

Fraud and Compliance Risk: Effectively Navigating Through the Mounting Storms

A major storm is brewing, and like a tornado or hurricane it threatens to wage destruction on those caught unaware in its path.

Traditionally, financial institutions have had to weather threats from increasing organized crime on one side while riding out waves of compliance requirements on the other. Financial crime has always provided challenges to financial institutions, as fraudsters traditionally remain one step ahead of risk management efforts. Criminals evolve their methods of operation more quickly than institutions can react, and recent trends are moving toward attacks against the main customer accounts.

white paper



EVERY SECOND. EVERY DAY.

© 2005 ACI Worldwide

330 South 108th Avenue
Omaha, Nebraska 68154
402.390.7600

All rights reserved. All information in this document is confidential and proprietary to ACI Worldwide Inc. No part of this document may be photocopied or reproduced in any manner without the prior written consent of ACI Worldwide.

Table of Contents

Executive Overview.....	1
The Expanding Threat of Fraud Risk	3
1.1 Payment Card Fraud	4
1.2 Account-Based Fraud.....	5
1.3 The Expanding Threat of AML Compliance Risk.....	8
Navigating the Storms.....	12
2.1 Best Practices for Risk Mitigation: Point Solutions.....	12
2.2 Best Practices for Risk Mitigation: Partnerships.....	13
2.3 Best Practices for Risk Mitigation: Multi-Channel Consolidation	13
2.4 Summary	14
Fraud Risk Consolidation	15
AML Risk Consolidation	17
Fraud and Compliance Risk Consolidation?	18

Executive Overview

A major storm is brewing, and like a tornado or hurricane it threatens to wage destruction on those caught unaware in its path.

Traditionally, financial institutions have had to weather threats from increasing organized crime on one side while riding out waves of compliance requirements on the other. Financial crime has always provided challenges to financial institutions, as fraudsters traditionally remain one step ahead of risk management efforts. Criminals evolve their methods of operation more quickly than institutions can react, and recent trends are moving toward attacks against the main customer accounts.

Meanwhile, compliance risk has gained significant momentum in the area of anti-money laundering (AML). Over the past several years, government regulators have recognized the global threat of money laundering and terrorist funding. It seems that every day new regulations emerge globally or changes in existing mandates are announced country by country. Instead of weakening, these storms are gaining strength, and for some financial institutions, they threaten serious loss along with diminished value and brand.

Risk management has traditionally taken a focused approach, addressing risk along lines of business. While fraud and compliance have normally operated separately, even within fraud operations a silo approach to managing risk has been the norm. Institutions offering electronic banking took responsibility for automated teller machine (ATM) and debit card fraud. Credit card operations managed credit card fraud. Bank security personnel monitored check and deposit fraud. Compliance officers managed AML requirements.

Operationally and systemically, risk management departments within the business units put up their own protections to cost-effectively minimize both financial losses and risk to reputation. Over the years, these risk management techniques have proven effective in avoiding major damage. Nevertheless, the winds of fraud and compliance continue to shift and intensify, requiring institutions to either adapt or be swept aside.

There is, however, light shining through the clouds. A financial institution that is well informed and prepared can effectively navigate through the storm. Defensive measures are available to provide adequate protection and allow for profitable growth; cost-effective measures can be taken to manage risk without impairing business. Traditional risk management has occurred within the individual line of business. Methods are available at that level to build a strong first line of defense from a solution that is both operational and systemic. Furthermore, institutions do not need to fight the battle alone. Industry associations, new technology and law enforcement are providing support.

Finally, as fraud and money laundering continue to migrate across the enterprise to the deposit account level, institutions can operationally leverage internal resources to maintain a customer-centric (monitoring all customer accounts and transactions at a customer level) view of consumer relationships. New technology is advancing as well in the enterprise-wide fight against risk. Financial institutions can meet compliance demands cost effectively, thereby adequately mitigating fraud risk and profitably expanding their business.

1 The Expanding Threat of Fraud Risk

As recently as five years ago, few people predicted that in today's banking world we would be fighting major attacks in PIN-based transactions both at the ATM and point of sale. Who would have raised the alarm over potential massive database attacks where hundreds of thousands of cards or full identities would be stolen?

Consumers have access to the latest scanning, printing and graphics equipment that provide superb quality and detail. We should have expected that fraudsters would use those same devices to easily create bogus checks with their personal computers. With the growth in remote banking, relatively few anticipated that person-to-person (P2P) and electronic bill payment would open doors for criminals to establish phony business accounts enabling them to move fraudulent funds. The rejuvenated interest and movement to enhance cross-boarder payment products adds yet another dimension to fraud opportunities

Criminals continue to attack institutions at the points of customer payments, from established mechanisms such as ATMs, cards and checks to newer Internet-based points of interaction. Traditional fraud schemes are still used, but fraudsters also are exploiting the latest technologies to further gain advantage. Schemes have become more complex in nature to avoid the radar of risk management systems. Even more disconcerting are trends toward assaults at the core customer accounts. Identity theft and phishing are the hottest problems in the industry today and threaten to erode consumer confidence.

None of these trends is limited to one particular country or region. These trends have impact on financial institutions around the world. A main reason for this global impact is organized criminals' ventures into financial crimes. Syndicates have found the growth in electronic banking a lucrative opportunity to access their favorite commodity — cash — and in large sums.

The Internet has opened doors for anonymity and increased the speed of moving stolen cash and data. Many countries have fairly stable financial markets with minimal legislative force to prosecute these types of crimes.

Even more difficult to control is the “cross-border” nature of fraud. Criminals gain access to customer accounts in one country and access the accounts from a second or even third country. This scenario makes prosecution more difficult if not almost impossible at times.

Both the Internet and cross-border access to accounts provide perfect combinations from which to operate global crime organizations. As one financial institution, country or region implements risk management protection, thieves simply relocate to the next market where counter-fraud measures remain fairly weak. They then continue to use their global reach to commit fraud.

The following section provides a brief breakdown of fraud trends by line of business or payment type.

1.1 Payment Card Fraud

According to Tower Group, worldwide credit card losses exceed US\$4 billion annually.

The United States has consistently held the highest tab for card fraud. In fact, according to MasterCard, the United States accounted for approximately 47 percent of all credit card fraud losses worldwide in 2004. Card association statistics show that while average fraud compared to total sales remained fairly flat during that time, hovering between five and six basis points (bps), overall fraud losses consistently rose each quarter in 2004.

In western Europe, credit card fraud varies, but overall fraud losses by basis points have remained fairly flat at about seven bps. Individual country statistics reveal dramatic differences, though. For example, according to a recent Datamonitor report, countries such as the United Kingdom, Germany and Italy are running as high as 10 or 11 bps, while France and Spain are as low as three or four bps.

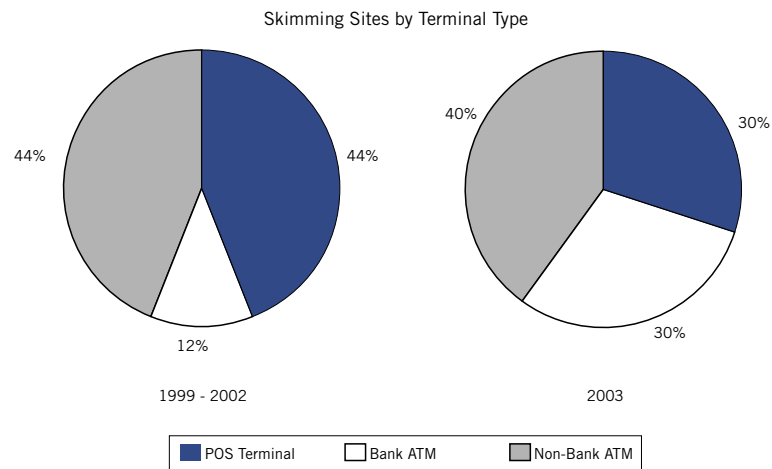
The major contributors to the rise in worldwide fraud losses are counterfeit and skimming fraud, with double-digit increases yearly for skimming. According to MasterCard, counterfeit fraud has surpassed lost and stolen card fraud losses and in 2004 ranked for the first time as the highest fraud type worldwide.

Within retail banks, the addition and expansion of electronic products and services have opened new revenue streams for financial institutions and reduced customer costs. Moving customers to ATMs, for example, can reduce per-transaction costs by as much as 40 percent. A recent banking survey in the United States revealed that 38 percent of customer transactions took place at ATMs compared to 32.5 percent at branches. Unfortunately, this shift has also been observed in criminal activity. Criminals' attraction to ATM and debit card fraud is obvious: Cash is king.

Industry fraud losses are much more difficult to determine in this area since there are no real self-imposed or industry-governed reporting requirements. A recent Celent report estimated ATM-fraud-related losses in the United States to be between US\$50 and US\$60 million annually. An estimated 70 percent of all debit card (PIN-based) losses in Canada are due to skimming at ATMs.

The Datamonitor chart in Figure 1.0 shows how ATMs have quickly become the preferred locations for compromising magnetic stripe cards, with subsequent fraud transactions also occurring at the ATM.

Figure 1.0



Skimming methods have been well documented, and these schemes are becoming significantly more sophisticated as technology improves. For example, organized criminals have accessed resources that create ATM “overlays” that almost indistinguishably imitate actual ATM devices. The overlay devices include card skimmers to capture card data, PIN pads to capture PIN numbers and transmitters to immediately send the information to PCs inside vehicles in the vicinity. The fraudster’s PC receives the information and downloads it to a portable card encoder. White plastic cards containing the skimmed data are then generated and fraudulent activities can be conducted almost immediately.

Overlays are generally left on a particular ATM for several hours, then moved to another location making it difficult to determine the actual point of compromise. ATM skimming is on the rise in every major financial market.

Summary

Payment card fraud is evolving and becoming more dangerous to consumer accounts. Even more threatening, however, are its ties to organized crime and terrorist funding. Note that according to a November 2004 News.Telegraph.Com article the 2004 terrorist bombings in Madrid, Spain, were partially funded by skimming fraud conducted in France. Furthermore, the escalation of PIN-based fraud loss threatens the very core of consumer confidence in the electronic banking channel. Global efforts by financial institutions, card associations, networks and law enforcement must equally escalate to overcome these fraud schemes.

1.2 Account-Based Fraud

Risk management departments must realize that criminals are beginning to extend their reach from payment card fraud across the enterprise. A June 2004 Gartner report revealed, based on the agency’s research, that the checking accounts of an estimated 2 million Americans had been raided in the previous 12-month period. Estimates show that these attacks averaged more than US\$1,200 per incident, pushing total losses over US\$2 billion.

The main schemes attributed to these account-based losses were identity theft and phishing.

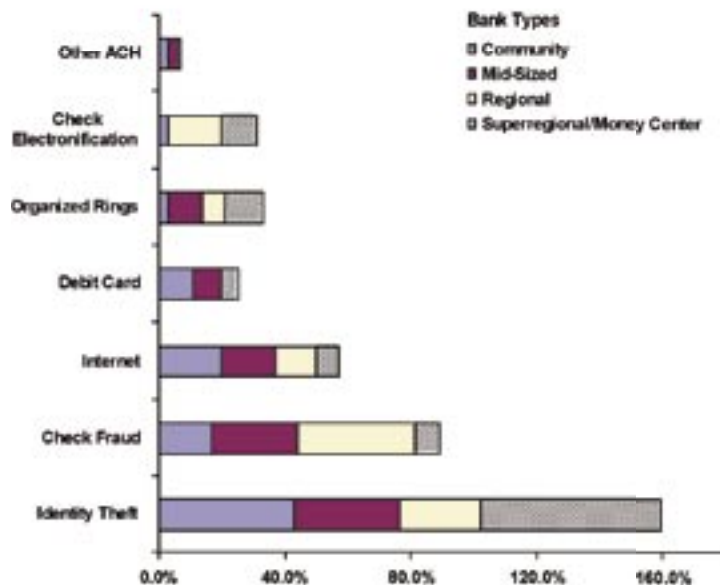
Gartner's study went on to evaluate what types of account-based fraud were used in committing identity theft. The study revealed that 44 percent of the loss is attributed to unauthorized transfers of funds from a deposit account; an additional 24 percent was due to check forgeries.

Identity theft has been well documented as one of the fastest growing fraud schemes during recent years. In the United States, a Federal Trade Commission (FTC) report showed that 9.9 million cases of identity theft from April 2002 to April 2003 led to over US\$5 billion in losses.

According to FinCen, approximately 10 percent of all suspicious activity reports filed in the United States were linked to identity theft. That number may appear low, but it represented a 120 percent increase from the prior year.

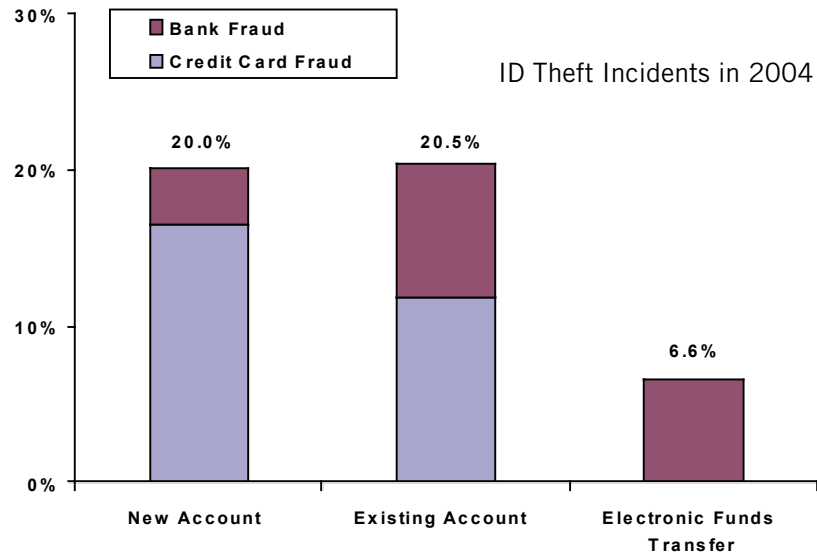
According to the FTC, the average annual growth rate for identity theft is 33 percent. As the chart from the FTC depicts (Figure 1.1), identity theft has encroached more on core banking accounts and retreated from credit card accounts.

Figure 1.1



According to a 2004 American Bankers Association survey, financial institutions rated identity theft as the No. 1 fraud threat to deposit accounts (Figure 1.2).

Figure 1.2



Phishing is competing with identity theft as the hottest topic in fraud news and actually facilitates a growing incidence of identity theft. Phishing attacks occur via the Internet where fraudsters establish spoofed (imitations of actual financial institution communications) e-mail accounts and Web sites and use them to bait consumers into revealing personal information, including account and PIN numbers, online banking passwords, and social security numbers. With this information, fraudsters are able to steal consumer account and identity information.

Phishing has given criminals a wide range of cost-effective means by which to steal data. A 2004 Gartner survey estimates that more than 57 million U.S. adults have received phishing e-mails in the previous six to 12 months. Of the 1.8 million consumers who recall providing data in response to phishing, more than half fell victim to identity theft-related fraud. The result is an estimated US\$1.2 billion in losses.

These schemes grew 4,000 percent during the first six months of 2005, according to the Anti-Phishing Working Group (APWG), an organization formed to identify and evaluate solutions to phishing. Figure 1.3 is a chart from the APWG that shows the number of phishing sites reported between December 2004 and March 2005.

Figure 1.3



Check fraud should not be forgotten. This old favorite of criminals still contributes to one of the largest segments of loss in retail banks in some parts of the world. An estimated 1.2 million fraudulent checks are written each year in the United States, according to the U.S. Department of Treasury. Advances in desktop publishing software and quality of home office copy machines, scanners and printers has complicated identifying counterfeit checks.

In the United States, the recently enacted Check Clearing for the 21st Century Act (Check 21) is a move to convert paper check processing from hard copy to electronic images. Although Check 21 is projected to save the banking industry millions in operational costs, the production of image replacement documents (IRDs) for checks will make the task of identifying counterfeit checks more difficult.

Summary

Criminals are moving away from specific payment types and on to attacks on the core deposit accounts. These schemes are becoming more complex as thieves gain access to consumer accounts enterprise-wide across financial institutions.

This evolution of enterprise fraud will look more and more like this: A fraudster opens a new account using data from an identity theft scam. After some time, a counterfeit check is deposited at the ATM. Through remote banking service the fraudster transfers the funds to his savings account. An automated clearing house (ACH) or wire transfer moves the funds to a bank account at a separate financial institution where the fraudster then removes the money. With effective kiting methods, the losses can grow quickly. And with electronic check processing expected to grow, it should not take long for criminals to adapt fraud schemes to take advantage of IRDs and the lack of a physical check.

1.3 The Expanding Threat of AML Compliance Risk

Another storm converging on financial institutions is an activist regulatory environment surrounding the monitoring of money laundering and terrorist funding. While numerous activities around the world were focusing on these problems, the Sept. 11, 2001, terrorist attacks in the United States initiated a legislative domino effect. The subsequent enactment

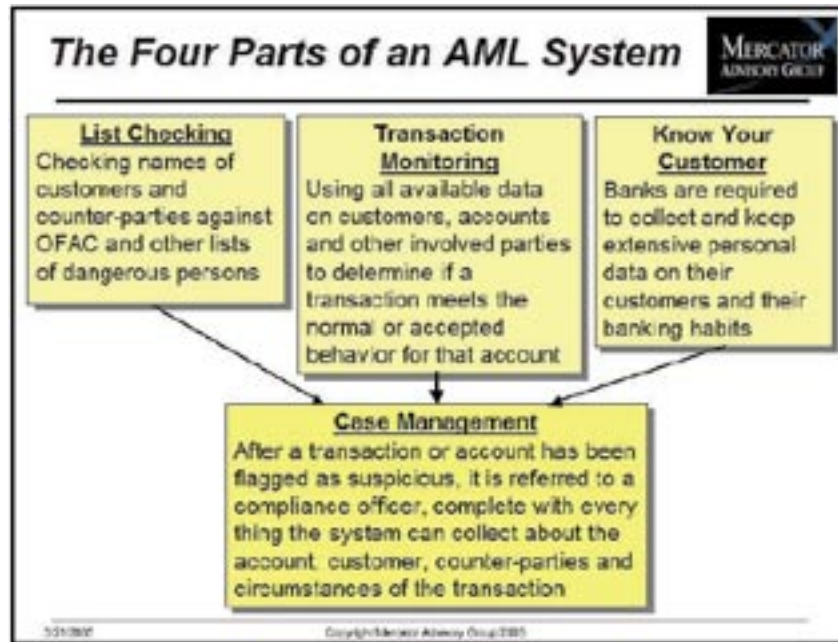
of the USA PATRIOT Act induced far-reaching impact not only to U.S.-based financial institutions, but also to any bank moving funds through U.S. accounts. International pressure and guidance from organizations such as the Financial Action Task Force (FATF) have influenced countries worldwide toward implementing new AML regulations. The European Union directives have evolved and grown in their reach as well.

The basic principles for most of these regulations rely on four core functions:

- 1) Name an executive compliance/risk officer with ultimate responsibility for the AML program.
- 2) Implement standard AML policies and procedures.
- 3) Provide thorough employee training at all levels of the institution.
- 4) Assure third-party auditing of the program.

Regulators have built upon this foundation a series of requirements for monitoring, detecting and reporting suspicious activity. For most institutions this requires the application of technology solutions to adequately satisfy auditors. These solutions cover four main business needs, which include list checking, transaction monitoring, customer identification and case management (Figure 1.4).

Figure 1.4



Since the AML regulatory environment is relatively young, the frontline regulators conducting banking reviews are still streamlining application and enforcement of the rules. This has created a difficult situation for financial institutions because the requirements are regularly undergoing modification. As markets have matured in this area so have regulations, and as they are announced within a market, institutions generally take only the basic steps necessary to be deemed compliant. As regulators become more comfortable with the basic principles, more stringent enforcement begins.

A good example of this trend can be found in an acceptable transaction monitoring system. Prior to the current onslaught of legislation, manual efforts and paper-based alert reporting was sufficient. In the early days after implementation of the latest regulations, basic, automated, rules-based systems were applied to monitor at the individual account level. However, mandates are changing to require the use of advanced analytics to monitor at a customer-centric level and scan all accounts enterprise-wide.

One thing is certain: No institution wants to fail an AML regulatory examination. Documented examples of disciplinary actions have shouted from media headlines. Of the 210 enforcement actions taken by U.S. regulatory agencies during the first half of 2004, 10 percent involved lack of compliance with AML rules. Of the most recent, one bank in the United States was fined US\$10 million for failing to establish an adequate AML program and failure to file accurate, timely and complete suspicious activity reports (SARs). Similarly, another's failure to comply with AML mandates cost it over US\$25 million, and a Caribbean bank was fined US\$26 million for AML violations.

These enforcement actions affected the desired result of driving up SAR filings as shown in a chart from Financial Insights (Figure 1.5).

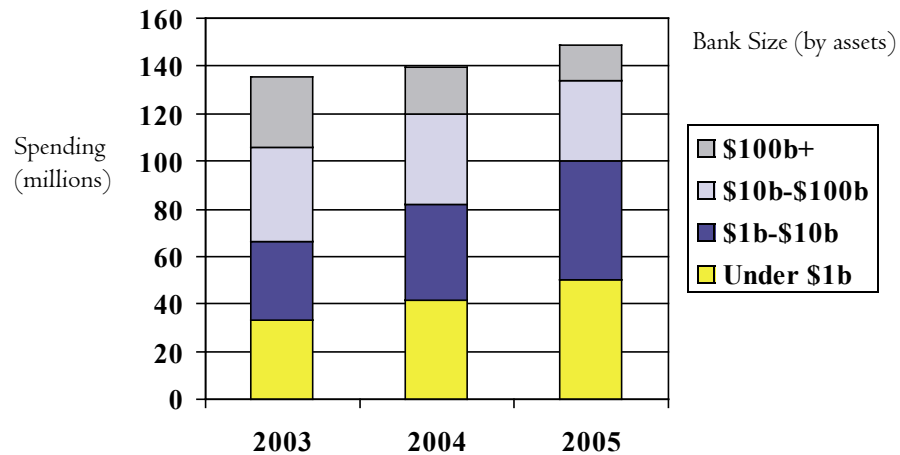
Figure 1.5

Suspicious-Activity Reports by Country, 2003

Country	Number of Reports	2002-2003 Increase (%)
Canada	9.5M	400
United States	203,538	25
United Kingdom	94,708	64
Japan	43,768	133
Hong Kong	10,000	10
South Korea	5,000	NA
Switzerland	863	32

This regulatory environment threatens institutions with severe penalties and fines for non-compliance, forcing them to heavily invest in AML programs and technology. Depending on size, institutions spend from hundreds of thousands to millions of dollars on AML programs. The following chart from Mercator (Figure 1.6) details U.S. bank spending on AML solutions over the past three years.

Figure 1.6



Avoidance of multi-million-dollar fines is a strong motivator for most institutions but does little for profitability and improving shareholder value. A 2004 KPMG International study on AML programs found that AML compliance spending increased by an average of 61 percent over the past three years, mostly in the area of transaction monitoring, and will continue to increase over the next three years.

Summary

Along with facing losses from fraud, institutions face a considerable amount of risk in the area of money laundering — specifically if they fail to comply with AML mandates and regulations that are emerging and evolving globally. If institutions fail to comply with AML regulations, the resulting penalties and fines can be devastating.

To properly comply with AML regulations, institutions must implement and maintain a transaction monitoring system that monitors, detects and reports suspicious activities, which generally requires a technology investment. Technology solutions overall can provide sound support in four main areas: list checking, transaction monitoring, customer identification and case management.

2 Navigating the Storms

Despite the rather bleak picture of the trends in fraud and compliance risk painted in the previous section, all is not lost. Excellent tools are available to help financial institutions successfully avoid major fraud losses, as well as ensure compliance with the most stringent AML regulations. To win the fight, institutions need to establish a strong defense both in operational techniques and with the latest technology solutions.

First, we should establish what it means to “win the fight.” From an AML perspective, this means passing regulatory reviews and gaining regulator approvals for an AML program. As daunting a task as this is, a diligent and ongoing effort in this area can position institutions to achieve compliance. The challenge is more difficult on the fraud side. Fraud will always be with us; the best efforts from the most skilled staff will not eradicate fraud loss. What can be accomplished is successful mitigation of fraud losses, allowing institutions to operate profitable businesses. Even more critical is maintaining a sound reputation. Falling victim to failed AML compliance or suffering a significant fraud loss event that becomes public knowledge can be devastating. Such risks to reputation are becoming the primary concern for many institutions. The following information will provide assistance in preventing fraud losses.

2.1 Best Practices for Risk Mitigation: Point Solutions

As noted earlier, the traditional approach to risk management has been to address risk within the business at a specific point of customer interaction. For the most part, this has proven effective in mitigating risk at the financial institution product level.

“Best practices” are readily available for every financial product on the market, so they will not be covered in detail here. For card products, the card associations like Visa and MasterCard offer a wealth of information about risk management. Regional PIN-based networks and switches, such as Interac in Canada, also provide this type of support. And ATM hardware vendors are moving quickly to address ATM security against skimming attacks.

Numerous industry associations, such as APACS in the United Kingdom, are ideal resources to tap for assistance as well. Several AML, security and fraud investigation organizations like the International Association of Financial Crimes Investigators (IAFCI) and the Association of Certified Anti-Money Laundering Specialists (ACAMS) also provide excellent data on trends and schemes.

Regardless of the product or financial services line involved, transaction monitoring is critical in mitigating risk and reducing fraud losses. As more types of transactions become electronic, such as checks have with the advent of Check 21, greater opportunity arises to utilize advanced analytics to quickly identify fraud attacks and complex money laundering activity.

2.2 Best Practices for Risk Mitigation: Partnerships

Often criminals appear to have better communication networks in place than the risk management community. Risk is an area in which institutions should be less concerned about competition and more open to working together to fight a common enemy.

The associations previously mentioned are excellent starting points. One of the most effective methods is to form alliances with financial institution risk managers on a regional basis. Along with technology, most solution providers have risk management product user groups that provide excellent avenues for sharing trends in fraud and risk, as well as best practice rules for detecting suspicious activity.

The establishment of task forces between the private and public sectors is another growing trend. Unfortunately, financial crime has historically been a low priority for law enforcement. Little action was taken for fraud crimes unless the dollar loss was extraordinary. In some countries, the laws deal very little with financial crime and, especially in electronic banking, make prosecution almost impossible when suspects are found.

Fortunately, this situation is turning around. Financial crime is receiving more media attention and, combined with organized crime's involvement, has drawn the attention of law enforcement and government agencies. Some countries have established successful partnerships between private risk management sectors and law enforcement task forces. The United Kingdom is a good example; the Metropolitan Police in London formed a specific financial crime group to work with risk teams at local banks. The banks fund this task force, which has been effective in catching and prosecuting crime rings. Similar groups have been formed in Toronto, Canada, and major cities in the United States.

Money laundering prevention can be just as frustrating as fraud prevention. Institutions are pressed to file suspicious activity reports, but to what end? Very little, if any, feedback is given about the outcome of reports. Individual regulators often interpret and enforce regulations differently, making it difficult for institutions to understand what is expected of them for compliance. In some regions, AML compliance officers have moved to form alliances that include their regional regulatory agencies. This allows for an open forum in which to discuss trends in suspicious activity and solutions available, as well as to set general expectations for banks.

2.3 Best Practices for Risk Mitigation: Multi-Channel Consolidation

Fraud and AML risk trends have placed enormous pressure on institutions to take a customer-centric view of all of their relationships. Identity theft and phishing are opening the doors to the core account funds for criminals, providing lucrative and feasible opportunities for fraudsters. Regulators are also requiring this same customer-centric

view to maintain compliance with AML regulations. In order to adequately address this new environment, financial institutions are implementing consolidated risk management approaches, both operationally and technically. This environment will be discussed in more detail in section 3, “Fraud Risk Consolidation.”

2.4 Summary

Several tools can help financial institutions avoid losses from both fraud and non-compliance. Establishing solid operational techniques and utilizing the latest technology solutions is imperative. Although the eradication of fraud is impossible, institutions can leverage these tools to remain profitable.

The traditional method of addressing risk at specific points of customer interaction remains one of the most effective. Fortunately, institutions have assistance in this area from card associations, regional PIN-based networks and switches, ATM hardware vendors, and industry organizations.

Intricate communication networks are great strengths for criminals committing fraud. Financial institutions should learn from this example and create their own anti-fraud communication networks among themselves, rather than striving to compete in this area. Industry organizations provide an excellent foundation for development of communication networks. Forming alliances with risk managers from other institutions in the region is another way in which to keep abreast fraud trends, as is joining a user group hosted by a solution provider. Yet another growing trend in alliance is establishment of task forces between the private and public sectors, which also solicits law enforcement’s involvement, an area typically lacking in the fight against fraud.

Identity theft and phishing are the fastest growing means by which criminals are committing fraud. Consolidated risk management approaches can benefit financial institutions both operationally and technically. Furthermore, by taking a customer-centric view of all of their relationships, institutions can establish a clear line of defense against attacks on core account funds, as well as maintain compliance with AML regulations.

3 Fraud Risk Consolidation

Within fraud management, the global trend has been moving toward the formation of a centralized fraud operation within each organization. Institutions are still trying to determine the best route to take in implementing this approach, but there is a great deal of activity in this direction.

There do exist variations on how a centralized operation functions; however, regardless of reporting structures at least two constants remain strong: First, at the top of the organization, a senior-level executive for risk management is established with a core support staff. This positions the institution to create and implement a centrally driven strategic risk plan. This core group is also responsible for tracking and reporting all risk-related loss events. Second, on the other end of the organization, in the trenches, the structure retains risk management expertise at the product level. Even if operations are consolidated into one overall department, individual product risk analysts are still assigned to manage fraud within their areas of expertise. What differs from institution to institution is how the rest of the organization is structured.

Moreover, one core theme persists among the varied organizations: Position resources to assure that an enterprise view of customer relationships is taken.

For institutions of any size this can be a daunting task and one best tackled in a phased approach. First, leave the frontline risk departments intact at the product and individual account level. Next, establish an “enterprise fraud staff” that resides above the product risk staff. This new group receives data from the product groups and monitors activity across all of those relationships. This allows them to see fraud trends across products and to identify high-risk customers or fraud attacks at the product level that can be unnoticed until too late. Finally, once the enterprise department is well established with solid workflow, policies and procedures in place, the product risk groups can collapse into one organization. Benefits of a phased approach include improved cross training of staff, increased employee retention by keeping analysts interested in new areas and, of course, improved risk mitigation.

Technology can be a great ally to institutions, but it can also pose a significant challenge to centralized fraud operations. Financial institutions often utilize multiple platforms, databases and fraud detection systems. The latter might be a combination of in-house and third-party products that vary from paper-based to advanced analytics.

Gaining the ability to bring these together into a central monitoring and detection system that uses a common database with a view to all customer transactions can provide analysts with a powerful tool in the battle against enterprise fraud risk. The systems must offer advanced analytics, such as neural networks, which influence authorization decisions in real time to produce the greatest impact on reducing risk. Over the past year, solution providers

have begun to offer comprehensive automated case management systems for working fraud cases, and these are also becoming increasingly common in fraud shops.

Summary

As more and more institutions are consolidating their fraud management operations to form centralized units, two constants remain: designation of a senior-level executive for risk management with a core support staff and risk management expertise at the product level. Moreover, the core theme that persists is to position resources in a way that assures that an enterprise view of customer relationships is taken.

A phased approach to consolidation can ensure that institutions suffer the least amount of impact possible. Furthermore, institutions should consider technology an ally, while recognizing the challenges it poses, and maximize the resources that are available and can help ensure a smooth transition. A successful combination of these can provide fraud analysts with a powerful tool in the battle against enterprise fraud risk.

4 AML Risk Consolidation

Within AML compliance organizations little segregation of responsibilities has been established. This group has traditionally remained small and closely tied. Thus, the move to a customer-centric view is more a technical issue than operational one.

However, larger, tier one financial institutions and those with a global presence will experience operational challenges where there remains some silo approach. Monitoring for suspicious activity may occur in different departments in different regions or countries. It is even more critical that AML compliance solutions can identify suspicious activity across the entire customer relationship. This is primarily due to the focus of regulators, but also because money launderers are evolving to more complex schemes to hide the flow of funds. Steps similar to those described in the “Fraud Risk Consolidation” section must be considered for the compliance organization.

Technically speaking, there has been a sizeable increase in the number of solution providers in the market. This fact has not escaped the notice of regulators in more mature markets who now require technology to be utilized in compliance with AML programs. The trend is moving from mere compliance using basic, low-end solutions to more advanced analytics that truly detect money-laundering activity.

In countries where AML regulations are just beginning to roll out, the initial focus has been more on implementing solutions, no matter how basic. These areas can expect that current requirements will evolve and become more stringent as in other markets, and they too will demand more advanced solutions to guarantee compliance.

Summary

Institutions’ move to establish a customer-centric view is more of a technical than operational issue, although larger, tier one financial institutions and those with global presence generally experience some operational challenges as well, since monitoring for suspicious activity may occur in various regions or countries.

The number of technology solution providers visible in the market has increased. Regulators are aware of this trend and as a result are requiring institutions to step up from mere compliance using basic solutions and implement more advanced analytics. Even countries in which basic solutions currently suffice, regulators will soon demand more advanced systems to ensure institutions are compliant.

5 Fraud and Compliance Risk Consolidation?

It is unlikely that fraud management operations and AML compliance departments will consolidate; to be most effective, these groups each need to retain their respective main focus. In the past, an organization's AML compliance group may have sometimes assisted the fraud management group by detecting fraud schemes sooner because AML compliance groups maintain enterprise-wide views of customers.

However, as fraud management operations move toward achieving a customer-centric view, such situations will occur less often. The structure becoming increasingly customary is for both the fraud management and AML compliance groups to report to the same executive-level risk management department as previously noted in the "Fraud Risk Consolidation" section. Moreover, regulatory changes, such as Basel II, are encouraging this type of structure.

The greater opportunity for consolidation between fraud management and AML compliance departments is in technological solutions. Institutions are investing large amounts of money into AML technology. For the most part, they gain no return on investment — only peace of mind for compliance and the avoidance of large fines. Thus, institutions are seeking ways in which to derive value from their AML investments — and extending the technology across the enterprise to attain both fraud management and AML compliance appears to be a natural fit, since both monitor the same data at the same level of interaction.

While technological solutions offering options to extend the AML compliance investment into fraud risk management are beginning to enter the market, there are distinct differences in these areas that must be considered before taking this step.

The first consideration is how quickly the institution needs to respond to the risk. Systems usually operate in one of the following ways: real time, utilizing the risk management techniques to impact an authorization decision by responding to data or input immediately; near-real time, making risk decisions within seconds or minutes of receiving data or input; and batch, analyzing data within longer timeframes, even at the end of the day or the next day.

Within AML systems there is little need to operate in real time. The only areas in AML that require real time or near-real time actions are those necessary to comply with know-your-customer requirements when opening a new account and when authorizing wire transfers. In other situations, AML generally requires only a batch analysis of activity. Transactions generally do not need to be stopped, only reported at a later time. In fact, shutting down accounts at times can cause non-compliance issues. Many institutions also choose not to monitor smaller transactions; for example, transactions under US\$50 carry little risk of money laundering or terrorist financing.

The scenario is entirely different, however, within a fraud management environment. Criminals are often trying to steal as much money as they can as fast as they can. One-time losses at the product level, such as debit cards, can reach thousands to tens of thousands of dollars. At the core account level one-time losses can reach much higher amounts. Therefore, fraud operations must not only be reactive in monitoring, but also be proactive with trends moving from detection to prevention. This requires real time capability to enable fraud management operations to prevent and stop losses. This capability requires the technology to function in a high-volume environment processing tens of millions of transactions per day and to operate 24 hours a day, seven days a week.

Summary

Criminals are constantly modifying their methods and tactics to stay one step ahead of risk management. Governments are attempting to pass legislation to force the financial industry to aggressively and accurately monitor and detect money laundering and terrorist financing activities, demanding an environment of constant fraud and compliance risk management. Nevertheless, institutions must remain flexible both operationally and systemically while adapting to the shifting environment around them.

Although the storms appear poised to reap destruction, the good news is that defenses are available to provide institutions outstanding protection. Like a good weatherman, institutions should use a combination of technology and solid operational practices to effect accurate predictions and realistic results. By implementing common technology to achieve fraud management and AML compliance, organizations can leverage the cost to predict the storm's path and interpret advanced warning signs, providing both hard dollar savings and mandate compliance.

AWP2436 06-05