

KEY MESSAGES***Compliance remains high on banks' agendas, but banks need to focus on a risk-based approach***

Compliance and security staff are challenged by the task of ensuring that the appropriate operational processes across the entire organization are in place, and are being adhered to. The challenges continue to evolve, as does the regulatory environment in which banks operate. For example, the enormous growth in suspicious activity reports and currency transaction reports after the early 21st century wave of anti-money laundering and counter terrorist financing regulations has considerably increased the workload for both banks and regulators. In addition, many banks find it challenging to comply with the growing regulatory requirements across a wide client base, or find that their current approach does not reduce the exposure to financial crime to an acceptable level. Therefore, banks in many countries started to apply a risk-based approach to minimize their exposure to financial crime. This drives the implementation of advanced deviation detection capabilities and risk measurement techniques through the use of technology.

The evolving digital economy creates new money laundering and fraud threats

The ongoing development of the digital economy brings with it unwanted side effects. The lack of counter-measures to unintended uses of new payment methods, customer data theft and a growing cyber-crime community is resulting in an increased number of financial crime events. In order to minimize their exposure to money laundering or fraud, banks need to apply both rules-based and risk-based approaches to combat financial crime, and also strengthen security.

Banks need to focus on automation to increase the speed of processing, accuracy of detection and understanding of data

While pressure from regulatory bodies and industry associations is increasing, internal IT departments, software vendors, consultants and IT services companies are developing technologies that are helping banks to improve the level of accuracy in identifying financial crime events, increase real-time detection capabilities, and successfully manage and understand the underlying data.

Growing costs are driving increased standardization of business processes

Since the emergence of the first significant wave of financial crime detection and prevention programs, costs have far exceeded expectations. The cost is quite often spread over many different business functions, such as operations, compliance, risk and security. Therefore, banks may not be able to have a single unified view of all the associated costs related to anti-money laundering or anti-fraud activities. This also means that banks may not be able to make efficient decisions regarding how best to direct their resources to focus on the major areas at risk of financial crime. Consequently, there is a strong demand for the necessary business process enhancements and the supporting technological solutions.

Vendors should align the positioning of their solutions with their clients' main hot-spots

In order to enhance their marketing messages, vendors should focus on addressing the most important customer pain points. For many banks, the top priorities when investing in anti-money laundering and anti-fraud solutions are effective monitoring and detection capabilities, as well as strong workflow capabilities to support effective investigations.

TABLE OF CONTENTS

Overview	1
<i>Catalyst</i>	1
<i>Summary</i>	1
Key Messages	2
<i>Compliance remains high on banks' agendas, but banks need to focus on a risk-based approach</i>	2
<i>The evolving digital economy creates new money laundering and fraud threats</i>	2
<i>Banks need to focus on automation to increase the speed of processing, accuracy of detection and understanding of data</i>	2
<i>Growing costs are driving increased standardization of business processes</i>	2
<i>Vendors should align the positioning of their solutions with their clients' main hot-spots</i>	2
Market Opportunity	6
<i>Banks need to comply with the growing amount of regulatory requirements</i>	8
<i>Banks need to focus on balancing rules- and risk-based approaches</i>	10
<i>The increasing burden of operational risk management</i>	11
<i>Banks are moving from a reactive to an intelligence-based, proactive approach</i>	11
Evolution of the Anti-Financial Crime Discipline	13
<i>The evolving digital economy creates new money laundering and fraud threats</i>	13
<i>Banks need to focus on automation to reduce error and increase deviation detection levels</i>	16
<i>Growing costs are driving increased standardization of business processes</i>	19
Technology and Vendor Landscape	21
<i>The sophistication of back and middle office technology is growing</i>	22
<i>Front office monitoring solutions have proliferated in response to demand</i>	25
<i>The market is still fragmented due to its immaturity</i>	27
<i>User-friendly AML and anti-fraud management tools increase workflow efficiency</i>	28
<i>Real-time detection capability enhances successful prevention</i>	29
<i>An increasingly cost-driven market drives adoption of a hosted delivery model</i>	30
Go to Market	32
<i>Vendors should align the positioning of their solutions with their clients' main hot-spots</i>	32
<i>Banks are seeking end-to-end solutions across financial crime types and investigation chains</i>	33
<i>MISs are forecast as one of the fastest growing areas of technology expenditure</i>	33
APPENDIX	35

Table of Contents



<i>Definitions</i>	35
<i>Methodology</i>	36
<i>Further reading</i>	36
<i>Ask the analyst</i>	37
<i>Datamonitor consulting</i>	37
<i>Disclaimer</i>	37

TABLE OF FIGURES

Figure 1:	<i>Which three financial crimes do you consider the highest priority to address?</i>	6
Figure 2:	<i>Rules-based approach vs. risk-based approach</i>	8
Figure 3:	<i>Evolution of financial crime detection and prevention management</i>	12
Figure 4:	<i>Which areas of regulatory compliance will be driving IT project spending in 2009?</i>	17
Figure 5:	<i>Worldwide monitoring and management of risk and compliance key figures</i>	20
Figure 6:	<i>Overall AML and anti-fraud technology architecture</i>	21
Figure 7:	<i>Analysis of payment flows</i>	23
Figure 8:	<i>The anti-financial crime vendor offering landscape</i>	28
Figure 9:	<i>Graphical user interface – example of a fraud analyst dashboard</i>	29
Figure 10:	<i>Please rate the importance of the following objectives to your IT investment strategy in 2009</i>	31
Figure 11:	<i>What are your organization's top three priorities when investing in anti-money laundering (AML) and anti-fraud solutions? (Rank top three in order of priority)</i>	32
Figure 12:	<i>Retail banking technology spending by business function globally</i>	34

TABLE OF TABLES

Table 1:	<i>Regulatory drivers – major implications</i>	9
Table 2:	<i>Major industry associations or government agencies</i>	10
Table 3:	<i>New payment methods - money laundering and terrorist financing risks</i>	14

MARKET OPPORTUNITY

Introduction

Money laundering has become a major issue across many industries in recent years. Financial services institutions (FSIs) have been both knowing and unknowing participants in money laundering activities. Banks have been major targets of laundering operations as they provide a variety of services and products, such as traveler’s checks and wire transfers, which can be used to conceal the source of illegal income. Likewise, criminals use the part of the financial services ecosystem that is less regulated than the banking sector to hide or disguise the origins of funds derived from illegal activity. For example, they use person-to-person payments, money transfers, or other services in order to exploit their loopholes and weaknesses. Furthermore, as a result of increased terrorist financing activity, especially related to the 9/11 terrorist attacks, a new wave of regulatory strengthening went through the financial services sector, imposing significant pressure on banks and their business processes. Due to the regulations, banks went from assisting authorities in dealing with money laundering and terrorist financing, to the stage where the onus to stop financial crime is now on the banks. As shown in Figure 1 below, money laundering is the financial crime most banks regard as the highest priority to address.



Another significant area of financial crime is related to alarming fraud statistics. Banking customers would like to know how safe their deposits, and debit or credit cards are, as well as other banking products and services. In addition, regulators question how customer data is being protected by retail banks, wealth managers and/or card providers, and more

importantly, what the institutions are doing to fight criminals. While retail finance institutions are concerned with the possible damage to their reputations, the monetary losses that the industry currently incurs due to fraudulent transactions or security breaches tend to be low enough for banks to swallow, making banks reluctant to invest in costly anti-fraud solutions.

Banks need to exploit the synergies between anti-fraud and anti-money laundering

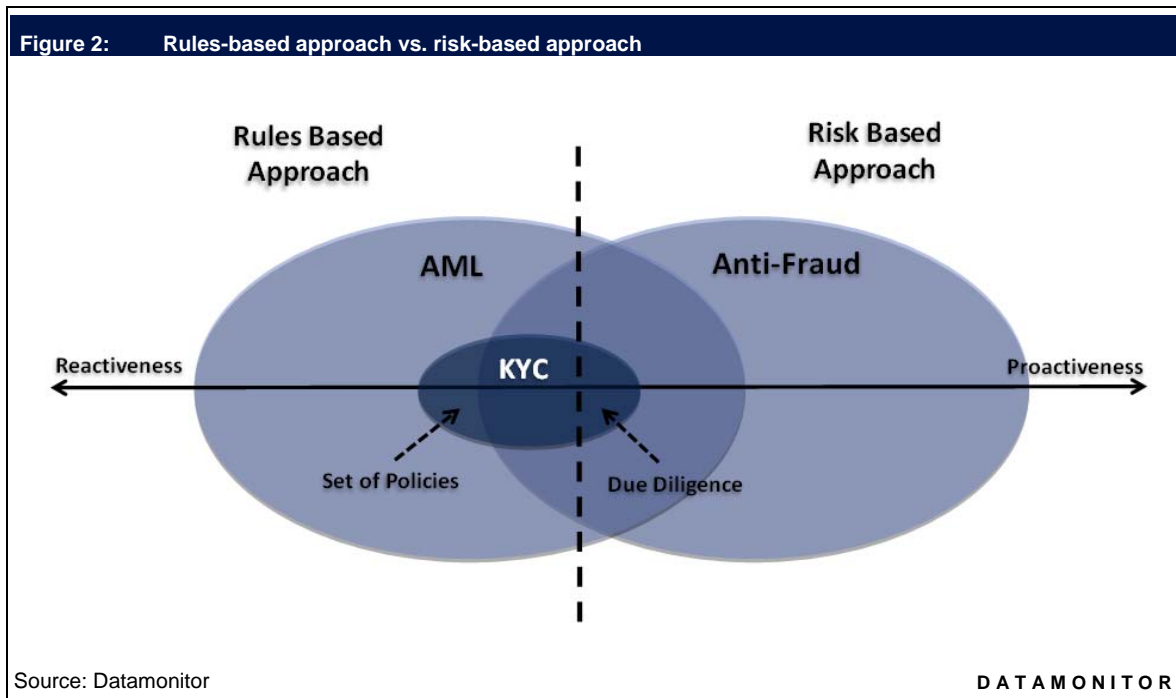
While FSIs have a number of issues they need to deal with in the area of anti-money laundering, anti-fraud and also security, these issues are typically handled by separate departments. In a larger institution these issues can be handled by separate departments for every individual line of business (e.g. retail to corporate banking, brokerage, card processing, etc). All these different business lines tend to have their anti-fraud and anti-money laundering units. However, as the financial crime sector is growing, there is anecdotal evidence that increasing numbers of banks are combining their compliance, fraud, and security departments into one single unit to take care of similar risk areas. Datamonitor expects that this approach will result in an emerging trend of standardizing business processes and technologies to create an enterprise-wide view of compliance and fraud risk within an institution or across business lines, which can be viewed on management dashboards to keep track of various risks across the enterprise. This report will highlight potentially significant synergies between anti-fraud and anti-money laundering in areas such as compliance or risk management.

Banks needs to address three major areas to combat financial crime

Below are the major areas of concern that retail banks, online brokers, private banks, card processors and insurance providers need to develop further, in order to successfully combat the increasing threat of financial crime.

Anti-money laundering (AML) – this term describes the legal controls that require FSIs to prevent and/or report suspicious activity. The AML guidelines became especially important after the 9/11 terrorist attacks, which resulted in the enactment of the USA PATRIOT Act. The new law has made a number of changes to existing US law; the key acts changed were the Foreign Surveillance Act of 1978, the Electronic Communications Privacy Act of 1986, the Money Laundering Control Act of 1986, the Immigration and Nationality Act, and the Bank Secrecy Act. The European Union followed in December 2007 with its Third Money Laundering Directive (an enhancement and update of the content of the First and Second EU Directives on the prevention of money laundering; it should be noted that these Directives cover all countries in the European Economic Area). Nowadays, most of the banks are required to monitor, examine and report suspicious transactions (by filing a Suspicious Activity Report (SAR) or a Currency Transaction Report (CTR)) to the anti-money laundering unit of the central bank in their respective country.

Know your customer (KYC) – due to AML regulations or internal risk mitigation strategies, FSIs have to perform due diligence by having proof of a customer's identity and that the use, source and destination of funds do not involve money laundering. KYC is a set of policies (due diligence and banking regulations) that banks need to comply with while identifying their clients and ascertaining relevant information pertinent to offering financial services or products to them. KYC comprises the rules-based based approach (regulations) and the risk-based approach (risk management). The visual representation of these approaches is shown in Figure 2 below. Know Your Customer policies have become increasingly important on a global scale, in an effort to prevent identity theft fraud, money laundering and terrorist financing.



Fraud detection and prevention – this is a set of rules and techniques that detect and prevent a known execution of, or “an attempt to execute, a scheme or artifice to defraud a financial institution or to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises” (Title 18 U.S. Code § 1344; the Bank Fraud Statute). Fraud detection, prevention and investigation procedures address both internal (employee) and external fraud.

Banks need to comply with the growing amount of regulatory requirements

The compliance burden is an increasing challenge for many retail banks, retail brokers, card processors, private banks and insurance providers. Banking compliance officers or senior executives have to ensure that the appropriate operational processes across a complex financial business are in place, and are being adhered to. However, the challenges faced by banks will continue to evolve, as will the regulatory ecosystems in which they operate. The table below presents the major regulations and guidelines that affect the financial services industry today.

Table 1: Regulatory drivers – major implications		
Major regulations and guidelines	Main implications	Geographical scope
EU Third Money Laundering Directive	The introduction of measures to combat money laundering and terrorist financing across the member states. The directive also requires that senior management approval is required for certain AML/KYC-related tasks, such as the establishment of corresponding banking relationships and the acceptance of customers that are classified as 'high risk'.	European Union (directly), and Global (indirectly)
The USA PATRIOT Act	The Act contains specific legislation that requires banks to put AML/KYC programs into place, such as the development of internal policies, procedures and controls, the designation of a compliance officer, an ongoing employee training program, and an independent audit function to test the program.	The United States of America and consequently banks doing business with American banks (especially the rest of the Americas)
FFIEC's authentication guidance	Banks are being forced to introduce multifactor authentication into their online banking channels, thus rendering internet banking less susceptible to fraud attempts	The United States of America
Identity Theft Red Flags Rule	FSIs must include now practical policies and procedures for detecting, preventing and mitigating identity theft and enable the FSI to identify relevant patterns, practices, and specific forms of activity that are 'red flags' signaling possible identity theft and incorporate those red flags into the FSI's program.	The United States of America

Source: Datamonitor DATAMONITOR

In order to successfully fight money launderers and fraudsters, it is important that there is a joined-up approach between the banking industry and government agencies. While banks are developing their own intelligence in relation to suspicious activities, individuals and entities, the regulatory focus has now shifted towards better cooperation and intelligence-sharing between the private and public sectors. Banks need to focus not only on improving the effectiveness of AML efforts, but they also need to tackle terrorist financing and ensure that customer data is well protected. As many regulators have recognized the need for anti-financial-crime intelligence sharing, they have placed a strong emphasis on working with the industry to improve understanding of financial crime issues and regulatory requirements and expectations. To date, sharing efforts have not succeeded everywhere, and many countries have not trained police forces or other special units to deal with high-tech crime effectively. Nonetheless, the network includes industry associations (listed in Table 2 below) and formal working parties and committees.

Industry associations or government agencies	Purpose	Web site	Geography
The Financial Action Task Force (and FATF-style regional bodies)	Development and promotion of national and international policies to combat money laundering and terrorist financing.	www.fatf-gafi.org	Global
The Egmont Group of Financial Intelligence Units	Improvement of interaction among financial intelligence units (FIUs) in the areas of communications, information sharing, and training coordination.	www.egmontgroup.org	Global
United Nations Global Programme Against Money Laundering	Provision of anti-money laundering (AML) training and technical assistance and, since 9-11, counter-terrorist financing (CTF) training and technical assistance.	www.unodc.org/unodc/en/money-laundering/index.html	Global
The Financial Crimes Enforcement Network	Enhancement of U.S. national security, deterrence and detection of criminal activity, and protection of financial systems from abuse by promoting transparency in the U.S. and international financial systems.	www.fincen.gov	The United States of America
The Federal Financial Institutions Examination Council	Prescription of uniform principles, standards, and report forms for the federal examination of financial institutions by the US government branches, and to make recommendations to promote uniformity in the supervision of financial institutions.	www.ffiec.gov	The United States of America
The Joint Money Laundering Steering Group	Promulgation of good practices in countering money laundering and offering practical assistance in interpreting the UK Money Laundering Regulations.	www.jmlsg.org.uk	The United Kingdom
The Serious Organised Crime Agency	Reduction of damage caused to people and communities by serious organised crime.	www.soca.gov.uk	The United Kingdom

Source: Datamonitor DATAMONITOR

The financial services sector is evolving to using a more advanced approach to deal with the issue of money laundering, terrorist financing and wider financial crimes. This approach combines cooperation and feedback between various branches of government and government agencies, and the financial services industry. Moreover, there is anecdotal evidence that banks (especially the larger entities) are increasingly combining their compliance departments with anti-fraud units and security divisions into a comprehensive single unit. This cooperation and convergence implies standardized approaches to operational processes, and in some cases standardized technologies, to deal with the increasingly broad scope of different types of financial crime. For example, a similar transaction monitoring system can be used for both fraud detection and money laundering, and similar principles can be applied to staff training.

Banks need to focus on balancing rules- and risk-based approaches

The difficulty of handling the implications of the rules-based approach has resulted in the adoption of a risk-based approach. This is due to the fact that the enormous growth in suspicious activity reports (SARs) and currency transaction reports (CTRs) after the early 21st century wave of anti-money laundering and counter terrorist financing regulations has caused a lot of pain for both banks and regulators. With both banks and regulators starting to realize that quantity is not the same as quality, the focus has shifted on risk mitigation strategies. They imply that banks should allocate their AML/anti-fraud resources according to an assessment of the level and type of financial crime to which they are at risk of exposure. This approach is quite often used during account opening, retrospective account remediation (the correcting and updating of existing customer identification files), or ongoing account monitoring. The requirement to know your customer

strengthens efforts to counter money laundering, terrorist financing, and fraud, and quite often is a legal requirement in many markets. When a bank approves a new client, it provides the client with an access point to that bank both domestically and internationally. Therefore, it is critical that the bank understands each client's status and financial situation and knows with whom it is dealing. Many banks find it logistically challenging to apply their existing approaches across a wide client base, or find their current solutions do not meet expectations. Therefore, the regulatory focus in many countries has been moving toward encouraging FSIs to apply a risk-based approach to KYC. This also means that a bank may choose a different approach or different risk level while identifying prospects depending on line of business, product or a customer group.

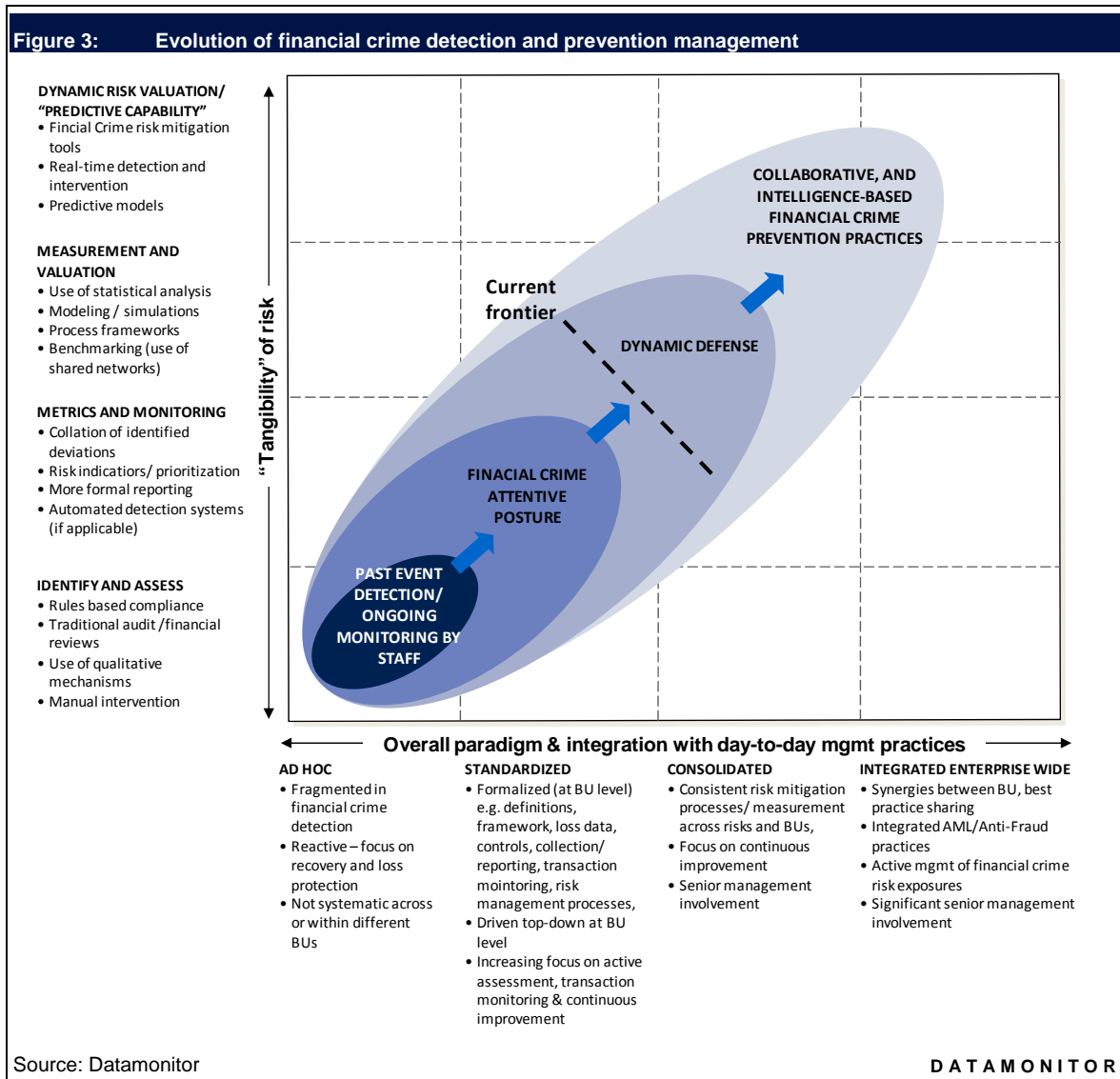
The increasing burden of operational risk management

The enhanced screening process at account opening is just one step towards complying with the law and reducing financial losses related to criminal activities. The types of suspicious activity today are many and varied. Financial crime is no longer simply about the laundering or theft of money, it is about high profile issues such as customer data theft, financial misreporting, and many others. The current economic crisis further exacerbates the situation. The extremely severe conditions within the financial services industry, with many banks teetering on the brink, will only give rise to additional unethical behaviors. They could increase the risk of potential internal fraud as well as possibly increase suspicious behavior originating from outside of the institution. Furthermore, cost-cutting pressures may affect AML/anti-fraud departments, among others. Some banks have already announced budget and staff reductions. As a result, reduced vigilance may open new windows of opportunity for money launderers and fraudsters. The economic downturn may result in the industry seeing a new wave of financial mis-statements, account manipulations or internal fraud, as employees try to preserve their jobs and lifestyles.

While the potential financial loss arising from financial crime is a significant element to banks, many institutions recognize the negative impact on their reputations as well. This is due to the fact that in recent years bank security failures have become fodder for the media in many markets, leading to widespread distrust of the industry as a whole. Vendors who provide security technology quite often position the idea that this apprehension towards the industry could potentially translate into a competitive advantage for those banks that are reputed, rightly or wrongly, to have stronger levels of financial crime prevention. So far, clients have not stopped using online banking in any significant numbers, in spite of all of the scare stories.

Banks are moving from a reactive to an intelligence-based, proactive approach

While analyzing the development of the AML and anti-fraud areas, Datamonitor expects the field to continue to mature in terms of deviation detection capabilities, risk measurements techniques, integration of compliance and security categories, advanced software use, and the assimilation of a stronger financial crime awareness culture in all parts of the organization. AML and anti-fraud are expected to develop as considerable disciplines, just as market and financial crime have evolved. Figure 3 below illustrates Datamonitor's view of the evolution of financial crime capabilities and practices.



The growing adoption of a risk-based approach to counter financial crime issues drives the implementation of advanced deviation detection capabilities and risk measurement techniques through the use of technology. The major benefit is automation. This also enables banks to move from a reactive to a more proactive approach by focusing human resources to deal with the highest risk cases. Datamonitor believes that most participants in the financial services market are progressing from the second (Financial Crime Attentive Posture) to the third phase (Dynamic Defense). Given the efficiency pressures in financial crime management initiatives towards the post-credit crisis banking environment, we expect many institutions to adopt a more incremental approach to the development of AML/anti-fraud risk capabilities in the next phase

EVOLUTION OF THE ANTI-FINANCIAL CRIME DISCIPLINE

The chapter describes the most important factors, in Datamonitor's view, that currently influence the evolution of anti-money laundering, and fraud detection and prevention areas. A number of emerging threats, business process and technology blending, and increasing cost pressures shape the development trajectory of the anti-financial crime discipline.

The evolving digital economy creates new money laundering and fraud threats

Datamonitor has identified a number of potential threats that may increasingly contribute to the growth of financial crime events. The criminal exploitation of new payment methods, customer data theft and epicenters of cyber-crime such as Central and Eastern Europe, as well as Central Africa, are potentially the greatest emerging threats to the financial sector.

Unregulated 'virtual world' transactions are an emerging challenge to combating financial crime

While law enforcement struggles with the many low-tech but typically extremely effective ways in which criminals launder money or finance terrorism, we are at the same time witnessing a plethora of new, high-tech value transfer systems that can be abused. These are some of the most innovative electronic payment products that use the internet, wireless devices, and even well-established payment networks, classified as 'new payment methods' (NPMs). The move away from paper payments to standardized electronic transaction processing has had the effect of breaking down the payment system into distinct business segments. This particular segmentation has led to the entry of non-banks as both outsourced service providers to the banking industry and occasionally competitors in the clearing services segment. The proliferation of electronic processing technologies has enabled non-bank service providers to customize their payment instruments and package them with complementary products in order to serve niche markets. As a result, a number of new services and products are now available, such as internet payment services, prepaid cards, mobile payments, and digital precious metals.

The potential financial crime risks that these new payment methods are posing may vary from one product or service provider to another, especially if there is no applicable anti-financial crime regulation that establishes a uniform standard. Table 3 below presents the major potential risk factors and current and potential risk mitigants that are associated with a selection of new payment methods. These risk factors may be common across many types of NPMs in a single jurisdiction. However, in some cases the service providers are located in an offshore financial center and therefore subject to a less sophisticated system of laws and regulations. In order to minimize exposure to money laundering or terrorist financing, the FSIs need to apply both rules-based and risk-based approaches to combat financial crime. While the institutions need to apply the applicable risk mitigations laws, regulations, and industry rules and practices, they also need to build their risk models to take into consideration the potential risk factors discussed above. Consequently, technology providers will find the opportunity to address the growing area of a risk-based approach to anti-money laundering and counter terrorist financing (CTF), and offer the functionality to banks and other financial services providers.

Table 3: New payment methods - money laundering and terrorist financing risks		
Payment method	Potential risk factors	Current and potential risk mitigants
Internet payment systems (payment services provided by non-bank institutions operating exclusively on the Internet and that are only indirectly associated with a bank account)	<ul style="list-style-type: none"> • Anonymous accounts • Anonymous funding and receipt of funds (ATMs) • High or nonexistent account funding limit • Offshore service providers may not observe laws in all jurisdictions 	<ul style="list-style-type: none"> • Identify account holder • Maintain transaction record identifying payer and recipient • Monitor transactions and report suspicious activity • Limit funding options • Implement account block • Limit access to the service
Prepaid cards (provide access to monetary funds that are paid in advance by the cardholder)	<ul style="list-style-type: none"> • Anonymous card holder • Anonymous funding (inflow) and anonymous access to funds (outflow) • High card value limit and/or no limit on the number of cards an individual can acquire • Access to cash globally through ATMs • Offshore issuers may not observe laws in all jurisdictions 	<ul style="list-style-type: none"> • Verify cardholder identification • Limit funding options • Limit card value and/or the number of cards that an individual can acquire and/or value per transaction • Limit cross-border access to cash • Monitor transactions and report suspicious activity • Implement a card/account block • Limit access to network by undesirable merchants and ATM providers/networks
Mobile payments (the use of mobile phones and other wireless communications devices to pay for goods and services)	<ul style="list-style-type: none"> • Anonymous accounts • Anonymous funding and receipt of funds • High or nonexistent account funding limit 	<ul style="list-style-type: none"> • Account holders are identified when phones are used as an access device to a bank or credit card account or when the telecom verifies phone owner identification • Limited cross-border functionality • Limited account and transaction value • Limit funding options • Monitor transactions and report suspicious activity • Implement a card/account block • Limit access to network
Digital precious metals (a relatively new online system that involves the exchange of options or the right to purchase an amount of precious metals at a specific price)	<ul style="list-style-type: none"> • Anonymous accounts • Anonymous funding and receipt of funds • High or nonexistent account funding limit • Offshore service providers may not observe laws in all jurisdictions 	<ul style="list-style-type: none"> • Identify account holder • Maintain transaction record with payer and recipient • Monitor transactions and report suspicious activity • Limit funding options • Implement account block • Limit access to service

Source: FATF

DATAMONITOR

Customer data theft is an increasingly painful issue, due to the potential implications of ID theft

Theft of customer data has become a high-profile security issue, particularly for FSIs that store and manage large quantities of sensitive customer data. The loss of personal data could weaken customer confidence and retention levels due to bad publicity. However, it can also be financially costly, especially in a situation when a FSI can be held responsible for the security breaches and sensitive customer data losses, which could lead to high fines and litigation. The current wave of regulations, originated in western economies, is spreading over many jurisdictions, and is only contributing to potentially greater financial losses in case of a lack of compliance. For example, the state of California adopted The Security Breach Information Act in 2003, and by the end of 2007, 38 states have followed. Some other countries, such as Canada and New Zealand, also adopted a similar law.

Typically, the primary reason for data breaches that lead to identity theft and potential further financial loss is the theft or loss of a computer (hard drive) or other medium used for data storage or transmission such as a USB drive or a back-up storage device. It is also worth mentioning that there are different risk levels associated with various media used for data

storage or transport. For example, a loss of a tape is potentially less risky than a loss of a CD, because of the software and hardware required to read the tape. In addition, a data breach can be caused by an insecure policy if it can be attributed to a failure to develop, implement, or comply with adequate security policies. Hacking is another technique to steal customer identities from large data centers. It is more purpose-driven than simply exploiting the lack of a secure policy, as it is an intentional act with a defined purpose of stealing data which can be used for fraudulent purposes. In addition, public awareness of data breaches is increasing, as media outlets happily are quick to report the loss of storage devices with sensitive customer information, or hacking incidents.

However, aside from the general media noise, the cyber-crime economy is growing. Once sensitive customer data is stolen, it can be sold on the underground economy's Internet servers. These are black market forums used by criminal organizations to advertise and trade stolen information or services, usually used in identity theft. The portfolio of information that can be acquired by a fraudster is getting broader and broader. The "cyber-crime supermarkets" already sell government-issued identification records, credit/debit card numbers, login data for bank accounts, or other types of information.

The exchange of information on offer can be facilitated by the new payment methods mentioned earlier, for example, by using a person-to-person transfer service that does not require the verification of identity in order to execute a transaction. The illegally obtained information can be used to commit further crimes such as:

- **Account takeover** – occurs when a fraudster acquires a victim's existing account information and purchases products or services using the stolen records.
- **Application fraud** – occurs when a fraudster uses a victim's identifying information to open a new account in the victim's name. Victims are not likely to learn of application fraud for some time, as the monthly statements are mailed to an address used by the imposter.

The threat is increasingly growing, although it was noticed a long time ago and some prevention programs have already been established. FSIs, in order to protect their customer base and themselves, need to take more secure measures to verify and authenticate users. A number of regulatory bodies or industry associations are working on appropriate regulations and guidelines. For example, the Federal Financial Institutions Examination Council (FFIEC) in the US requires banks to upgrade to a multi-factor authentication system for online banking. In addition, security features such as the use of one-time passwords can make it more difficult for fraudsters to gain access to and exploit stolen customer information.

New windows of opportunity are opening for fraudsters during the current financial turmoil

In the bricks-and-mortar economy, the correlation between the economic downturn and crime levels is quite high. Unfortunately, the same rule applies to the digital version of the economy that we all live in. During the current financial turmoil, the numbers of financial crime activity (especially cyber-crime) are growing exponentially. The cost reduction pressures throughout the financial services industry are felt also in compliance and security departments. In principle, the security area is typically recession-proof, meaning that the cutting of budgets for anti-crime related activities is one of the last ideas that banking executives would be willing to execute. However, cost reduction and efficiency pressures also mean that compliance officers and fraud experts may not be given the extra resources needed to fight an increasing number of financial crime issues. These issues are potentially escalated by the growing number of newly unemployed skilled

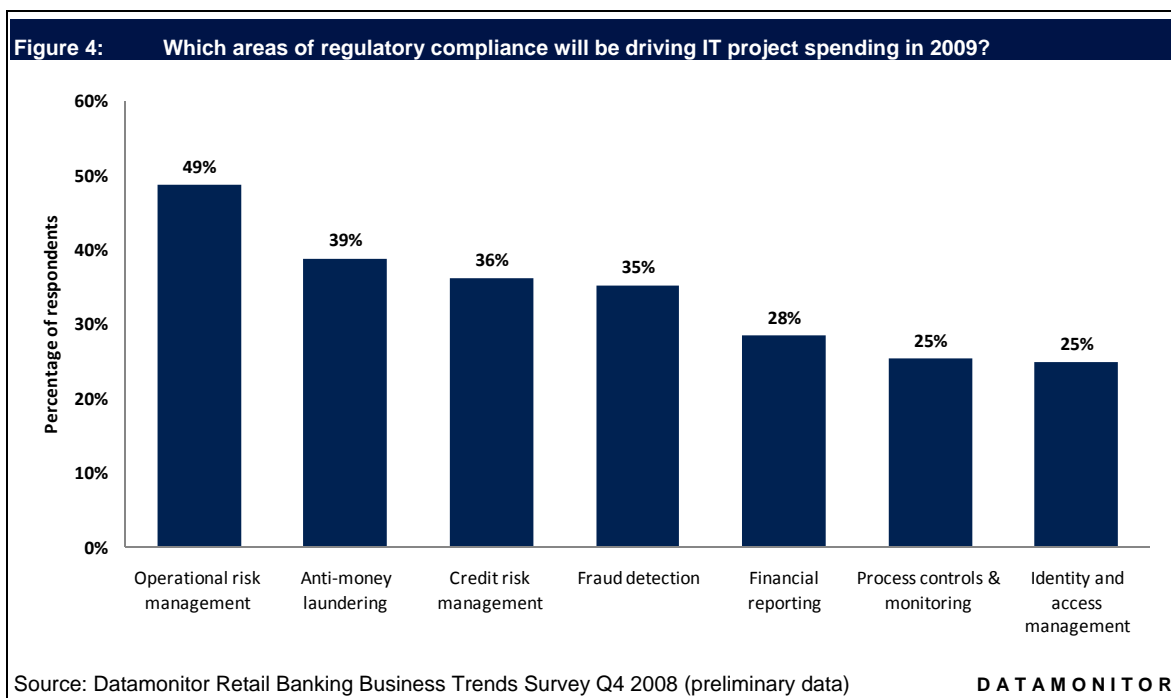
technology workers (quite often from the financial services sector), who are finding ways to exploit their skills in the underground economy. These former IT employees, with their abilities to steal sensitive data or commit fraud along with specific knowledge of their former employer's IT systems, could become a growing threat. Moreover, fraudsters are finding a variety of smart ways to surprise confused customers of banks who are suffering in these turbulent times. For example, security companies are tracking "phishing" emails following practically every rumor of a bank merger or collapse, impersonating official bank statements and asking users to "verify your account details".

Central and Eastern Europe and Central Africa have become epicenters of cyber-crime

The financial crisis, which originated in the US market due to sub-prime lending practices, has spread to other markets. Many other economies were infected, in both developed and emerging markets. It will likely drive more IT employees into the Central and Eastern European or the Central African cyber-crime communities. This will happen due to the increasing number of laid-off employees entering the underground economy or simply because of the potentially significant increase in compensation levels. Local governments, such as in Romania and Nigeria, have been reporting that a number of well-skilled engineers are migrating from legitimate computer work to the underground cyber communities. These are quite often very talented IT workers, who may be looking for employment opportunities or simply being lured by higher earnings, and the ambition to be an important personality in the underground economy rather than simply back office IT staff in a large western corporation.

Banks need to focus on automation to reduce error and increase deviation detection levels

In the global retail banking industry, technology expenditure on regulatory compliance will be primarily driven by operational risk management, fraud detection, and anti-money laundering areas. Figure 4 below represents the results of a survey, conducted by Datamonitor in the fourth quarter of 2008, of 194 IT decision makers from retail banks worldwide. The outcome proves that the areas of risk mitigation and anti-financial crime are high on CIOs' agendas, due to strong regulatory and government attention, which forced banks to make investments to deal with increasing requirements. While the use of technology has become prevalent across many jurisdictions, tight deadlines often force banks to implement the quickest solutions. These are often single point solutions that meet the most necessary, rather than optimum, requirements for dealing with the medium to long-term challenges of mitigating risks and fighting financial crime, or obtaining synergies of unifying compliance and security processes and underlying technologies. The first wave of investments into automated monitoring systems resulted in many cases where more resources were required for ongoing maintenance costs or to fully implement the more complex systems.



Banks need to improve the accuracy of identifying financial crime events

While pressure from regulatory bodies and industry associations is increasing, internal IT departments, software vendors, consultants and IT services companies are developing technologies that are helping banks to improve anomaly detection. Technology vendors bring to the table automated intelligence to examine suspicious behavior across transactions, so that the output can be leveraged to detect money laundering or fraudulent activities. To date, transaction monitoring is the area of highest expenditure among all of the anti-financial crime technology components.

However, the early implementation of newly developed anti-financial crime systems has not always met expectations. Many banks have realized that significant resources are still required for the continual updating of monitoring solutions, data feeds for transactions, and ongoing reviews of the exceptions and potentially suspicious transactions identified by the system. Vendors, consultants, or internal compliance or anti-fraud experts have found it quite difficult to develop sufficiently accurate typologies for identifying fraud, money laundering or terrorist financing, and adjust the number of flagged-up cases for further manual intervention to a number with which banks are comfortable. The issue still remains unsolved in many banks. This is quite often due to the fact that many of the earlier systems contain complex mathematical algorithms that make it difficult to comprehend intuitively the inter-relationships between the information fed into the systems and the output. Regardless of the issues related to the implementation of immature solutions, many institutions are entering the stage of re-engineering (and in extreme cases, replacing) the existing platforms. Typically, this is happening through a focus on refining the risk engines in order to achieve better accuracy and a more efficient management of workflow.

Real time detection is an increasingly urgent requirement

Unfortunately for banks and their clients, criminals aim to identify emerging patterns and are driven by exploiting the imperfection of mainstream solutions. Security and its circumvention have been, and always will be, a 'cat-and-mouse' game. Real-time money laundering and fraud detection solutions can be applied as they can flag apparent suspicious activity at the time of execution. The attractiveness of such functionality is increasing, as banks are moving toward straight through processing (STP). In addition, as customer sophistication is growing, users are demanding the ability to use their cards in shops and ATMs, and access online banking accounts around the world. Banks are looking for solutions that are able to detect whether such activity is likely to be genuine or fraudulent in real-time, and the potential for implementing such solutions is increasing.

Banks need to focus on data management to improve their ability to detect anomalies

Regulators expect banks to capture, validate, maintain, and control access to the right data regarding their customers, as this enables institutions to verify a customer's identity prior to a new account opening. Consequently, customer due diligence and related banking regulations are becoming a significant driver for data management activities, particularly in the anti-financial crime area. Institutions providing any kind of banking services need to make fundamental enhancements to the way they manage data, strengthen internal procedures, and put systems in place to prove that they are in control and complying with the law. In addition, banks need to capture and retain correct client data and full transaction details that can be reviewed on request, along with copies of related proof to validate the adherence to applicable laws and regulations. The KYC technology element is responsible for the provision of a comprehensive view of disparate data. While the amount of data is growing, technology is taking control over issues such as:

- data capture;
- data quality;
- data accuracy;
- data retention;
- information accountability.

Therefore, the functionality ideally fulfills the requirements to verify compliance and identify risk-susceptible identities.

While the accuracy of detecting deviations and anomalies is increasing, it will still not be possible to successfully achieve implementation of financial crime prevention solutions without solid data management. Today's FSIs are collecting and storing a mind-boggling quantity of data, and the size of some banks' databases is approaching petabytes. In response to this growing amount of data, technology vendors offer to improve banks' storage capabilities and associated technologies. Today, many organizations still struggle to manage and efficiently analyze their data. Preparing an organization's data structure to support anti-money laundering or anti-fraud activities necessitates an enormous effort to integrate disparate data sources and accurately manage metadata. However, loading the data into real-time data warehouses or all-in-memory databases may become an expensive exercise. Whether banks are able to increase their accuracy or not is typically based on how successful banks are with executing their data management strategy.

Banks need to understand customer data to successfully implement their compliance and risk strategies

As the financial incentive is high, the criminal community is developing very fast. Business-related risk mitigation pressures are typically ahead of legislation. It is becoming imperative that risk-based monitoring for unusual or suspicious activity is based on an understanding of the underlying data that represents the normal activity for an individual or entity. FSIs historically have not held much information on long-standing customers, due the fact that regulatory requirements related to customer identity increased after an account was opened. Therefore, the situation resulted in the increased risk of assessing existing customers whose relationship with a given institution pre-dates the introduction of current KYC policies. As a result, many banks have decided (and some are obligated by law) to implement functionality that allows retrospective remediation to fill in gaps in their KYC data.

There are many options which banks may pursue. The North American banks have focused more on transaction 'look-backs', while their European counterparts have focused on remediating KYC information. Transaction 'look-backs' typically require an institution to review historical transactional data using scenarios or parameters negotiated and agreed upon with the relevant regulator. While many banks have decided to implement solutions that allow remediation, several have underestimated the complexity, time taken and cost of such projects. There are still potential cost savings and operational synergies for the banks that are able to implement KYC policies successfully. The technological know-how delivered by internal IT departments, technology consultants or software vendors will be critical to achieve the required level of compliance and minimize risks.

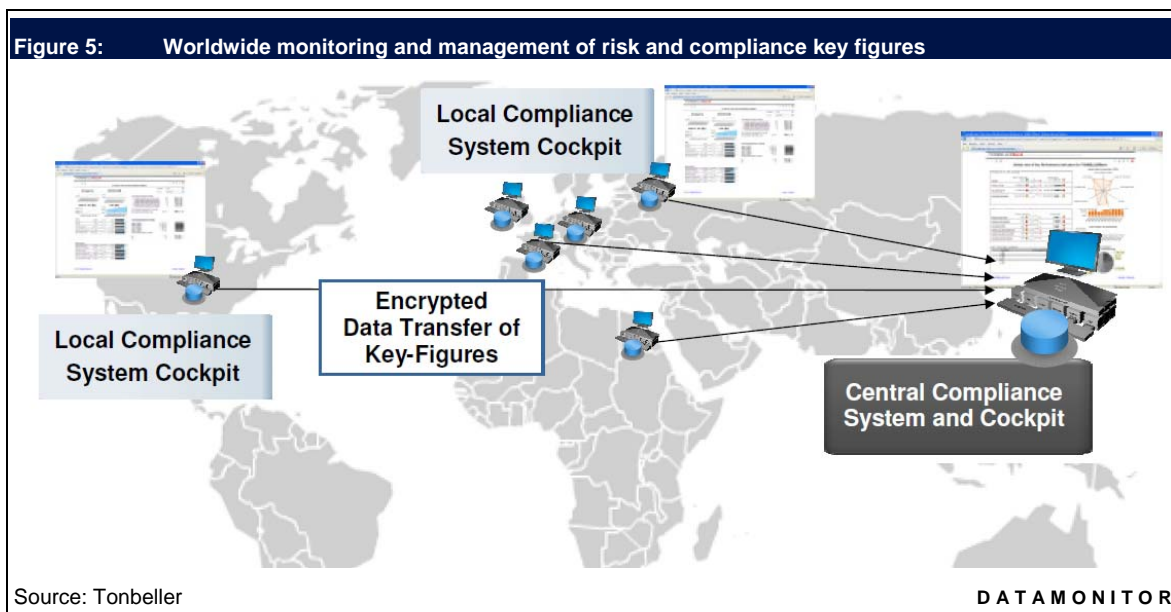
Growing costs are driving increased standardization of business processes

Since the emergence of the first significant wave of financial crime detection and prevention programs, costs have far exceeded expectations. Growing regulatory pressures resulted in a strong demand for the necessary business process enhancements and the supporting technological solutions. Apart from the technology expenditure, the total cost of experienced technical and non-technical compliance and anti-fraud experts has significantly increased in the past several years. This is mostly due to the fact that the number of compliance/security personnel has increased significantly in the past several years.

The cost is quite often spread over many different business functions, such as operations, compliance, risk and security. It may also overlap with processes that are embedded in regular business practices, such as payment processing or credit risk analysis. In addition, the cost can also be spread over many locations domestically or internationally, especially in the case of larger institutions. All these factors together mean that banks may not be able to have a single unified view of all the associated costs related to anti-money laundering or anti-fraud activities. This also means that banks may not be able to make efficient decisions regarding how best to direct their resources to focus on the major areas at risk of financial crime. As a result, there is a growing opportunity for business and technology consultants or vendors that are able to improve a bank's understanding of the full range of anti-financial crime related processes that exist across the entire organization, and further implement all the necessary enhancements to the existing process.

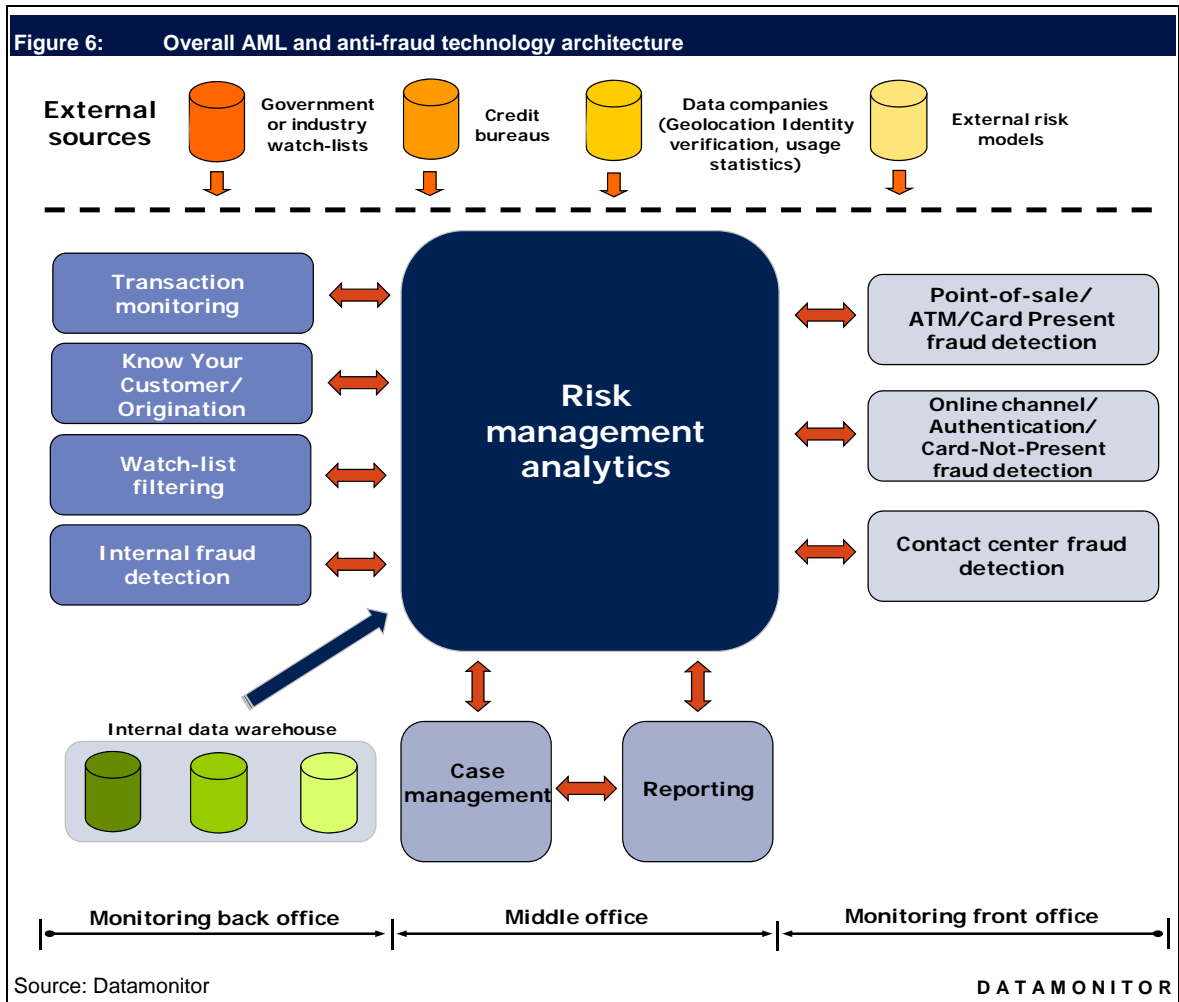
Banks need to balance accountability for risk and low-cost sourcing alternatives

While banks are enhancing their cost analysis capabilities and the understanding of the drivers behind higher expenditure, the use of outsourcing or off-shoring remains an issue. Many banks have been unwilling so far to consider moving compliance and security functions off-shore or to a third party. This is primarily due to legitimate concerns among banks about the potential loss of control and the complexity of the exercise due to the lack of a standardized approach, as a wide range of different functions are now included in compliance and security processes. Overall, banks have had more success where they moved compliance and security functions along with accompanying operational processes, rather than the functions in isolation. Nonetheless, the banks that moved into the outsourcing/off-shoring mode still retain the responsibility for financial crime risks, regardless of the sourcing strategy. In addition, many banks (especially the larger entities) are trying to move toward a central and unified management structure in order to standardize many diverse processes spread over a number of subsidiaries, either domestically or internationally. Many vendors have recognized the demand, and are working to provide the technology that facilitates central management. This is typically delivered in the form of management cockpits or collaborative tools that are able to integrate many single-point solutions, developed either in-house or delivered by third party vendors. Figure 5 provides an example of a central compliance system and cockpit. This management system has been ordered by a Japanese bank as a bespoke project in order to manage locally-deployed systems in various subsidiaries.



TECHNOLOGY AND VENDOR LANDSCAPE

The increase in both the number and the sophistication of financial crime events, and consequently both the business and regulatory response to them, have resulted in the proliferation of anti-money laundering and anti-fraud products and services and the vendors that support this fragmented market. As of today, the market is characterized by a number of business function solutions (especially for fraud detection purposes), delivered typically by niche vendors. In general, institutions must integrate these point solutions from numerous vendors. However, banks are shifting toward a cross-business function strategy that encompasses a cross-channel offering for fraud prevention and integrated back-office functionality for suspicious behavior detection. This chapter explains the main anti-money laundering and anti-fraud technology elements. In addition, this section provides an insight into the vendor landscape. Figure 6 below illustrates the main elements of an overall anti-money laundering and anti-fraud technology architecture.



The sophistication of back and middle office technology is growing

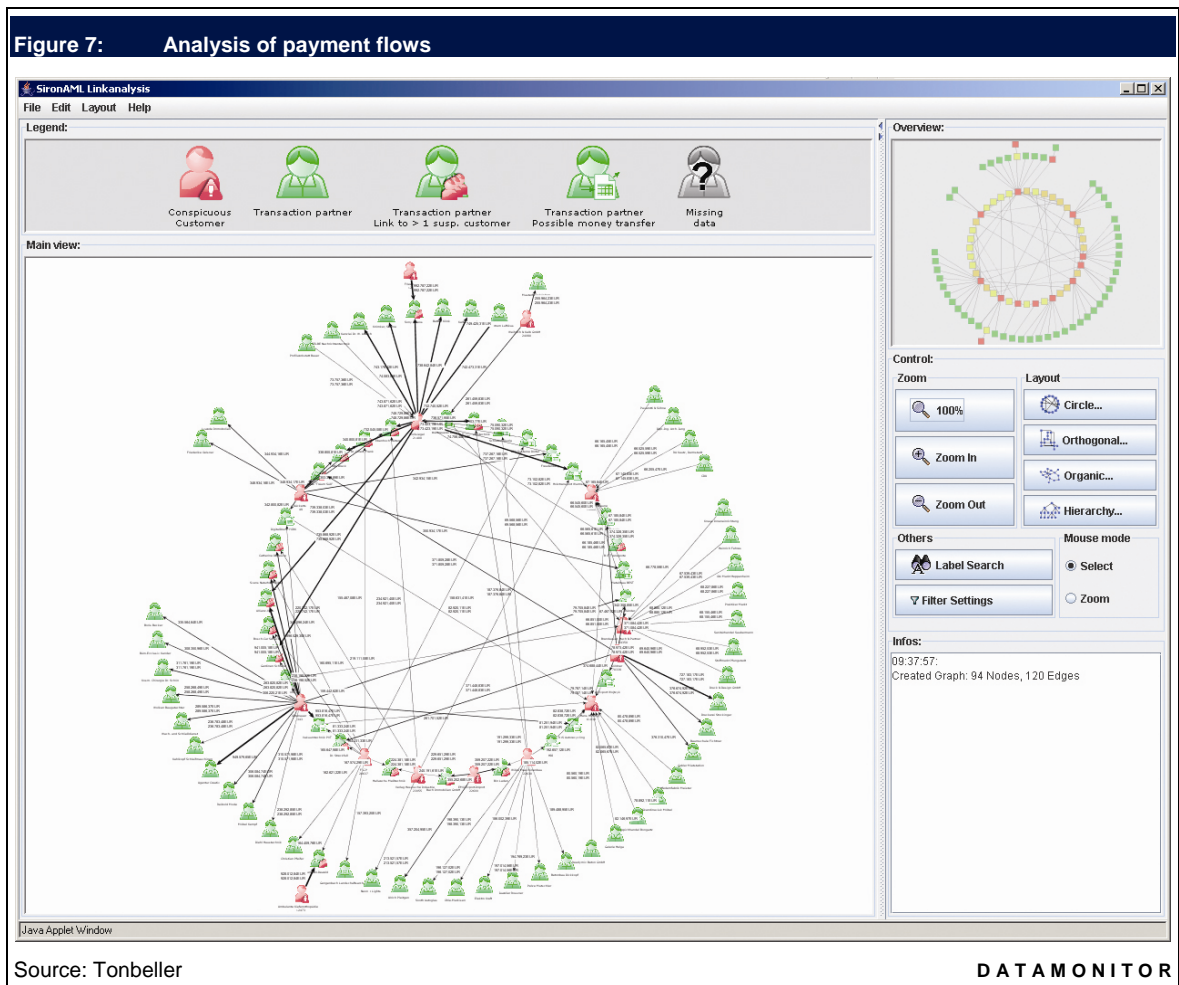
The paragraph below describes solutions that typically involve monitoring back and middle-office activities. It explains the items from Figure 6 located in the middle and on the left-hand side of the diagram in more detail, and provides insight into vendor offerings.

Risk management analytics – this involves either batch or real-time transaction processing and an anomaly detection engine that is able to integrate transactional front and back office data streams with information stored in data warehouses. This risk engine tool offers a broad range of analytical capabilities, such as:

- aggregations;
- statistical analysis;
- moving averages;
- regression;
- time-series analysis;
- name, phone number and address matching;
- dynamic profiles, and others.

The engine can be either a part of a single solution or built as a base platform for a set of solutions.

Transaction monitoring software – this is the fundamental analytical tool that scans transactional data or customer account information, and analyzes it to identify potential suspicious activity. The tool also investigates relationships between accounts, which can be examined through analyzing either beneficiaries, related beneficiaries on different accounts, or through transactions between accounts (including transactions that use intermediaries). All this information can be analyzed using predefined business rules and various types of analytical models that are designed to uncover any potential suspicious activity. An example is shown in Figure 7 below, which graphically presents analysis of payment flows, and highlights suspicious activity (highlighted in red).



Transaction monitoring solutions are typically delivered as either anti-money laundering solutions or transactional data fraud detection solutions. A similar risk management engine for both types of solutions can be embedded into the functionality. Several vendors have developed solutions that monitor transactions. The solutions listed below are typically found on the market. **ACI** delivers ‘ACI Proactive Risk Manager’. **SAS** has developed its ‘SAS Anti-Money Laundering’ and ‘SAS Fraud Management: Network Investigation & Analysis’ suites. **Norkom** delivers ‘Anti-Money Laundering’ solution. **Tonbeller** offers ‘Siron FD’ and Siron AML”. **Actimize** markets ‘Suspicious Activity Monitoring’ and **Fortent** provides ‘Fortent AML’. Though the **NetEconomy** acquisition, **Fiserv** now offers ‘Anti-Money Laundering Software Solution’. **Banker’s Toolbox** sells directly and through **Fidelity IS** partnership ‘Fraud Manager’ and ‘Bank Secrecy Act Anti-Money Laundering Management System’. **Metavante** offers ‘BSA Reporter’. **Oracle** through the Mantas acquisition provides ‘Oracle Mantas Anti Money Laundering’. **Memento Security** sells its ‘ACH Fraud’ solution. **Wolters Kluwer FS** also offers ‘Wiz Sentri: Transaction Monitor’.

Know Your Customer (Customer Due Diligence) – this element is primarily used to automate the account set-up stage for a new individual or entity. Its primary function is to check the prospect's identity, including running the prospect's name through various types of watch-lists, running credit history checks (internal or with credit bureaus), running through a system that scores the likelihood of fraud associated with an applicant's identity, or other types of identity checks. The element also includes a workflow that helps to manage the process of checking related individuals, or entities to the prospect (unless local regulations forbid doing so). This functionality is primarily used to set up a risk-based approach to anti-money laundering, and also to eliminate any future fraudulent activities. Once the account is set up, the technology will help to score the likelihood that a prospect will remain in low-risk standing, and help to estimate the potential change of risk for that customer in an ongoing manner.

Many technology vendors embed elements of this functionality into a general anti-fraud or AML solution. However, this report highlights several vendors who have developed a solid offering. **ID Analytics** provides 'ID Score' products that analyze potential risk levels of new customers. **Norkom** sells its 'Customer Due Diligence' product; **Actimize** and **Fiserv/NetEconomy** have similarly called offerings. **Fair Isaac** offers 'Falcon ID' for identity theft prevention. **Early Warning Services** has developed 'Identity Check'. **Metavante** sells 'EDD Reporter'. **Fidelity IS** offers a solution for applicant validation and authentication called 'FIS Origin'. **Fortent** positions its 'Fortent KYC' solution in this segment. Through the **Mantas** acquisition, **Oracle** now offers now 'Oracle Mantas Know Your Customer'. **Memento Security** sells its 'New Account Fraud' and **RSA** offers 'RSA Identity Verification'. While **Wolters Kluwer FS** provides 'WIZ Senti™: RiskID'.

The KYC component (as well as fraud detection tools) may use services that provide data for authentication purposes from external sources. Typically these services are used extensively in markets where shared data on individuals or entities is readily available, such as the US. Many vendors provide data, such as geo-location intelligence provided by specialists including **Quova** and **Digital Element**, phone number identification data from **TargusInfo**, customer identity data from **Lexis Nexis** or **IDology**, or data from credit bureaus (**Experian**, **Equifax**, **TransUnion**).

Watch-list filtering – this element is responsible for checking individuals and other entities related to financial transactions inside and outside of the bank or other FSI. In addition, the solution checks these individuals or entities against various government watch-lists such as those delivered by OFAC, the Bank of England or OFSI. The development of a more risk-driven approach has also resulted in enhancing the solution through functionality that checks against other types of databases of potentially high-risk individuals and businesses, such as known terrorists, criminals, politically exposed persons (PEPs) or others. The solution is usually embedded within the general AML or KYC/origination offering, and is provided by vendors such as **Actimize** and **Norkom**, although **Tonbeller** sells a stand-alone product called 'SironEmbargo', and **Metavante** provides 'OFAC Reporter'.

Internal fraud detection (for retail banks) – this component has been created in response to insider fraud, as the black market for stolen customer or financial data by banking employees is growing, as is the number of identity theft issues. The tool automates the detection of common types of employee fraud, and further provides investigation capabilities to senior compliance management or anti-fraud experts. These capabilities can be provided as fraud alerts, advanced query tools, SAR filing or workflows.

Due to the discovery of many cases of collusion between banking employees and fraudsters, some vendors have started selling products that detect suspicious activity among employees. **Fortent** provides 'Employee Access Monitoring' that monitors employees and their interaction with banking systems. **Actimize** sells out-of-the box 'Employee Fraud' that offers

detection and investigation functionality. **Memento Security** developed an insider fraud detection solution with case management. The Memento Security's solution is also offered by **Fair Isaac**. **Fiserv** offers this functionality through 'The Employee Fraud Manager' developed by **NetEconomy** (acquired by **Fiserv** in 2007). **Oracle**, through the **Mantas** acquisition, offers 'i-flex Mantas Fraud Surveillance'. **Early Warning Services** has developed and 'Internal Fraud Prevention' service. **Intellinx** also specializes in insider theft.

Reporting – this is the component typically responsible for regulatory reporting (such as filing suspicious activity reports, currency transaction reports, or other reports required by regulators), but it also manages any type of internal reporting requirements. This particular component is typically embedded in the general anti-money laundering offering. The research highlights **Actimize**, **Norkom**, **Fortent** and **Fiserv/NetEconomy** for their reporting capability, although some vendors provide this offering as a stand-alone product. For example, **Wolters Kluwer FS** offers 'Suspicious Activity Report Documents', and **Metavante** offers Prime Legal Reporter that is designed to comply with the 314A requests for information from regulatory and legal entities.

Case Management – this tool is designed to manage the workflow of compliance or anti-fraud staff members, but also to examine and manage the output of various AML/anti-fraud systems. The component is responsible for managing potential cases flagged up for further investigation by the automated portion of a system, and also for possible reporting to regulators or internal senior compliance or security management.

Due to the fact that over time employees tend to lose track of the logic that creates the alerts, vendors responded with case management solutions either for fraud or for compliance related workflows. The focus is to create a system that is easy to understand by staff. Many vendors provide case management systems. Quite often the basic functionality is provided in addition to the core offering. However, there are several vendors who have developed quite advanced case management systems. **Actimize** offers 'Risk Case Manager' (Figure 9 on page 29) that is already deployed within over 100 FSIs. **Norkom** provides this functionality through its 'Enterprise Investigation Management' solution, and **Fiserv/NetEconomy** delivers its 'Case Management System' that is integrated within the 'Financial Crime Suite'. **Wolters Kluwer FS** also offers its 'Case Management' solution.

Front office monitoring solutions have proliferated in response to demand

The paragraph below describes solutions that typically involve the monitoring of front-office activities. It explains the items from Figure 6 located on the right-hand side of the diagram in more detail, and provides insight into vendor offerings.

Point-of-sale/ATM/Card-Present fraud detection – these are the fraud monitoring systems that operate at the point of sale when the card is present, that is, when a card interacts with a payment terminal through swiping or touching. This element is designed to run transactions through a risk model, and return a score that indicates the propensity for fraud. The score is then passed through a filter of predefined business rules that determine subsequent actions. These systems must be operational at the same time as the transaction is being processed in order to make real-time decisions to stop fraud. While quite often the predefined rules are based on previously noted fraudulent behavior, the systems may not be able to stop the first suspicious transaction, due to the fact that a pattern of a fraudulent activity has not yet been recognized. In general, the technology offered at this point of time is not able to entirely replace human senses. Therefore, staff training (unless members of staff are in collusion with fraudsters) still remains high on the retailer's agenda.

This is the oldest area where fraud detection and prevention functionality has been deployed. This is one of the reasons why the market in this segment is less fragmented than the Card-Not-Present area. Several major technology vendors are successfully competing for market share. **ACI**, **Actimize**, **Alaric**, **Fair Isaac**, **Fidelity**, **Norkom** and **SAS** have developed a sound foundation in order to dominate this segment.

Fair Isaac introduced its 'Falcon Fraud Manager' in 1992, which is currently serving 17 of the 20 credit card issuers worldwide. The solution is known for its use of transaction profiles and a neural network engine to detect abnormal behavior patterns and generate a fraud score. The Falcon product line has been enhanced by newer solutions such as the 'Falcon Predictor with Merchant Profiles', that adds merchant data analysis in order to achieve increased detection, and by the 'Card Alert Service' that checks for counterfeit debit cards and ATM deposit fraud. **ACI Worldwide** moved into the segment by leveraging its payment processing experience, and currently offers the 'ACI Proactive Risk Manager'. **Actimize** (acquired by **NICE Systems** in 2007) offers 'ATM/Debit Card Fraud' with its phase-based analytic models. The solution has been implemented by MasterCard, Bank of America, Lloyds TCB and Wells Fargo. **Norkom** mainly offers automated point of compromise analysis. The functionality is part of its multichannel fraud management solution. **SAS** has recently moved into the anti-financial crime segment by leveraging its analytic capabilities, mostly due to its partnership with HSBC that has resulted in developing the 'SAS Fraud Manager'. **Fidelity IS** provides 'Check Elert' and 'Deposits Shield', solutions that identify check fraud at the point of sale and prevent check-deposit fraud. **Fortent** offers 'Fortent Fraud Monitoring' designed to detect and prevent ATM/debit card and check fraud. **Fiserv** also delivers 'Carreker FraudLink' for ATM, card, check and ACH fraud mitigation, and 'Fiserv Imagesoft's FraudGuard' solution for remote capture fraud.

Online Channel/ Authentication/ Card-Not-Present Fraud Detection – these tools have been in high demand recently due to the overall development of the online channel. Fraud migration from the bricks-and-mortar economy to the digital world, such as that resulting from the introduction of Chip-and-PIN payment cards in Europe at the point of sale (forcing fraudsters to migrate to the e-commerce channel), has become an additional factor that contributes to the increasing demand. Finally, there are regulatory pressures; for example, the FFIEC has forced US banks to introduce multifactor authentication into their online banking channels. In general, these systems run transactions through risk models and return scores similar to the Card-Present transactions. However, as the card (or any other payment tool) is not physically used while making a purchase, merchants must take extra precautions against fraud exposure and associated losses. Therefore, extra layers of authentication are required, such as address verification, phone number verification, card verification services and others.

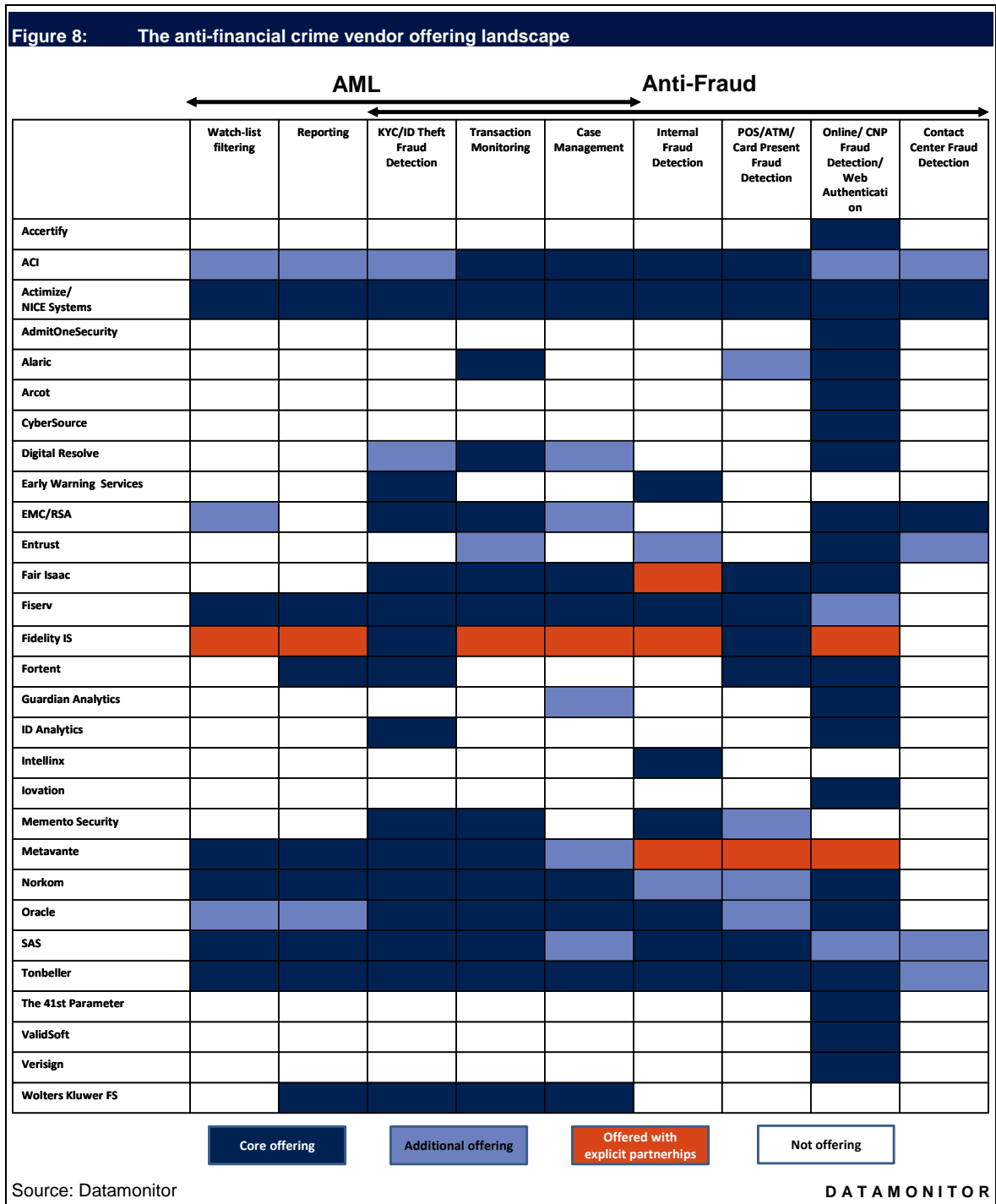
This is the most fragmented segment due to the fact that the online channel is relatively new. Therefore, many solutions have been initially developed by smaller companies, and many of these have been recently acquired (e.g. **Entrust** acquired **Business Signatures**, or **Oracle** bought **Bharosa**). There is a number of major vendors in the market and many small niche players. **Fair Isaac** offers 'Falcon Fraud Manager for Merchants'. **Actimize** sells its 'Remote Banking Fraud Prevention'. **Norkom** delivers the functionality as a part of its 'Multi-Channel Fraud' suite. **RSA** offers a very strong solution 'RSA FraudAction'. **VeriSign** provides 'VeriSign Identity Protection Fraud Detection Service'. **Oracle** through the **Bharosa** acquisition offers now 'Oracle Adaptive Access Manager'. **Entrust** sells 'TransactionGuard'. **Alaric** positions its 'Authentic' and 'Fractals' fraud detection solutions that utilize the Bayesian approach to card fraud detection (based on probability theory). There are also many smaller vendors who are targeting this segment such as: **The 41st Parameter**, **AdmitOneSecurity**, **Arcot**, **Guardian Analytics**, **Accertify**, **CyberSource**, **Iovation**, **Digital Resolve**, or **ValidSoft**.

Contact Center Fraud Detection – this set of solutions is developed specifically to accommodate the needs of the contact center channel. These technologies allow identifying suspicious phone calls, such as a call coming from a proxy intended to camouflage the originating number. In addition, it assesses the caller's intonation in order to detect nervousness and agitation (tones associated with suspicious activity). This functionality also associates the caller's voice with voiceprints already registered and flags up suspicious activity.

This particular segment is quite immature as of today. The voice analysis functionality was developed originally for military and security purposes and has found its way into different industries. There are very few vendors who offer voice-based fraud detection for the banking industry. **NICE Systems** (which acquired **Actimize** in 2007) is one of them. The company offers the 'NICE Perform Compliance Suite' that monitors voice based activity. Through the **Verid** acquisition, **RSA** offers a solution that monitors activities related to the call center environment.

The market is still fragmented due to its immaturity

Technology is critical to achieving sophistication in identifying and managing potential suspicious activity, whether money laundering or fraud. However, technology is also raw number crunching power, as well as automation. Figure 8 summarizes the very fragmented and still immature vendor offering landscape (in alphabetical order) and positions vendors in the overall anti-financial crime offering segment. The figure highlights vendors that provide the functionality listed as a 'core offering'. 'Additional offering' means that in specific cases products also offer basic functionality, typically embedded into other solutions. The chart ranks neither vendors nor the strength of their offering.



User-friendly AML and anti-fraud management tools increase workflow efficiency

The area of fraud or money laundering detection, as well as the broader area of business intelligence, has typically been the preserve of a select group of ‘power users’. Generally, strong mathematical skills were required to be an anti-fraud or

anti-money laundering expert. These skills are still required to some extent. However, the major portion of statistical analysis is now automated through technology, and the handling of anti-fraud or anti-laundering technology is migrating from the statistician/programmer community to business analyst groups. This is especially due to a growing appreciation of the importance of applying more automated and behavior- or probability-based intelligence to decisions the FSIs make. Moreover, the proliferation of graphical user interfaces and the automation of workflows allow less mathematically skilled business analysts or compliance officers to implement new rules, or manage financial crime cases. The chart below is an example of a graphical user interface offered by a software vendor. The system can be used with minimal knowledge of the statistical analyses that are being performed in the background.



Real-time detection capability enhances successful prevention

The need for instant financial crime detection capabilities in order to hold or stop a transaction has necessitated real or near real-time delivery functionality since the introduction of fraud or money laundering prevention programs. Nowadays, customers require many types of transactions to be processed immediately. For example, a merchant cannot afford a situation where a client has to wait more than a few seconds for his transaction to go through at the cash-desk in a retail store. However, an illegal transaction still needs to be stopped within these few seconds. Therefore, IT departments, systems integrators (SIs) or independent software vendors (ISVs) work on monitoring raw transactional data in order to

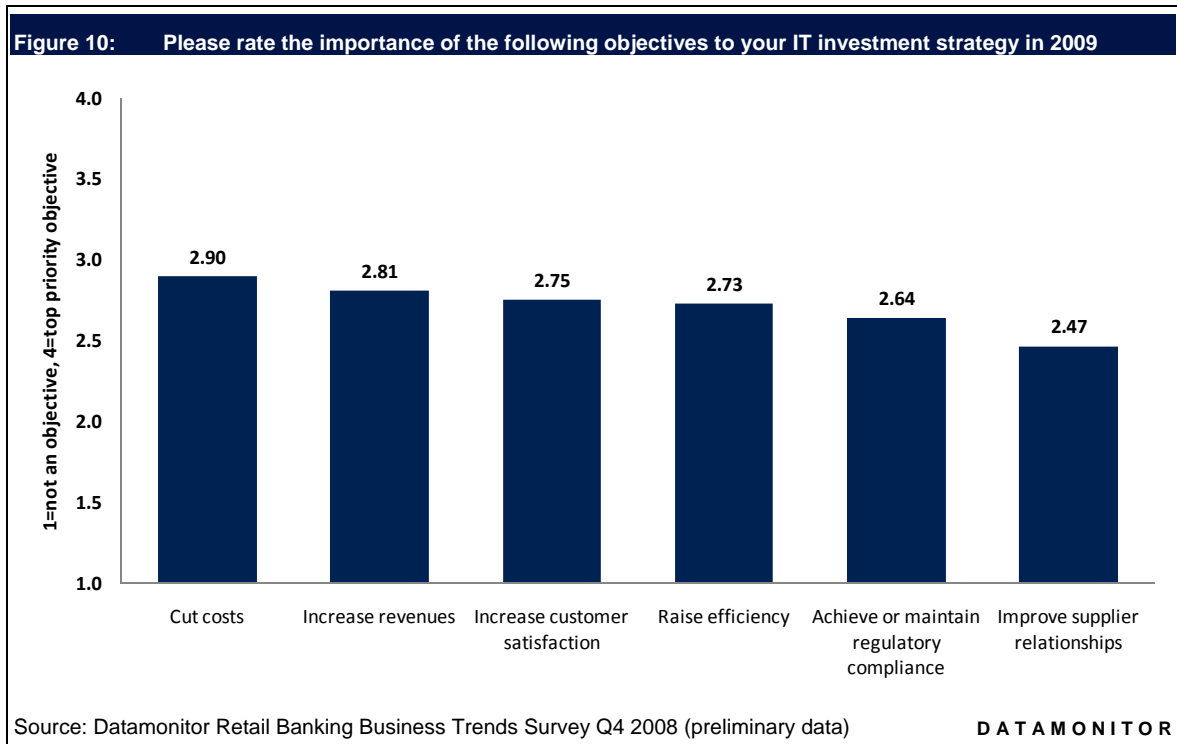
detect anomalies in an instant, as this functionality is an attractive offer to the market. These real-time delivery capabilities have promoted anti-money laundering and anti-fraud tools from their status as financial crime detection applications into the domain of the financial crime prevention area. In spite of these advances, many institutions are still lagging behind, and not in a position to fully utilize this functionality. Real-time capability allows the comparison of current business events with historical patterns in order to detect deviations automatically, with the detection engine based on either pre-defined rules or client behavior. Although real-time capability is quite often a necessity, it is not always possible to achieve given the current stage of technological development. For example, during the time when behavior-based systems need to learn the behavior of new clients, (e.g. recently developed keystroke biometric signatures - typing behaviors) or rules-based systems are not yet pre-defined to cover unknown suspicious patterns (e.g. a fraud analyst would have to create a rule based on a past fraudulent activity that was discovered manually).

Regardless of increasing technology capabilities and speed of processing, there is still a significant gap between detection and prevention. Automated prevention requires the system to automatically feed back into an operational system in a closed loop, without any human intervention. This real-time processing functionality necessitates two critical elements: first the ability to integrate data in real-time, and second, the ability to analyze it and detect deviations in real-time. Both of these components require supporting infrastructures and appropriate governance structures. Therefore, a number of supporting technologies will be required for fully automated financial crime prevention and detection engines, such as:

- data integration;
- low latency operational data store;
- message broker;
- real-time analysis.

An increasingly cost-driven market drives adoption of a hosted delivery model

The recent macroeconomic environment has resulted in increased pressures on cost cutting strategies, and there are many banks which are suffering extensively during the current financial crisis. Some of their counterparts, which are not under such pressures, are also cutting costs equally aggressively. A worldwide survey of 194 IT decision makers from retail banks conducted by Datamonitor in the last quarter of 2008 shows that cost-cutting will be the most important objectives driving banks' IT strategy in 2009 (Figure 10). A year ago, internal IT departments were in a much better position to hold onto their technology silos, and were less willing to move from a license-based to a subscription-based model. This year however, in the middle of the financial crisis, banking management is primarily interested in low cost solutions, with minimal exposure to fraud and compliance issues.



The hosted delivery model alleviates the customer burden of software maintenance, ongoing operation, and support. The opex-replacing-capex argument is heard louder and louder in the industry. The hosted delivery model's capability to reduce the up-front expense of software purchases through on-demand pricing is becoming a more popular option. Not that long ago, banking executives were reluctant to relinquish control over security or compliance related software or services, but now in an increasingly cost driven market, cost-cutting pressure takes priority over handling the security and compliance issues in-house. Many technology vendors have noticed the trend and are rushing to deliver their solutions (or particular components) in a hosted delivery model. However, it is worth noting that the hosted delivery model will be one of many delivery models, and ultimately, the pricing strategy will determine the final delivery model. Vendors should not expect any revolutionary changes in the foreseeable future, although, many vendors interviewed for this report hold the view that that the uptake in interest is definitely out there.

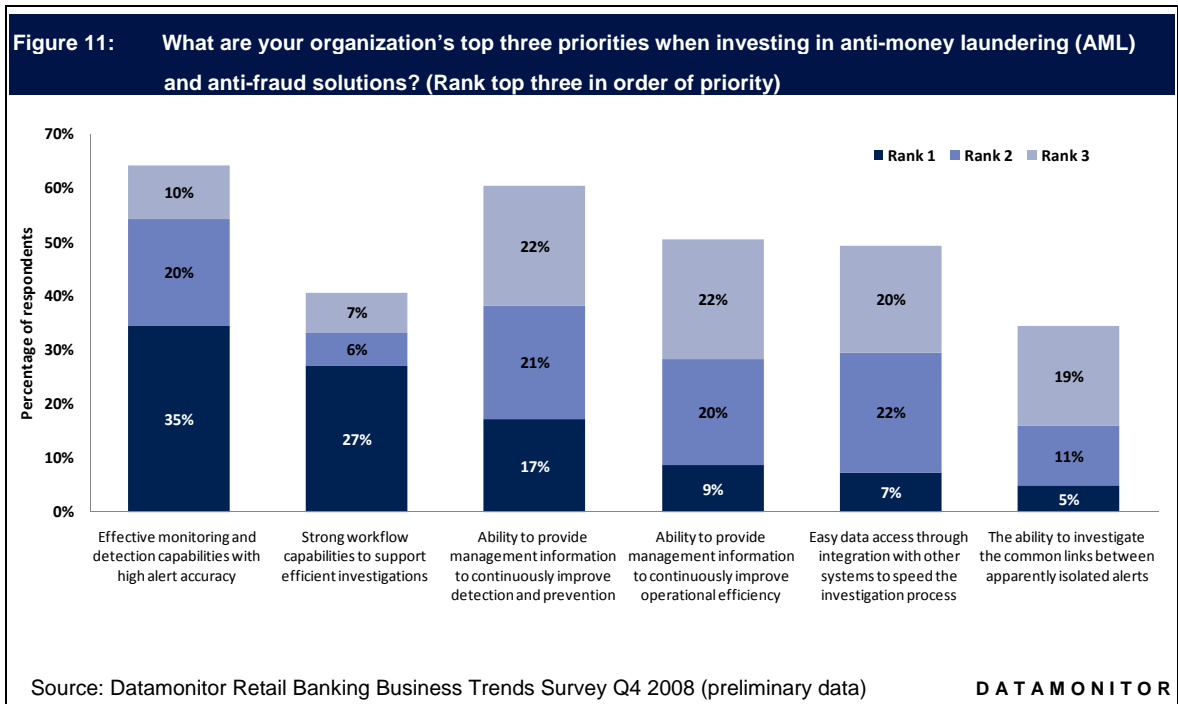
GO TO MARKET

The following recommendations focus on addressing the top priorities that banks take into consideration when investing in anti-financial crime solutions. Moreover, the chapter explains the benefits of approaching the market with end-to-end solutions, and provides quantified information on management information systems expenditures by retail banks.

Vendors should align the positioning of their solutions with their clients' main hot-spots

The vendors that will succeed in their marketing efforts are the ones that will address the most important customer pain points. Vendors should approach the market with an offering that provides the functionality described below and prioritized in Figure 11.

The financial crime detection and prevention discipline has been focusing primarily on transaction monitoring and anomalies detection capabilities. This fundamental functionality is still the highest priority for banks when investing in anti-money laundering and anti-fraud solutions. Nearly 64% of all the IT decision makers questioned by Datamonitor in the fourth quarter of 2008 pointed to the “effective monitoring and detection capabilities with high alert accuracy” as one of the three most important priorities when making their anti-financial crime technology investment decisions. For 35% of the respondents, this ability is at the top of their priority list. Many vendors have improved their detection capabilities, through implementation detection techniques such as artificial neural networks, Bayesian theory, or link analysis. They have also marketed their solutions focusing on how their detection engine works. However, solutions purchasers' greatest concern is to acquire a solution that provides high alert accuracy. Vendors need to focus on providing numeric proof (or if possible benchmarking studies) to their potential clients that demonstrates the reliability of their solutions.



While effective transaction monitoring for deviation detection is typically at the heart of every anti-financial crime solution, in order to perform well, it has to take feeds from a series of data sets generated around the business. Whether banks are able to increase the accuracy or not is typically based on how successful banks are with executing their information management strategy. For 60% of the IT decision makers, the “ability to provide management information to continuously improve detection and prevention” is one of the top three priorities when investing in anti-money laundering and anti-fraud solutions. It is also the top priority for 17% of the respondents. Therefore, vendors need to focus on promoting their solutions’ ability to work well in a very database- and middleware-intensive environment, and collaborate with technologies such as data warehousing, data mining and online analytical processing.

Even the most accurate and efficient detection solution that is available on the market will not solve financial crime issues without a proper investigation capability. Fraud and compliance analysts need their case management systems to perform well. Therefore, 41% of all IT decision makers prioritize “strong workflow capabilities to support efficient investigations”, and for 27% of the respondents, this functionality is the top priority. Vendors with strong case management systems should focus on positioning them to the target audience. Strong workflow capability is important to offer, but the solution should also support easy data access through integration with other systems. This is also an opportunity to provide IT services for a variety of consultants and IT services organizations.

Banks are seeking end-to-end solutions across financial crime types and investigation chains

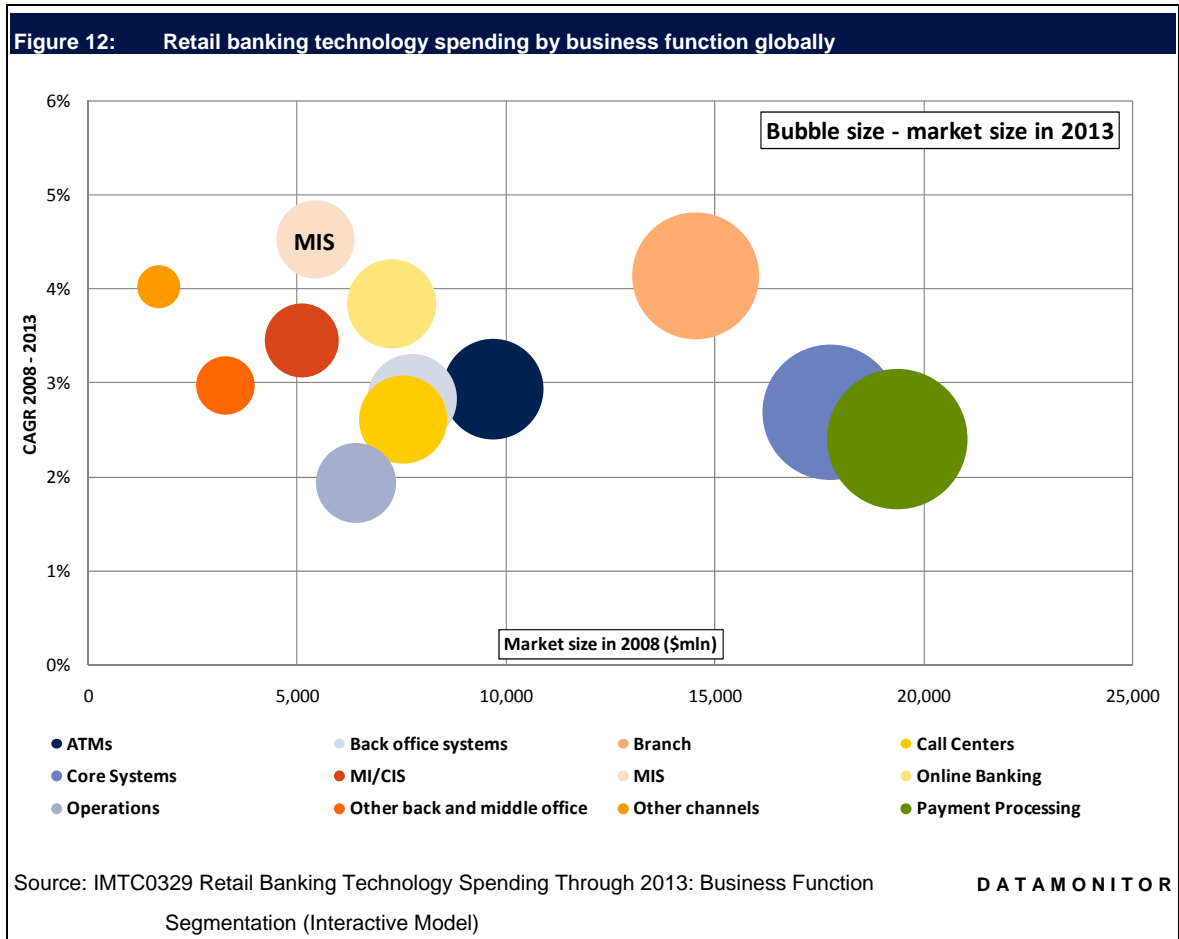
Given the fact that IT departments are pressured to centralize their data infrastructure and core processes, and reduce the number of vendors they work with, the proposition of end-to-end anti-financial crime solutions sounds appealing to banks. Furthermore, end-to-end implementation can act as a vehicle for the introduction of a central infrastructure strategy and data sources consolidation, driving out legacy and patchwork systems, not to mention that it can offer a cost effective approach. Apart from the benefits of an end-to-end offering, technology consumers need to take into consideration that decentralized data and project ownership make an enterprise-wide anti-financial crime functionality hard to achieve. An integrated application suite remains an ideal solution; however, it is clearly not yet an off-the-shelf proposition. The trend is toward offering a solution that offers integration across back and front office monitoring engines and that covers compliance, risk and security issues.

Integration of anti-financial crime solutions with IT infrastructure and core operational systems brings benefits for both vendors and the end user community. For vendors, it provides the opportunity to offer an enterprise-wide solution, rather than point-based deployments. Consequently, this is a chance for vendors to increase the user base of their offering and increase revenue streams, such as licensing, maintenance, or professional services. For end-users, an integrated platform offers the opportunity to make more effective use of their information assets.

MISs are forecast as one of the fastest growing areas of technology expenditure

Management information systems (MISs) are used to provide various layers of management decision-makers with the information required and typically take feeds from a series of other data sets generated around the business. This is the broader area that covers performance management, financial analysis, fraud detection and prevention, risk management and compliance among others. Datamonitor expects the overall amount spent by retail banks on MISs to grow from \$5.4

billion in 2008 to \$6.8 billion in 2013 globally (Figure 12). This will increase its share from 5.1% to around 5.5% of the overall (\$123.1 billion) technology expenditure in 2013. The area is one of the healthiest in terms of the expected growth. The expenditure on MISs is forecast to grow at a faster rate than other areas such as core systems, payment processing, or call centers. Figure 12 below is the graphical representation of the forecast growth of expenditure on various business functions in retail banking globally.



Technology vendors will find that around 85% of the global expenditure on MIS in 2008 belongs to retail banking institutions located in North America, Western Europe, and newly industrialized and developed economies in Asia Pacific. However, this share is expected to decline to about 82% in 2013. This is due to the fact that banks in emerging economies are forecasted to increase their spending at a higher rate than their counterparts in more developed markets. Central and Eastern European banks' IT budgets are expected to be the fastest growing opportunities for vendors, as the CAGR between 2008 and 2013 is forecast to stay at the highest level (10.1%).

APPENDIX

Definitions

AML – Anti-money laundering.

Back Office - Contains the core mission-critical systems in the financial institution that are not customer-facing.

Bank of England – The central bank of the United Kingdom.

CIS – The Commonwealth of Independent States.

CTF – Counter terrorist financing.

CTR – Currency Transaction Report.

Digital precious metals – A relatively new online system that involves the exchange of options or the right to purchase an amount of precious metals at a specific price.

FATF – The Financial Action Task Force.

FFIEC – The Federal Financial Institutions Examination Council.

FinCEN – The Financial Crimes Enforcement Network.

FIU – Financial Intelligence Unit, a centralized unit within a nation or jurisdiction to detect criminal financial activity and ensure adherence to laws against financial crimes, including terrorist financing and money laundering.

Front Office – Contains the systems that are used by the distribution channels and as such is the most diverse area in terms of systems used across the three core financial services sectors.

FSI – Financial services institution.

Internet payment services – Payment services provided by non-bank institutions operating exclusively on the internet and that are only indirectly associated with a bank account.

JMLSG – The Joint Money Laundering Steering Group.

KYC – Know your customer.

MI/CIS – Multichannel integration/customer information systems.

Middle Office – Contains the non-mission-critical systems within the financial institution that do not interact directly with the customer and provide 'added-value' to the institution beyond the systems essential for the institution's operations.

MIS – Management information systems.

Mobile payments (m-payments) – The use of mobile phones and other wireless communications devices to pay for goods and services.

NPM – New payments methods.

OFAC – The Office of Foreign Assets Control;

OFSI – The Office of the Superintendent of Financial Institutions.

PEP – Politically exposed person.

Prepaid cards – Provide access to monetary funds that are paid in advance by the cardholder.

SAR – Suspicious Activity Report.

SOCA – The Serious Organised Crime Agency.

STP – Straight through processing.

USA PATRIOT Act – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

Methodology

Interviews – Discussions with leading banks and technology vendors, conducted specifically for this report.

On-going vendor briefings – Datamonitor conducts interviews with software, hardware, networking and services vendors serving the retail banking sector on an ongoing basis.

Annual primary research – Datamonitor conducts 200 interviews annually with retail banking IT decision makers.

Secondary research – Other secondary sources of information, including company reports and web sites, international organization statistics, national and international industry associations, SEC filings, broker and analyst reports, and business information libraries and databases.

Further reading

Application Architecture Strategies in Retail Banking (Strategic Focus), November 2008, DMTC2260

Branch Strategies for the 21st Century in European Retail Banking (Strategic Focus), September 2008, DMTC2252

Online Banking in the Age of Web 2.0 (Strategic Focus), May 2008, DMTC2192

Building a Technology Platform for the “Ultimate Offering” (Review Report), August 2007, DMTC2090

Retail Banking Technology Spending Through 2013: Business Function Segmentation (Interactive Model), November 2008, IMTC0329

Retail Banking Technology Spending Through 2013: Source Segmentation (Interactive Model), November 2008, IMTC0285

Wealth Management Technology Spending Through 2013: Business Function Segmentation (Interactive Model), October 2008, IMTC0328

Wealth Management Technology Spending Through 2013: Source Segmentation (Interactive Model) October 2008, IMTC0323

Ask the analyst

The Technology Knowledge Center Writing Team

Author: Jaroslaw Knapik, Analyst, Financial Services Technology (jknapi@datamonitor.com)

Datamonitor consulting

We hope that the data and analysis in this brief will help you make informed and imaginative business decisions. If you have further requirements, Datamonitor's consulting team may be able to help you. For more information about Datamonitor's consulting capabilities, please contact us directly at consulting@datamonitor.com.

Disclaimer

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, Datamonitor.

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Datamonitor delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Datamonitor can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.