcement agencies, the U.S. Patriot Act was transformed into law in October 2001. One provision, entitled Title III, legalized the freezing of U.S.-based assets of any suspected organization or individual involved in money-laundering, with the sole agenda of “starving” terrorist networks. In the UK, the Parliament passed the Terrorism Act 2000, and following the events of 9/11, the Proceeds of Crime Act 2002 (POCA) was passed. The Serious Organized Crime Agency (SOCA) was created in April 2006, whose aim is to reduce the impact of serious and organized crime, and subsequently the EU's Third Money Laundering Directive was implemented in December 2007 across the European Economic Area.

These acts mandate financial institutions to alert law enforcement officials on banking activity that is deemed suspicious.

In addition, the U.S. Congress granted the Treasury Department with regulatory powers to penalize any U.S. financial institution that might participate in these schemes, whether knowingly or not.

These financial sanctions, regulations and compliance activities tend towards a “zero tolerance” regime.

Regulatory Impact

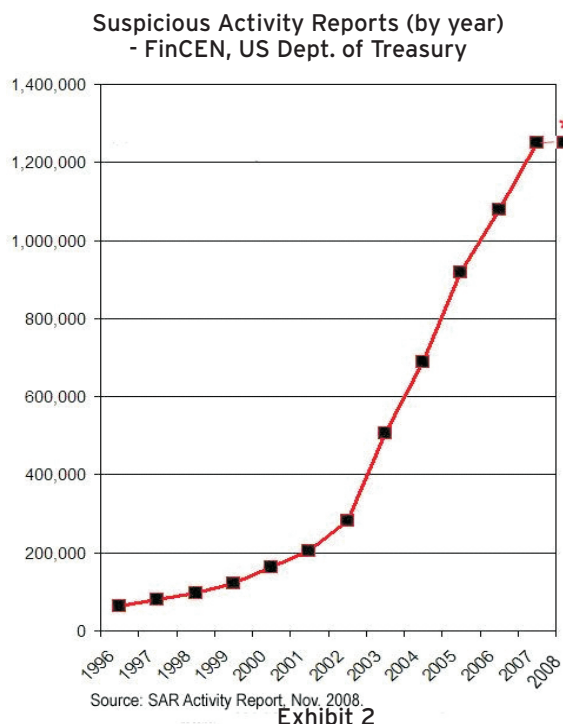
LTSB Bank paid \$350 million for breaches of compliance reporting relating to monetary transactions to sanctioned countries Sudan, Iran, etc. between 1995 and 2007.
- CNN News, January 10, 2009

Riggs Bank agreed to pay \$25 million in civil penalties for what federal regulators called a 'willful, systemic' violation of the Patriot Act's anti-money-laundering law.
- The New York Times, July 20, 2004

New Challenge: The Economic Downturn and Beyond

While financial crime has always been a threat to the economy, the ongoing downturn set off a "tipping point" syndrome. Financial institutions seeking new revenue streams have taken refuge in technologically advanced services to stay ahead of the competition. But the introduction of innovative financial instruments like stored value cards, remotely created checks (RCC) and Mail Order / Telephone Order (MOTO) by financial institutions - along with the increasing use of plastic money, e-commerce, online banking and high-tech

payment processing infrastructure -- has opened up new opportunities for financial criminals and has enabled their modus operandi to become more sophisticated. Financial institutions may have put in place state-of-the-art infrastructures to counter the spate of money laundering and financial fraud activities, but there is still a lot of ground to be covered. Unfortunately, most of the IT-enabled solutions leveraged by these organizations adopt a piece-meal approach addressing the needs of a specific business unit or performing only a part of the desired chain of counter-fraud activities, thus leaving a lot to be desired in terms of risk reduction, loss minimization or productivity improvement.



Failure to meet stringent anti-money laundering regulations or allowing suspicious transactions to go undetected can have a severe impact on any financial entity, including damage to its reputation, market capitalization, as well as its customer perception and loyalty.

Can BPM Show the Way in Solving Financial Crime Problems?

Leading financial institutions today leverage IT systems to combat the financial crime threat and meet regulatory compliance obligations. However, a quick look at the current technology landscape is good enough to unravel the "siloed" approach and the underlying disjointed architecture - direct fallout of which is additional investigation effort and prolonged turnaround time, leading to customer defection and loss of business.

A typical financial crime check solution (see Exhibit 3, below) comprises multiple fraud and money laundering

detection systems feeding into a human interface application for subsequent manual investigation. This also requires pulling data from other legacy systems such as customer datawarehouse, transactional data store, third-party credit bureaus etc., to facilitate the research process and take action on the flagged entity (customer / transaction).

Additionally, filter applications exist for matching entity (customer and transactions) with sanctions and politically exposed persons (PEP) watch lists, resulting in "potential hits" referenced in the downstream case management application, as well. As most of the early financial crime detection solutions are based on rigid pattern matching rules (e.g., flagging any transaction over £5,000 and involving a suspect), only transactions breaching those rules were previously identified and reported.

With the introduction of new, innovative financial instruments, these solutions are unable to uncover the

With the introduction of new, innovative financial instruments, these solutions are unable to uncover the stratagem, allowing perpetrators to exploit these systems.

stratagem, allowing perpetrators to exploit these systems.

Additionally, the manual case investigation procedure is extremely time consuming and non-standardized, leading to inordinate delays and incorrect decisions. In

absence of a structured layer enabling smooth orchestration of atomic tasks, the entire case investigation process is left at the mercy of the knowledge level and skills possessed by the individual investigators. The manual mode of data interchange with external systems often poses a bottleneck in terms of getting the correct information at the right time. Furthermore, the lack of a holistic view of the entity leads to redundant effort or leaves fatal gaps in the investigation process with severe monetary implications. All these factors contribute to the overall process inefficiency and render the investigation process virtually ineffective. This is precisely the reason why organizations should pursue a holistic approach, through the adoption of business process management (BPM) methodologies, to ensure a well-rounded solution that provides better ROI.

BPM (business process management) is a methodology which ensures smooth end-to-end modeling, orchestration, visibility and optimization of complex business processes spanning multiple functional areas across organizational silos. BPM tools offer a proper mix of business rules and workflow orchestration to ensure best-in-class management of business processes using off the shelf features such as intelligent task routing, rule-based decision making, event-driven systemic correspondence, SLA-triggered responses, and automated report generation capabilities.

Why a Holistic Approach to Financial Crime Prevention is Important

The primary priority of financial institutions should be to truly understand and assess customers, shifting the focus from merely identifying the customer to undertake customer due diligence (CDD) to "Know Your Customers" (KYC) from an anti-money laundering (AML) and sanctions, as well as enabling perspective. Accordingly, a robust and thorough KYC process is imperative for fulfilling the objectives of both AML and sanctions financial institutions to (a) determine if the AML risk of the customer is within an acceptable threshold and (b) perform in-depth screening on prospective clients to ensure they are not sanctioned individuals or companies. To implement effective KYC procedures, financial institutions need to rapidly acquire better in-depth knowledge of their customer base (i.e., where does their customer's money come from, and what do they do with it?). This effort should be coordinated with other customer-focused initiatives in the organization to ensure any investment yields the greatest impact. For instance, enhanced KYC may overlap with efforts to obtain a single view of the customer, and ongoing CDD could complement the requirement to monitor the customer relationship. *(Please refer to Exhibit 3 on the following page).*

The next section of this white paper explores the use of BPM-enabled matured solutions as part of a holistic approach for preventing losses and mitigating risks pertaining to financial crime.

Applying Customer Due Diligence

CDD encompasses processes and practices which ensure a "single" view of the customer across the board, along with periodic sanity checks on customer data primarily from two aspects:

- Named screening of customers
- Screening of PEPs

Typically, customer attributes (Name, Country, Address, etc.) are screened against list records (provided by OFAC, PEP, Bank of England, HMT, etc.) using industry-leading filter applications such as Fircosoft or Fiserv. "Potential Hits" produced as a result of such screening are passed to the downstream BPM application for detailed investigation with additional capture of customer data through automated SLA-driven multiple KYC requests. This is where BPM plays a significant role by reducing the turn around time and elimination of redundant paper work.

Advanced BPM tools ensure comprehensive information capture through intelligent features such as "phonetic" search capabilities along with visual depiction of linked

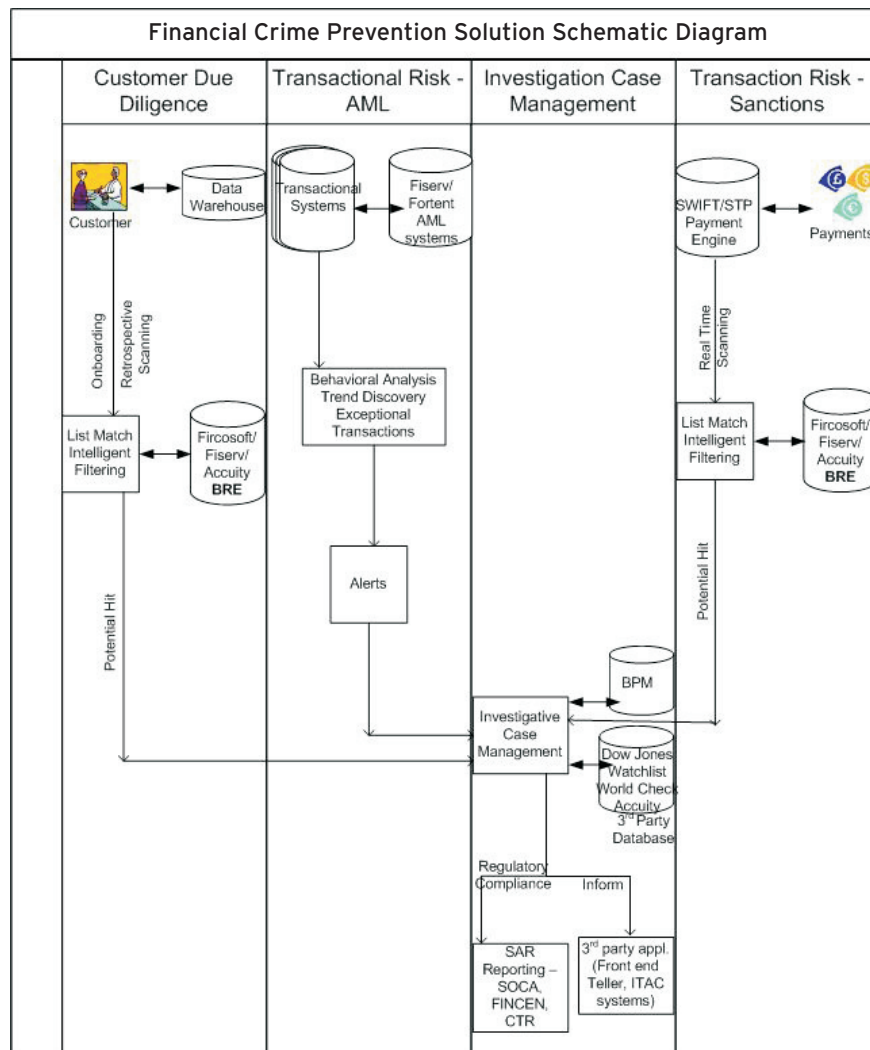


Exhibit 3

The above diagram provides a holistic view of the financial crime check workflow spanning customer screening, transaction monitoring & AML “flag” detection scenarios leading to detailed investigative case management, including automated generation of compliance reports.

relationships (account types, transactional history, related party, connected party, etc.). Additionally, to reduce the number of “false positives” it is desirable that the filter application has built-in adaptive intelligence. This is where a business rules engine (BRE), an integral part of a BPM tool, fits fills bill. A standard BRE can be used to configure complex rules to eliminate false hits based on a risk-based algorithm, thus reducing workload on the BPM application, leading to enhanced productivity. Furthermore, well-known BPM applications are usually service oriented architecture (SOA)-compliant, and hence exposing such rules as “services” will ensure cost effectiveness as well.

Sanctions Check

This involves real-time scanning of automated payment messages based on their origin as well as destination customer accounts and places (countries). Payment messages are internally managed using a payment engine

that predominantly which adheres to payment scheme guidelines and service level agreements, apart from facilitating the interfacing with accounting and charging systems. BPM tools possessing strong integration features and decision-centric capabilities (e.g., event-driven triggering of decisions based on complex business-rule intensive logic such as automatically rejecting a SEPA-DD Core Scheme Initial Collection five days ahead of the settlement date if associated case is not resolved within the delivery day) support an organization's payment system by providing an efficient and effective investigation process.

Once the customer record or the individual transaction is screened and a “Potential Hit” is recorded, the entire set of information is passed on to the case management application for thorough investigation. The case undergoes detailed scrutiny at multiple levels involving interaction with third-party data sources (e.g., World Check, Factiva, etc.) as needs dictate.

Fraud and AML Detection & Management

An effective combination of different technologies helps in proactive detection and prevention of fraudulent and anti-money laundering transactions. Industry-leading behavioral detection products like Fortent and SAS, etc. uncover potentially suspicious activities pertaining to the entity as a whole or an atomic transaction. Such an intricate level of filtering is based on scenario and threshold match involving complex statistical analysis on behavioral patterns and transaction trends using peer group analysis, variance analysis, etc. Potentially suspicious events are “red flagged” and the generated alerts are passed to downstream BPM systems for detailed investigation. BPM systems possess built-in intelligence to dig out related incidents (if any) from the fraud reporting application and automatically trigger necessary actions (e.g., a “Negative ID” flag on an investigative case is sent to the front-end Teller System to avoid any activity against the victimized customer's

Potentially suspicious events are “red flagged”, and the generated alerts are passed to downstream BPM systems for detailed investigation.

accounts; identity thefts are reported to Identity Theft Assistance Center, etc.). This kind of rule-driven, timely, automated correspondence ensures an operationally efficient and cost-effective solution.

Case Management & Regulatory Compliance Reporting

Timely and accurate intimation of fraud incidents to various regulatory agencies such as Financial Crimes Enforcement Network (FinCEN), SOCA, etc. has been the utmost priority of financial organizations, and failure to do so leads to severe penalties. Accordingly, automated and seamless report generation is one of the most important “must-have” features of any financial crime check solution.

BPM systems facilitate processing of investigation cases and the reporting of possible violations to the right regulatory authorities at the right time with the right information. On one side the built-in case management features of a BPM system enable unprecedented agility in responding to market events. (These features include automated case creation; rule-intensive, role-based access; case prioritization involving parameters such as scheme cut-off, payment type, settlement date & settlement amount; investigative research through seamless integration with third party data sources; duplicate case check; related case link-up; external correspondence and automated rule-driven accounting adjustments such as write-off/charge-off. On the other

side their strong “off the shelf” rule-driven automated report generation capabilities reduce manual effort, eliminating redundant paperwork and ensuring timely adherence to stringent regulatory norms. For example, BPM applications facilitate the generation of pre-filled SARs (Suspicious Activity Reports) through seamless integration with incident data and customer data along with providing appropriate validations to prevent unnecessary delay in SAR filing (e.g., transactions worth more than £5000 and involving a “suspect” would necessitate a SAR filing to FinCEN).

This kind of a well-rounded integrated solution comprising CDD, sanctions, fraud and AML systems coupled with BPM-enabled investigation case management and regulatory reporting systems keeps financial institutions and the economy as a whole ahead of the global threat of financial crime.

Organizational Adoption: The Softer Aspect

As always, the people factor is among the most important elements in determining the extent of success or failure of an organization-wide initiative - it's a well known fact that a solution is only as good as the way it is used.

Though leveraging financial crime prevention technology comprising effective and appropriate AML and sanction systems is crucial, breaches often happen due to staff failing to execute procedures correctly. So staff training is another preventive control measure that firms should adopt to ensure a more effective approach to financial crime. Since AML and sanctions regulation and legislation are extremely complicated, frontline staff cannot be expected to know its intricacies. Accordingly, they should be supported by such preventive systems through proper training to educate them on key principles along with a 24x7 hotline to address unresolved queries.

The Road Ahead

Industry experience suggests that the number of flagged entities (customer / transaction) post fraud detection is on a steady uptake with a decent growth rate (possibly due to sophisticated detection logic leading to enhanced coverage). Additionally, the sizes of industry standard lists such as OFAC and PEP are also growing on a regular basis due to inclusion of new entities (customer, country, and vessel). Accordingly, a huge jump is expected in the volume of requests requiring manual investigation. This would definitely necessitate the use of “best of breed” BPM tools possessing excellent routing features, business-rule enabled automated decision making capabilities and seamless external integration support.

BPM vendors are likely to offer packaged frameworks specifically targeted towards servicing the AML and fraud management domain. There is also a possibility of the enablement of backward integration from solutions provided by some of the market leaders (e.g., offering BRE features).

In fact, even BRE pure play vendors might attempt to gain a toehold in this area. Finally, advanced attributes such as graphical depiction of network relationships and Google map integration are also likely to be featured as a part of BPM offerings to facilitate and expedite case disposition, thus resulting in an optimized investigation process.

Cognizant possesses varied exposure to the financial crime check domain with substantial expertise in envisioning, conceptualizing and delivering solutions across functionalities ranging from investigative case management, anti-money laundering, fraud prevention and customer due diligence. Cognizant has helped financial institutions in U.S. and UK markets to build

¹http://news.cnet.com/8301-1009_3-10186176-83.html

About the Authors

Rakesh Banerjee is a Lead Consultant with Cognizant Technology Solutions engaged in Business Process and Strategy consulting in the Banking, Capital Markets and Insurance industry verticals. Rakesh has more than 12 years of experience in Financial Services Industry. His area of expertise has been Business Process Management, Business Rules and Analytics.

He was involved in providing consultancy to the largest UK bank in setting up their Financial Crime prevention unit's Sanctions, AML, KYC processes and satisfying FSA's compliance needs. In addition to being an Economics Graduate, he holds a Master's in Business Management specializing in Finance.

Anirban Mukherjee is a Senior BPM Consultant with Cognizant Technology Solutions and possesses close to 6 years of experience in the BPM landscape across topics such as Business Process Analysis, Vendor Evaluation & Business Case Preparation.

He has worked in the capacity of a BPM consultant in multiple engagements pertaining to AML & Fraud Prevention for major banking organizations across geographies in the UK and U.S. Anirban holds a Master's in Business Management with specialization in Finance.

About Cognizant

Cognizant (NASDAQ: CTSI) is a leading provider of information technology, consulting, and business process outsourcing services. Cognizant's single-minded passion is to dedicate our global technology and innovation know-how, our industry expertise and worldwide resources to working together with clients to make their businesses stronger. With over 50 global delivery centers and more than 68,000 employees as of September 30, 2009, we combine a unique onsite/offshore delivery model infused by a distinct culture of customer satisfaction. A member of the NASDAQ-100 Index and S&P 500 Index, Cognizant is a Forbes Global 2000 company and a member of the Fortune 1000 and is ranked among the top information technology companies in BusinessWeek's Hot Growth and Top 50 Performers listings. Visit us online at www.cognizant.com.

Notes:

For more information on how to drive your business results with Cognizant, contact us at inquiry@cognizant.com or visit our website at: www.cognizant.com.

processes to check financial crime and meet regulatory compliance in those markets. The engagements undertaken included building robust filtering processes for handling sanctions list screened transactions, customer screening, fraud detection and prevention, servicing upstream AML application and downstream compliance reporting needs.

Key Acronyms and Terms Used

- AML - Anti Money Laundering
- KYC/CDD - Know Your Customer/Customer Due Diligence
- PEP - Politically Exposed Persons
- POCA - Proceeds of Crime Act
- SOCA - Serious Organized Crime Agency
- FinCEN - Financial Crimes Enforcement Network
- OFAC - Office of Foreign Assets Control
- HMT - Her Majesty's Treasury
- FSA - Financial Services Authority
- SAR - Suspicious Activity Report



World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters

Haymarket House
28-29 Haymarket
London SW1Y 4SP UK
Phone: +44 (0) 20 7321 4888
Fax: +44 (0) 20 7321 4890
Email: infouk@cognizant.com

India Operations Headquarters

#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com