

We build trust into payment systems, our customers depend on us and what we do.

**Ratna Chandra**  
Technical Consultant, Singapore

# Taking risk management from the silo across the enterprise

An ACI view

Financial institutions face ever-increasing challenges around fraud. Phishing, skimming, hacking – criminals continually dream up new fraud schemes with the intention of staying one step ahead of those trying to combat such tactics. The burden on financial institutions is to protect their customers from fraud, protect themselves from fraud losses and comply with mounting national and international regulations and mandates.

→ By capturing a broader view of customer activity, financial institutions gain a complete understanding of a particular customer's risk profile to better detect and prevent fraud.

The concept of enterprise risk management (ERM) emerged in the early 1990s and is based on the reasoning that to effectively prevent and detect fraud, a financial institution must develop a framework for managing risk across the organization. This includes understanding and maintaining internal controls; ensuring all risks are identified and mitigated in strategic planning initiatives; and underpinning all of this with sound, low-risk operational management at every level and unit and across every business line, account, process, function and role.

ERM also takes a holistic view of a financial institution's relationship with a customer by collectively viewing every product or service the customer uses. This enterprise-wide approach protects financial institutions from fraud at every level, from money laundering activity to identity theft to deposit fraud – essentially any type of fraud that causes an institution or its customer's monetary loss or potentially damages the institution's reputation.

ERM is an evolving process, especially since governments have begun implementing and enforcing standards and regulations that are pushing financial institutions toward ERM. Although many institutions – particularly the large national and international financial institutions – have already adopted ERM approaches, others are still using reactive rather than proactive methods of risk monitoring and detection. Typically, these methods are the traditional silo approaches to fraud risk management and are rapidly becoming insufficient in preventing increasingly sophisticated transaction-based crimes.

Silo-based approaches are reactive and their functions segregated; each silo has its own tools and applications to assist with specific management and reporting requirements. Problems arise because these independent systems do not communicate with one another across business lines.



By capturing a broader view of customer activity, financial institutions gain a complete understanding of a particular customer's risk profile. This expanded view allows institutions to better detect and prevent fraud by monitoring transactions and events across the entire range of customer activity.

A true ERM model provides financial institutions with the architecture to enhance customer service while reducing infrastructure costs through better IT integration and providing a strategic advantage in the future.

### **Threats financial institutions are struggling to abolish**

Identity theft, card number and PIN compromise, white cards, phishing, hacking. The list of fraud challenges financial institutions face grows every year as criminals use more sophisticated methods of deceit. Financial institutions must protect both themselves and their customers from these scams.

Every day, financial institutions suffer losses in a variety of ways. Man in the browser schemes can lead to wire fraud issues. Retail fraud is committed with stolen credit and debit cards or card data collected through skimming – or worse a mass compromise – to create counterfeit cards. Fraud has existed since the day credit cards, debit cards, checks and other payment instruments were invented. Instances of forged checks have been found as far back as the 18th century, and credit card fraud became mainstream in the 1970s as credit card volumes increased.

The volume of fraud has risen year on year, and no matter what controls manufacturers of these products put in place to combat fraud, criminals find a way to defeat them. A good example of this occurred in the late 1990s when card schemes created a unique code in every magnetic stripe; it was impossible for criminals to make counterfeit cards with the codes. So the criminals started using magnetic stripe data from existing cards to make counterfeit cards.





In today's world, institutions and their customers must protect themselves from identity theft and account compromise, which occur through a myriad of methods. Some are as simple as criminals dumpster-diving for discarded mail and papers containing personal information. More sophisticated approaches lure unwitting victims to respond to phishing email messages and provide personal and account information. Hackers ingeniously overcome an institution's security and obtain customer and account information. Criminals in retail situations carry pocket-sized electronic skimming devices and swipe customers' card data at the point of sale. Criminals attach skimming devices to card intakes at legitimate ATMs, as well as a camera to record customers as they key their PINs. This is the only information fraudsters need to create phony debit cards and empty victims' accounts. As the methods become more widespread, the losses increase.

The statistics are staggering: There were 10 million victims of identity theft in 2008 in the United States (Javelin Strategy and Research, 2009). One in every 10 U.S. consumers has already been victimized by identity theft (Javelin Strategy and Research, 2009). 1.6 million households experienced fraud not related to credit cards (i.e. their bank accounts or debit cards were compromised) (U.S. Department of Justice, 2005). Those households with incomes higher than \$70,000 were twice as likely to experience identity theft than those with salaries under \$50,000 (U.S. DOJ, 2005).

Financial institutions understand the importance of detecting and preventing fraud. The potential for loss

is great for everyone involved. The customer loses money, the financial institution loses money; the institution may lose its integrity and reputation, and then it loses its customers.

The financial institutions that avoid these situations are those that have adopted an ERM approach to fraud and treat customers as customers, not as a series of products managed in isolation.

### **The downward spiral of the silo approach**

During the last two decades, silo-based approaches have been the prevailing methodology for transactional fraud risk management. According to the Economist Intelligence Unit survey, 78 percent of financial institutions currently operate under a silo approach.

The silo approach can be applied in many different forms; however, silos traditionally concentrate on how individual business units operate and perform. Each department within a financial institution is responsible for managing its respective channels. For example, within a large financial institution, the credit card channel has sole responsibility for the institution's profits and losses. Therefore, that department's risk management system monitors only a customer's credit card transactions rather than viewing the customer's complete activity across all products.

Under this structure, financial institutions use different products and procedures to manage each channel. A common approach is to create self-contained operational silos based on individual product lines. For example, many

—> **ERM embraces the 'convergence rationale,' effectively integrating individual business silos to form a centralized fraud and risk management framework, enhance internal control procedures and enable greater decision-making capabilities.**

financial institutions maintain two separate and mutually exclusive silos for managing credit and debit cards.

ERM embraces the 'convergence rationale,' effectively integrating individual business silos to form a centralized fraud and risk management framework, enhance internal control procedures and enable greater decision-making capabilities.

Silos also allow gaps in risk control to persist, presenting more disadvantages that produce greater impact to institutions. Comparable silos may operate in different locations of the financial institution, using differing technologies, platforms and software. This leads to significantly higher infrastructure costs as well as duplicated processes, technology and people. Breakthroughs and efficiency gains in one silo may not be passed on to others, and risk management changes can be made to one silo while completely disregarding a customer's relationship with other silos.

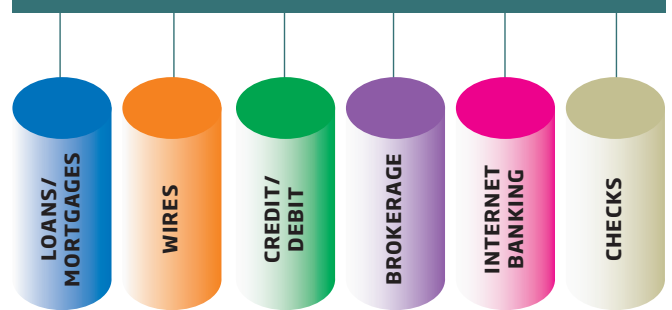
Today institutions face a multitude of differing, risk-driven events stemming from legislation across the globe. A silo approach to ERM, and particularly transaction monitoring, requires implementation changes to be configured at the silo level; thus, the implementations are costly and open to further risks since duplication of effort can lead to mistakes. As legislation such as the Sarbanes-Oxley Act and Basel II becomes increasingly common on a global scale, financial institutions will find operating without an ERM system difficult at best.

Moreover, changes in customer behavior cannot be measured or monitored with a silo approach. If customers change their patterns of spending due to a life event, such as getting married, their behavior could look strange and raise unwarranted suspicion. ERM's view across customer products into a single risk system prevents these false alerts.

### **A holistic, enterprise-wide approach to combat fraud**

In recent years, convergence has been the buzzword in every industry. Businesses gradually began to understand the benefits they could reap by bringing their disparate systems together into a single, cohesive, integrated system that operates more efficiently and effectively. Payments convergence also became a hot topic in the financial industry as financial institutions began to recognize that payments are a commodity business that would cost them profits if they failed to consolidate their infrastructures.

#### **Enterprise-Wide Risk Management Solution**



This same rationale is the driver for a transactional enterprise approach to risk management. ERM effectively integrates individual business silos to form a centralized fraud and risk management framework, enhance internal control procedures and enable greater decision-making capabilities. The key advantage to ERM is that financial institutions can monitor multiple transaction channels across all of their products. This capability is invaluable for profiling customer activity and developing a full, accurate view of each customer.

In today's successful transactional fraud teams, credit, debit, check, automated clearing house (ACH), billpay, internet and telephone banking transactions are all viewed side by side from a single customer perspective. Fraud teams can use their fraud tools to write rules across these disparate transactions, which is a substantial benefit over the silo approach.



Imagine a charge on a customer's credit card suddenly appears in Paris, and the customer has neither prior spending there nor a previous travel-related purchase on the card, such as an airline ticket. The transaction looks suspicious, so the financial institution must call the customer. But a financial institution using an ERM system could discover an airline purchase that was paid via debit card or check. Thus, the institution would know the transaction was authentic and there would be no need to call the customer.

Imagine a different scenario where a customer always uses telephone banking to transfer funds from one account to another. Then one day the fraud ERM system detects that the same customer transferred all of that money via the internet. The view with a silo approach would simply look like a transfer; in an ERM system, however, a transaction departing from a customer's normal habits would be highly suspicious given the customer's behavior profile.

### **The advantages of ERM**

It is becoming impossible for financial institutions to successfully mitigate and prevent fraud without an ERM approach. The operational benefits of ERM are enormous.

The advantages of ERM far outweigh the disadvantages. ERM reduces costs through IT consolidation and enables standardization and flexibility on platform applications. It improves workflow efficiencies and synergies. It increases cross-selling opportunities, service delivery to customers and measurability of the overall customer relationship. It enables institutions to consolidate customer services and offer cross-product, nonfinancial transactions.

The ability to prevent fraud across all products based on the knowledge of what, when and where the customer transacted provides fraud rules engines with information about all transactions a customer performs, allowing financial institutions to write more precise rules with fewer false alerts. These benefits extend to neural network models that institutions use to profile patterns of customer behavior.

ERM also enables financial institutions' units to share knowledge and best practices and support regulatory compliance at an enterprise level. A discovery in a particular channel is quickly and simply copied to the other channels, thereby ensuring a simple transfer of best practice within the team.

However, the compelling view must be that financial institutions need to treat customers in the same manner in which customers view their relationships with their financial institutions. If customers use multiple products, then they do not see their financial institutions as providers of credit cards, debit cards and mortgages; they see them as providers of holistic banking. And this is how financial institutions should regard their customers from a risk perspective.

A sound transactional ERM solution is fast becoming a competitive advantage in an industry that has always believed none existed. If financial institutions can successfully integrate all the information into their ERM strategies, then the criminals may just try to steal from somewhere else.

—> **The advantages of ERM far outweigh the disadvantages. ERM reduces costs through IT consolidation, enables standardization and flexibility on platform applications, and improves workflow efficiencies and synergies.**



## **ACI Worldwide**

Offices in principal cities throughout the world  
[www.aciworldwide.com](http://www.aciworldwide.com)

Americas +1 402 390 7600

Asia Pacific +65 6334 4843

Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide 2011

All rights reserved. All product names are trademarks or registered trademarks of their respective companies. ACI and the ACI logo are trademarks or registered trademarks of ACI Worldwide or its subsidiaries in the United States, other countries or both.

ATL4572 02-11

## **About ACI Worldwide**

ACI Worldwide powers electronic payments for financial institutions, retailers and processors around the world with the broadest, most integrated suite of electronic payment software in the market. More than 75 billion times each year, ACI's solutions process consumer payments. On an average day, ACI software manages more than US\$12 trillion in wholesale payments. And for more than 150 payments organizations worldwide, ACI software ensures people and businesses don't fall victim to financial crime. We are trusted globally based on our unrivaled understanding of payments and related processes. We have a definitive vision of how electronic payment systems will look in the future and we have the knowledge, scale and resources to deliver it. Since 1975, ACI has provided software solutions to the world's innovators. We welcome the opportunity to do the same for you.