



We're working with more than 150 organizations around the world to help them protect their customers, giving us a real insight into the fraud threats institutions face - and the tools to protect them.

Werner Liebenberg
Account Manager, Johannesburg

Managing risk in wholesale payments: Operational, liquidity and fraud

Mitigate risk with ACI Money Transfer System™ and ACI Proactive Risk Manager™

Risk is a central ingredient of the business of banking. In the process of providing financial services, banks assume various kinds of risk, which need to be identified, managed, controlled, and, where appropriate, mitigated by a combination of pricing and product design.



Managing risk in wholesale payments: Operational

The globalization of these financial services and the increasing sophistication of financial technology, mean that the risks of today are more complex and far-reaching; and the recent market turmoil, and the apparent fragility of some banking entities, have highlighted in a dramatic way the critical nature of some banking risks.

Payments, being at the very heart of a commercial bank's activities, are certainly not immune to these forces. There is a growing realization that the risks associated with payments processing do have the potential to become substantial, yet banks can take advantage of the sophisticated tools now available to help them manage these risks in a proactive manner.

Operational risk

Operational risk has many definitions, but at the core of it is the risk of loss resulting from the inadequacy or failure of internal processes, people and systems.

In the payments world, the substance of this is exacerbated by the deployment of more highly automated technology in globally integrated systems, which has the potential to replace the risks of manual processing errors with the risk of system failure.

In addition, the fact that certain banks are now setting themselves up as large-volume service providers in payments, perhaps through mergers or by acquisition, means that internal controls and the resilience of systems must be of the highest order.

Operational resilience is a 'sine qua non' for payment banks, and this begins with robust funds transfer processing software, and high-availability hardware and software. This resilience is now a regulatory expectation, not just a prudent business decision, and should lead to an increase in day-to-day processing efficiencies.

For example, the Basel II Capital Accord requires banks to focus in a formalized, comprehensive manner on the operational risks that can result from external influences.

Any investment in improved contingency procedures and approaches should be reflected in a reduction in the need for operational risk capital, and this should provide banks with the incentive to invest in new systems and practices to reduce the potential for serious losses from operational risk.

In terms of payments, the potential loss events to be guarded against include:

- Unauthorized activity (transactions unauthorized or not reported)
- Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients
- Product flaws and defects
- Exceeding client exposure limits
- Losses arising from disruption of business or system failures
- Losses from failed transaction processing or process management (data entry errors, missed deadlines, system misoperation, accounting errors, delivery failures, reference data maintenance)
- Failed mandatory reporting obligation
- Outsourcing and vendor disputes
- Internal or external fraud
- Improper business practices (money laundering)

None of this, of course, is new. But now, the mitigation of operational risk will be influenced to a very large extent by the effectiveness or otherwise of internal systems and control over the use of technology. More than ever, payments processing functions, capacity and connectivity issues are under the spotlight.

→ More than ever, payments processing functions, capacity and connectivity issues are under the spotlight.

The ACI response to operational risk

ACI Money Transfer System™ complements a financial institution's risk protection strategy by providing a systems solution which encompasses and addresses business critical areas of operation. The key focus areas of the Money Transfer System solution relevant to operational risk are:

Business continuity: Providing a solution that is able to recover quickly from the complete loss of a primary operations site

Business management: Providing a solution where financial transaction activity is managed within institution-defined credit limits, liquidity thresholds, processing rules, and security procedures

Ongoing compliance: Providing a solution that incorporates all regulatory requirements applicable to the markets in which the institution operates, for example conformity with OFAC rules

Operational resilience: Providing a robust and scalable architectural solution, ensuring the maximum throughput of transactions

Money Transfer System provides various monitoring capabilities to enable institutions to manage operational risk. Screens are designed for maximum user efficiency while guarding against operator errors with field edits and verifications. User profiles and privileges allow a breadth of segregation by function or task without hindering workflow. All of the options for processing and workflow are highly configurable to place control with the financial institution.

Money Transfer System employs multiple mechanisms to ensure availability and reliability. The software is designed to minimize points of failure and costly downtime. Alarms alert operators to system problems, and the state-of-the-art Remote Hot Standby™ (RHS®) module provides a redundant business recovery system. Central to a disaster recovery strategy is the ability to continue processing on a back-up site following loss of a primary site, with minimum interruption and no loss of data. RHS is a unique and proven business continuity solution that ensures complete data protection, and a fast recovery time.



SWIFT, the member-owned cooperative that provides the communications platform to connect over 8,500 banking organizations, securities institutions and corporate customers in more than 200 countries, achieves system availability of 99.999%. Money Transfer System banks are able to match that level of resiliency.

The review of messages by interdiction rules is commonplace at financial institutions in managing operational risk. Money Transfer System provides two functions, STOP and monitor, to evaluate messages and prevent further processing. The STOP filter is an additional optional component of Money Transfer System employed to immediately block payments and prevent them from leaving the financial institution. The STOP database accepts lists (for example from government and regulatory agencies) as well as manually maintained STOP tokens and phases, and Money Transfer System can readily interface with other external tools for a broader enterprise solution.



Managing risk in wholesale payments: Liquidity

Liquidity risk

Although managing liquidity has always been one of the most important services offered by banks, it has become a key concern as evidenced by the recent liquidity shortage associated with the banking crisis. The ability to provide liquidity to customers is a crucial activity, on which many bank activities depend either directly or indirectly. Until the global financial crisis, many banks considered their liquidity management to be fairly efficient. But the crisis has thrust liquidity management back into the limelight, particularly in the context of changing regulatory requirements.

Moreover, banks' corporate customers have also been impacted by the global slowdown and are looking to their banking partners to enable better, more up-to-date information for tracking payments as well as reporting for intra-day liquidity management. For example, corporate customers need to be able to specify which high-value payments must be made immediately and which can be delayed, what their positions are and how any excess cash should be invested. As such, these demands for increased functionality are now adding extra pressure on banks on top of basic regulatory compliance.

Defining liquidity

Essentially, liquidity refers to 'the ability of a bank to fund increases in assets and to meet obligations as they become due, without incurring unacceptable losses'. At the most basic level, this involves the bank ensuring that it has a wide range of deposits which can protect against liquidity shortfalls.

The management of liquidity has evolved over the years as the complexity of financial activities has grown. Banks and their regulators have increasingly recognized the link between sound liquidity management and the reduced probability of banking failures.

As a result of these tighter risk management requirements, the Basel Committee on Banking Supervision Report of September 2008 specified 17 clear liquidity principles that it expects banks to implement "promptly and thoroughly". The principles can be broadly divided into governance of liquidity risk management,

measurement and management of liquidity risk, public disclosure and the Role of Supervisors.

Banks now need to manage liquidity on an intra-day basis, as opposed to a daily basis, as failure to complete time-critical payments could have major repercussions across markets.

Intra-day liquidity management and multiple liquidity positions

A growing number of emerging payments systems are affecting liquidity in ways not experienced in the past. The introduction of initiatives such as Continuous Linked Settlement (CLS), U.S. CHIPS finality and U.K. Faster Payments drastically changed the landscape. For example, until the launch of the U.K. Faster Payments scheme, banks conducted their settlement overnight. However, now the real-time payments mechanism for person-to-person transactions means that those banks offering the service must conduct settlement up to three times a day, which has a further effect on liquidity.

Banks are increasingly operating across borders and in multiple locations, which has an impact on their liquidity management processes. Many banks now need to manage multiple liquidity positions across different currencies. In addition, while the introduction of the Euro means that European banks can manage liquidity in a single currency, this further adds to the complexity as new clearing systems are implemented but the consolidation and retirement of old systems is slow to progress.

In this environment, banks must now consider several major issues, such as how to manage liquidity within each system in the most cost-efficient way, how to transfer liquidity from one system to another, and how to choose the best trade-off between liquidity and transaction costs among the various payments systems.

In order to manage liquidity effectively, a crucial component must be good management information. Banks need a global view of liquidity positions across all of the currencies that they process and the major clearings in which they participate at both the bank and customer level. Moreover, this information must be provided in



Our software continues to underpin electronic payments in retail and wholesale banking and commerce, all the time, without fail.

Christine Moore
Executive Assistant, New York, U.S.A.

—> Many banks are beginning to realize that managing the flow of money in and out of the bank in a global environment can be a significant competitive advantage.

real time, as they need to be able to track payments and risk exposure on a minute-by-minute basis. In addition, banks need to manage liquidity to an intra-day, real-time position, while still forecasting end-of-day and collateral positions. Finally, banks need to control the release of payments based on actual and projected balances, ensuring that liquidity is optimized in order that costs are controlled.

Liquidity management has also begun to impact new parts of the bank. For example, the interaction between clearing and settlement mechanisms has become more prevalent, and the distinction between Real-Time Gross Settlement (RTGS) and automated clearing house (ACH) is becoming less obvious. Many of the liquidity concerns which had previously been restricted to the realm of RTGS are now beginning to be felt in ACH and 'retail' clearing and settlement systems. Therefore, liquidity management is now required across a greater range of payments processes.

Owing to its far reaching consequences, liquidity management has become critically important both internally and externally to the banks. Banks must be aware therefore that their own liquidity management is no longer an issue

just for them and their customers, but also an issue for the greater world community. The effect of poor liquidity management in one financial institution can spread all too rapidly in the global banking community, as has been highlighted by the recent global financial crisis. This is where improved regulation could help to safeguard against similar events in the future.

While regulatory pressures and market developments are ensuring that liquidity management is of increasing importance, many banks are beginning to realize that managing the flow of money in and out of the bank in a global environment can be a significant competitive differentiator. Banks that offer additional services to their corporate customers that enhance liquidity management will have a significant competitive advantage as this continues to take priority. In addition to ensuring that banks are prepared for future regulatory compliance, this should contribute significantly to safeguarding their future.

The ACI response to liquidity risk

Within ACI Money Transfer System, extensive tools are provided that enable the bank to maximize its utilization of available liquidity with minimal manual



input. The extensive configuration options allow the bank to move toward a highly automated process of liquidity allocation that will manage most of the day-to-day routine payments traffic. Such typical payment flows can be captured within the solution, and the information can be made available to an external reporting or other bank system, when analytics can assist in identifying any patterns or other characteristics.

In addition, to assist the bank to meet the demands of its customers for more payment information for their own liquidity management purposes, 'Payment Tracker' within Money Transfer System leverages the power of a single unified payments data store, one that provides users with a single view of all payments – allowing the bank to leverage payment data it already has and deploy that to a much wider audience.

Money Transfer System, with its intra-day multi-currency position-tracking functionality, can be used as a transactional repository for intra-day liquidity. With this approach, it serves as a liquidity transaction engine, accumulating all transactions and expected transactions that affect liquidity from a variety of back-office applications at the bank.

The projected and actual liquidity can be illustrated on a time-generated time line in real time, allowing the user to clearly see the indicated pattern of liquidity flows, and projected liquidity based on the time parameter using actual and anticipated transactions.

Finally, all liquidity positions, either on an individual currency basis, or on a consolidated aggregate basis, can be expressed in terms of a chosen single base currency, using a defined book or exchange rate.

Optimization of liquidity is challenging even in an easily predictable environment. Capital costs preclude holding excessive liquidity, while unpredictable events and business drivers produce asymmetric flows. The key to maintaining a balance between the diminishing returns of excessive liquidity and service failure because of uncovered short excesses is to utilize the real-time reporting and forecasting features of Money Transfer System so that intra-day positions can be monitored and positions forecast.



Managing risk in wholesale payments: Fraud

Fraud risk

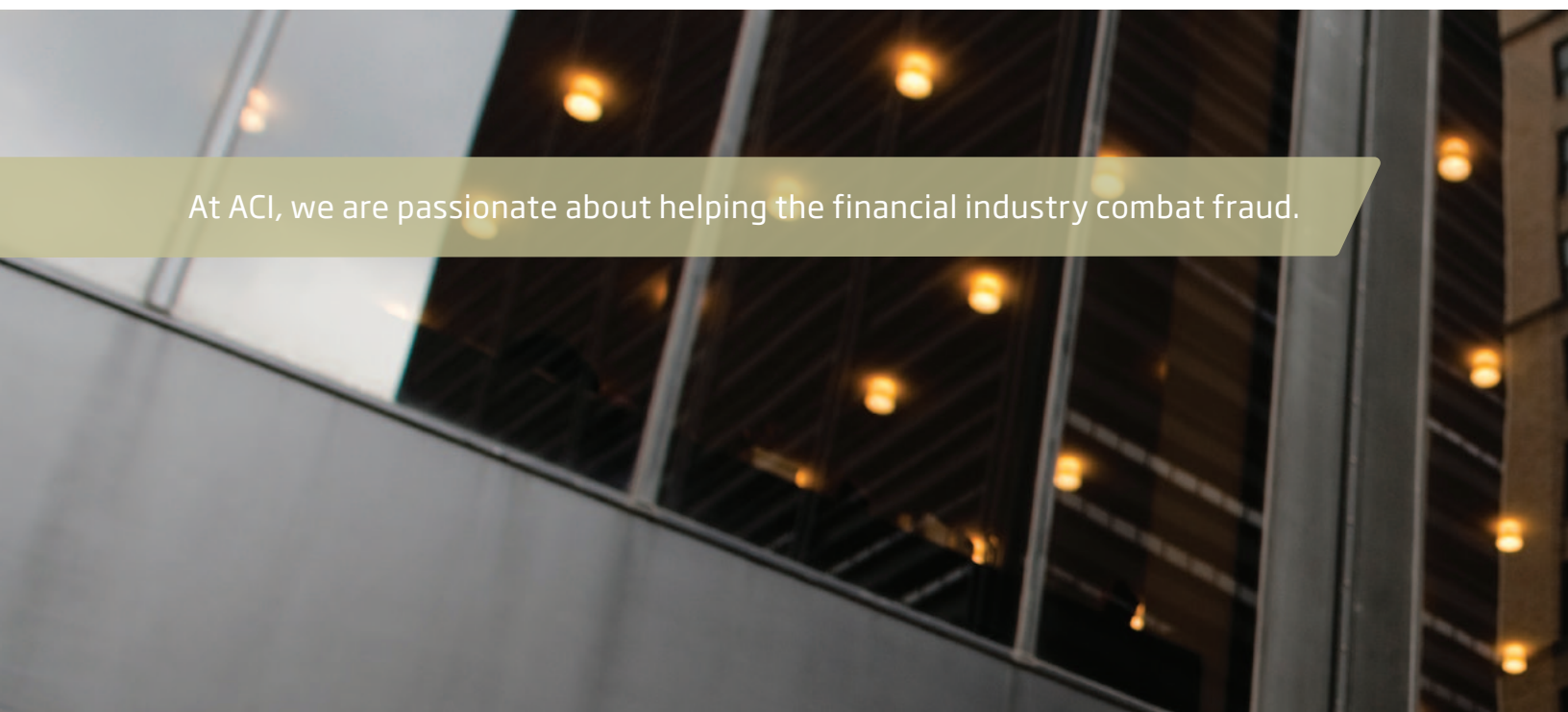
Financial institutions face ever-increasing challenges around fraud. Phishing, skimming, hacking – criminals continually dream up new fraud schemes with the intention of staying one step ahead of those trying to combat such tactics. The burden on financial institutions is to protect their customers from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

On top of this there is further pressure from customers and regulators forcing banks to improve the speed at which a payment reaches the beneficiary's account. Many countries are moving to a real-time or near-real-time process. For example, the U.K. has launched its Faster Payments initiative, which effectively reduces payment times between different banks' customer accounts, from three working days using the existing ACH system, to near real time.

From a customer perspective, the ability to send and access funds in this way provides significant benefits in terms of convenience and financial management. Unfortunately, the rapid availability of funds makes the U.K. online banking system an attractive target for criminals - especially since other initiatives, such as 'chip and PIN', have limited the ability to make fraudulent card transactions.

Although traditionally one of the more secure environments within a financial institution's operations, wire transfers pose perhaps the single greatest risk of loss to a financial institution. The speed with which losses can occur, the potential size of such losses and the lack of ability to recover funds once they are transferred to the destination institution all leave financial institutions vulnerable to criminal attack.

To fully understand the risk that exists in wire transfers, it is important to analyze the origin of the wire. Many financial institutions enable customers (businesses and



At ACI, we are passionate about helping the financial industry combat fraud.

Reducing fraud risk from wire transfers

There are a number of measures that a financial institution may take in their efforts to reduce such risk of fraud.

- Screen for wire activity that is not typical for the specific customer, and which breaches a customer's historical averages (amounts, frequency, etc.).
- Screen for wire activity on new accounts following large deposits.
- Screen for wire activity on accounts that have previously been dormant.
- Screen for wires sent to bank secrecy haven countries.
- Screen for wires sent after critical account settings are changed, such as changes to passwords, changes to call-back telephone numbers, or adding "authorized" wire initiators, etc.

consumers) to initiate wire transfers in-branch, over the phone or online. Each of these methods contains risk, although some more than others.

In general, wire transfers originating from branch locations are the least risky of all, as fraudsters are generally reluctant to put in a personal appearance. Despite this, it is important that branches have a documented authentication process, including requirements for multiple forms of ID or signature verification.

Financial institutions usually require individuals initiating a wire transfer request over the telephone – typically corporate customers – to be authorized to initiate wires on behalf of the company for the particular accounts. These individuals must be able to provide appropriate security codes or correctly answer previously established security questions. Yet, internal employees, both within the bank and the corporate, may gain access to account information and passwords to overcome such security barriers.

Similarly, financial institutions that enable customers to initiate wire transfers online open themselves to risk by fraudsters who are able to circumvent online authentication measures, whether by deploying a Trojan or some other type of computer malware to steal login and password information, or by performing man-in-the-middle or man-in-the-browser attacks. Multifactor



Matthew Richter
Senior Financial Analyst, New York



authentication – such as tokens, one-time passwords, keystroke identification, IP profiling, etc. – reduces the risk of online banking wire fraud. However, deploying multifactor authentication on a wide scale is costly, and criminals continue to develop techniques to circumvent strong user authentication.

The ACI response to fraud risk

Criminals are continually modifying their methods and tactics to commit fraud against financial institutions as well as to launder illicit funds. Wire transfer operations, although traditionally one of the more secure environments within a bank, may be exposed to the greatest risk of loss within the financial institution.

However, steps can be taken to further secure wire operations and protect against fraud and money laundering. By using a fraud detection system that analyzes wire transfer transactions in real time and near real time, financial institutions can augment current processes and resources to screen for high-risk activity and take action – often before the money leaves the bank.

Financial institutions worldwide use ACI's solutions and services to mitigate loss associated with criminal activity that spans the enterprise – including wire transfer operations. ACI Proactive Risk Manager™ enables organizations

to take an account-based view of risk, which allows analysts to defend against criminal activity at all transaction channels – ATM, POS, checks, ACH, teller and wire – as well as across all accounts at the customer level.

Proactive Risk Manager's ability to accurately identify fraud across the customer relationship allows users to recognize fraudulent behavior more quickly and efficiently. The solution's ability to identify changes in customer behavior patterns across multiple accounts helps fraud operations rapidly recognize attacks from fraud schemes, such as identity theft, phishing, account takeover fraud and money laundering. It thus helps financial institutions detect suspicious activity that may impact their customers' accounts, and stop fraud from occurring in real time. ACI software utilizes a combination of predictive analytics and user-defined rules to stop fraudulent activity in milliseconds – within the transaction authorization path. And, intuitive cross-channel case management capabilities support fast and effective investigations.

Proactive Risk Manager users have realized significant operational efficiencies enabling them to prioritize and analyze alerts faster – increasing the capacity of fraud cases worked by optimizing existing fraud resources, while lowering overall fraud losses and associated handling costs.



ACI Worldwide

Offices in principal cities throughout the world
www.aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide 2010

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 Corp. in the United States, other countries, or both.

ATL4427 11-10

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.