# Enterprise Fraud Management with ACI Proactive Risk Manager on IBM System z

Redguides
for Business Leaders

Alex Louwe Kooijmans
Rob Haake
Jim Goethals
Ethel Richardson
Dino Quintero

- The need for enterprise fraud management
- An overview of ACI Proactive Risk Manager
- Exploiting System z strengths and values with PRM

# Executive summary

Financial services institutions face a variety of challenges in the area of cybercrime. The risk is not limited to direct fraud losses either. Financial crime also affects an institution's ability to protect and retain customers, and makes it more difficult to comply with complex national and international reporting requirements.

Even while the amount of fraud is on the increase, the forms that it takes are continually changing as fraudsters become more clever at inventing schemes and exploiting technology. Staying ahead of the criminal element is a daunting task for fraud managers. The challenge is further complicated by the trend within the financial sector to constantly add delivery channels and increase the products and services offered to customers. That trend, combined with the common occurence of mergers and acquisitions, tends to increase the complexity of the IT landscape in which fraud monitoring must take place and is often mirrored within fraud departments, where different teams and systems deal with different types of fraud and different lines of business. The lack of a comprehensive view of each customer's activity across all channels makes the detection of abnormal (fraudulent) transactions more difficult.

ACI Proactive Risk Manager is an enterprise fraud management solution that helps financial institutions detect and react to fraud. It gives users the ability to be as fast and agile in responding to fraud as the criminals are in committing it. Proactive Risk Manager uses sophisticated analytics, easily configured by the user, to target fraud with precision, prioritize alerts, and manage fraud cases. It can be integrated with a vast number of backend systems and processes, provides a holistic view of customer activity.

IBM® System z® is an ideal platform on which to run ACI Proactive Risk Manager. System z offers the performance, security, scalability, and configurability to support and enhance PRM's capabilities. System z already has earned a prominent place in the financial services sector; many financial institutions use it to run their core banking transaction systems. PRM easily exploits the strengths of System z.

This guide provides details about how ACI Proactive Risk Manager on IBM System z can help you to meet the challenge of enterprise fraud management. The two companies each bring a proven track record to this effort, and their combined expertise is unmatched.

# The importance of enterprise fraud management

Financial institutions face common challenges in today's rapidly changing risk landscape. How do you best protect customer relationships from fraud, especially given the number of third-party data breaches, phishing incidents, and malicious code attacks? How do you identify complex cross-channel fraud and stop it quickly? How do you prevent payment fraud in real time before losses occur?

These are daunting tasks for many fraud managers, and the challenge is intensified by the fact that most financial institution fraud departments remain in silos. Typically, financial institutions have supported each new delivery channel and, sometimes, each new product or service, with its own fraud system, often on its own IT infrastructure. This, combined with the recent flurry of M&A activity, has meant that banking systems can be a confusing mixture of different application systems and technologies. This approach has been mirrored within fraud departments where different teams and systems deal with different types of payment fraud. Card fraud teams are often isolated from teams dealing with other types of fraud conducted via different payment tools or access points - such as Internet banking, ACH, or wire.

This makes it difficult to gain a comprehensive overview of customers' payment patterns or to identify fraud that crosses payment types. In a case of account takeover as a result of phishing, a fraudster who goes online and changes the account address and then requests a new card to use for fraudulent purchases may not be picked up within a siloed system. The address change may be viewed by one team and the card transaction by another team. In isolation, this may appear to be normal activity, but when combined, its abnormal nature is evident.

This chapter addresses trends in enterprise fraud management, including why now, more than ever, financial institutions are turning to an integrated risk management framework to better protect customers from fraud.

## Market trends in enterprise fraud

Reigning in payments fraud continues to be a challenge for financial institutions across the world. In addition to commonly known fraud types, such as card skimming and the ensuing counterfeit or card-not-present fraud, financial institutions are dealing with new sources of fraud. As new banking channels have opened up and grown in popularity, and the use of credit and debit cards has risen, fraud has evolved both in its sophistication and scope.

Cross-channel fraud has increased in complexity and significantly impacts financial institutions both in terms of increasing fraud losses as well as negative impact to customer satisfaction. Much of the increase in cross-channel fraud can be attributed to the increase in data breaches, phishing attacks, malicious code attacks, and skimming events that have compromised sensitive card-based and identity-related information for millions of banking customers. Armed with sensitive account and identity information, an increasingly sophisticated network of global criminals develop innovative methods to target debit and credit cards, ACH, check, and wire transfer activity occurring at a POS, ATM, or branch, or by phone or online.

By targeting their attacks across banking silos, fraudsters have been able to evade many traditional fraud detection countermeasures. And, by striking quickly, many fraud rings are scamming financial institutions out of millions of dollars in a matter of minutes.

## Why enterprise fraud management now

Financial services institutions are facing increasing pressure to cut costs and ensure maximum return on investment, particularly in the current economic environment. Yet these institutions must continue to focus on introducing anti-fraud strategies. Indeed, 2009 research into financial crimes conducted by Datamonitor reported that despite efforts to combat fraud, the global financial crisis could accelerate a wave of financial crime, with the financial institutions being the main targets for criminals.

Not only does an increase in financial crime impact the bank in terms of direct fraud losses, it also impacts their ability to retain customers. A 2009 ACI Worldwide survey of more than 2,400 consumers across eight countries found that if an individual or someone they knew was impacted by fraud, 22 percent would change financial institutions, and an additional 27 percent would consider changing financial institutions. For information on the survey results, and to download a guide on stopping card fraud, refer to the following Web site:

http://www.aciworldwide.com/stopcardfraud

In order to protect themselves and their customers against potential fraud attacks, financial institutions need to find ways of implementing more effective anti-fraud strategies while increasing efficiency and keeping costs to a minimum.

One obstacle to efficiency usually takes the form of individual silos for different payment channels and types, such as check and card, performing similar functions. This approach, illustrated in Figure 1 on page 5, leads to an inefficient use of technology, applications, and staff across the organization.

With a centralized enterprise fraud management strategy, financial institutions can better integrate siloed hardware and software fraud systems to reduce the risk of fraud while benefiting from more efficient operations.

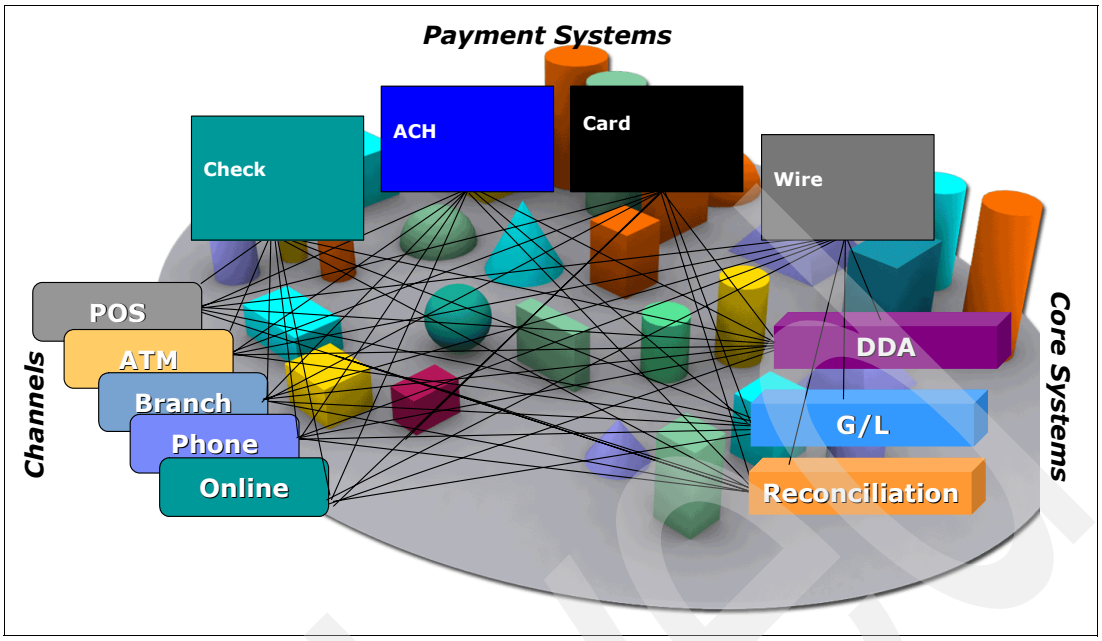


*Figure 1 Typical financial institution payment environment (simplified)*

Enterprise fraud management systems deliver significant return on investment (ROI) by providing streamlined systems and tools to increase analyst efficiency, improving cross-channel clarity to detect more sophisticated fraud, and eliminating redundant systems that drive up maintenance costs.

# Key considerations for enterprise fraud management

There are multiple factors and criteria that financial institutions should look for when choosing an enterprise fraud detection system:

## Fraud detection system agility

- Does the system utilize predictive analytics and user-defined rules to adequately stop fraud fast and to target fraud with precision?
- Does the system provide the ability to prioritize alerts and manage fraud cases efficiently?
- Does the system easily incorporate enterprise-wide transactions and demographic data to provide a holistic view of customer activity?
- Can the fraud system cost effectively integrate and perform with a multitude of related backend processes and systems?

## Real time fraud detection and blocking capability

- Does the system stop fraud in real time, within the authorization process?
- Is the hardware and software optimized to allow for the greatest level of real time analysis, but also accommodate near real time and batch processing?

## System scalability and availability

- As transaction levels increase or as merger and acquisition activity occurs, can the system handle a dramatic increase in scale?

- Is the system reliable and available during global banking hours and during known peak periods?

### Proven expertise

- Is the system proven in handling high-volume card, ACH, check, and wire activity occurring at a POS, ATM, branch, by phone, and online?
- Does the solution provide a strategic framework for payment processing and payments security?

The next chapter provides details on how PRM addresses the trend toward increased fraud in the financial services sector and heightened customer requirements to reduce losses due to fraud exposures.

# How ACI Proactive Risk Manager addresses financial crime trends

Financial institutions face ever-increasing challenges related to fraud. Data breaches, phishing incidents, malicious code attacks—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 losses due to financial crime, and comply with mounting national and international regulations and mandates.

In this chapter, we introduce the ACI Proactive Risk Manager solution, which is used by more than 150 customers worldwide, including half of the top 20 global banks. ACI Proactive Risk Manager helps financial institutions, card issuers, processors, and merchant acquirers detect suspicious activity that may impact their customers' accounts, and stop fraud from occurring in real time.

## What is ACI Proactive Risk Manager

ACI Proactive Risk Manager (PRM) is a complete fraud detection solution capable of managing risk across a financial institution's business lines and customer accounts. PRM combines the power of predictive analytics and expertly defined rules to provide fast, accurate, and flexible response to the growing and evolving world of financial fraud.

Through its custom neural network technology, ACI Proactive Risk Manager compares the characteristics of each customer's activity with the custom fraud model and recorded patterns of behavior for every account holder it sees. It then assesses and scores the risk in real time or near real time for each transaction using a variety of advanced algorithms, parameters, and accumulated statistics. In addition, ACI Proactive Risk Manager provides reviewers with precise reasons for the score, improving transaction analysis.

ACI Proactive Risk Manager provides comprehensive workflow management capabilities to fraud analysts, with expert rules-based strategies at the core of this process. This component builds on the fraud expertise of the staff by allowing the creation of real time rules. Transaction activity matching a rule generates alerts, which are delivered to reviewers via an intuitive

business user interface. A comprehensive set of tools enables supervisors to direct workflow and manage reviewers. ACI Proactive Risk Manager captures and maintains statistics on fraud savings and losses, as well as on reviewer and model performance, to provide valuable management information.

ACI Proactive Risk Manager interfaces with a number of ACI Worldwide products, including the ACI Automated Case Management System, BASE24, BASE24-eps and the ACI Money Transfer System. Proactive Risk Manager also integrates with any authorization and bank host system.

Figure 2 depicts the PRM process flow.

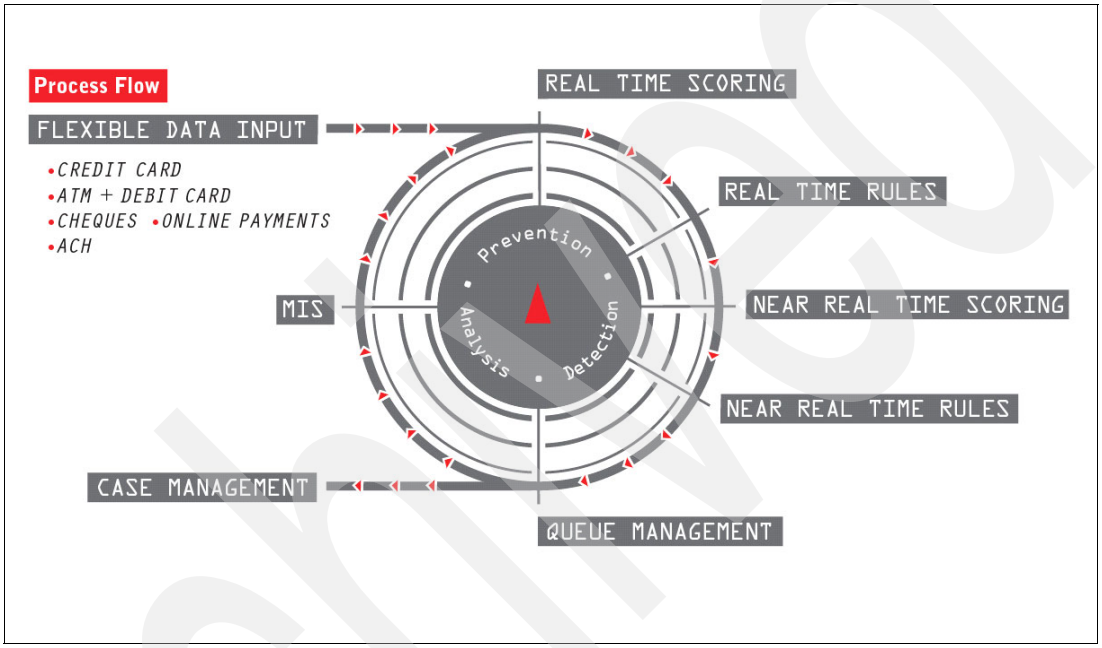


*Figure 2 ACI Proactive Risk Manager process flow*

## Functional components of ACI Proactive Risk Manager (PRM)

As shown in Figure 3, PRM provides the following functional components:

- PRM interface
  - Standard API
  - Support for all types of financial and non-financial transactions
  - Accepts externally generated alerts to integrate with legacy applications
  - Real time, near real time, and batch feeds
- PRM scoring engine
  - Benchmark neural network fraud model
  - Utilizes a 30-day customer history file (The length of the customer history file is configurable. ACI Worldwide recommends at least 30 days.)
  - Produces fraud scores from 0 to 999 based on complex analysis defined by the business
  - Real-time and near-real-time scoring
  - Custom neural modeling

- PRM analysis and review system
  - Flexible scripting engine
    - Real-time fraud prevention or near-real-time detection
  - User interface and historical database
    - Client access - Robust enterprise-wide demographics data, Web-enabled Graphical User Interface (GUI)
    - Workflow management and managerial controls
  - Enables extensibility to external systems

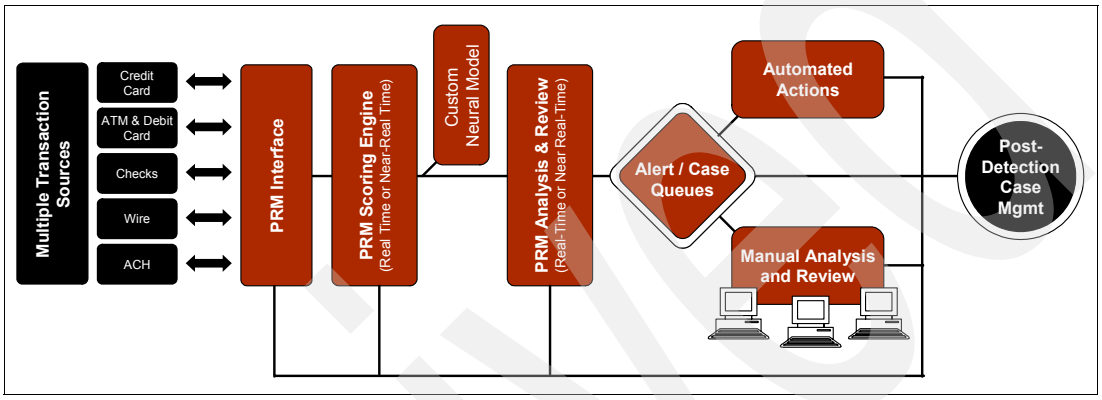


*Figure 3 PRM functional components*

# Advantages of ACI Proactive Risk Manager for addressing financial crimes

The following sections describe the advantages of PRM for addressing financial crimes.

## Fraud detection system agility

ACI Worldwide has established leading, global expertise in helping financial institutions on their journey to centralize high-volume card, ACH, check, and wire activity occurring at a POS, ATM, branch, by phone, and online. ACI Proactive Risk Manager offers advanced functionality, unmatched flexibility, and user control to detect virtually any type of fraud or money laundering scenario.

Customers can write rules that evaluate neural scores, transaction conditions such as countries, MCC codes, entry types, and so forth. If necessary, customers can choose to have some of their rules automatically block highly suspicious activity until an analyst has a chance to review it. Additionally, Proactive Risk Manager users can keep up with evolving fraud trends by deploying rules on the fly.

Rules can also reference customer profile tables, which could be used to capture data such as preferred ATM locations, frequency of cross-border activity, largest ATM withdrawal amount, historical online usage patterns, and so forth. One ACI Worldwide customer utilized customer profiling to reduce alerts by 40% while increasing their fraud detection rate to 85%.

ACI Proactive Risk Manager provides the ability to analyze common point of purchase activity for fraudulent transactions and determine point of compromise locations. Once a point of compromise is detected, analysts can take proactive steps to block or watch future activity.

ACI 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. One top five bank in the U.S. reported a 66% decrease in keystrokes, enabling their analysts to increase the efficiency of working fraud alerts and cases, reducing overall fraud losses.

### Real-time fraud detection and blocking capability

ACI Proactive Risk Manager works seamlessly with ACI Worldwide's payment engines and integrates with every authorization and bank host system to provide in-flight, real-time fraud prevention. The system utilizes a standard enterprise input process that is a mechanism for feeding data into ACI Proactive Risk Manager from external sources. This interface also serves as the mechanism for returning fraud scores and transaction response actions to the originating systems when used in a real-time mode.

### System scalability and performance

ACI Proactive Risk Manager has been proven to be a scalable, high performance solution, with customers monitoring over 13 million accounts and processing over 700 transactions per second.

### Proven implementation track record

Customers benefit from a fast implementation – typically around 12 weeks for the base system (depending on customer requirements). ACI Proactive Risk Manager consultants work with customers to tailor the system to satisfy each customer's unique requirements. ACI Worldwide has a proven track record for on-time, on-budget projects.

### Proven expertise securing payments

For 13 years, leading financial institutions have relied on ACI Worldwide for fraud and anti-money-laundering monitoring solutions. ACI Worldwide has over 150 clients worldwide using PRM, including - half of the largest 20 global banks. ACI Worldwide's online payment processing systems have been the industry standard for nearly 30 years. No competing risk management provider can match ACI Worldwide's expertise in high volume, high value, real-time payments.

## Compelling return on investment

Given the banking environment today, any investment in any type of technology has to have a compelling ROI. Most ACI Proactive Risk Manager customers realize their ROI in a matter of months.

The ROI for ACI Proactive Risk Manager is built on these three components:

- Stopping more fraud faster through system agility, more granular rules, customer profiling, and real-time blocking.
- Improving analyst efficiency, thus enabling each analyst to work more fraud cases, and prioritizing alerts more effectively to resolve the most risky cases sooner.
- Reducing costs by consolidating siloed fraud detection systems and by moving from an expensive consortium neural net to an effective custom neural network.

# Benefits of running the PRM solution on IBM System z

Financial institutions are focusing more and more on consolidation and integration of resources to save money (cut costs), prevent fraud, reduce risk, protect customer loyalty and brand image, and comply with regulatory agencies. There are real benefits in terms of costs savings, improved efficiencies, and growth flexibility for financial institutions that consolidate their fraud management framework onto a centralized enterprise fraud management system hosted on the enterprise-scale IBM System z mainframe.

## Infrastructure requirements to meet business demands

The underlying IT infrastructure for a payments fraud detection hub must meet specific requirements to support an enterprise risk management system. IBM System z provides a cost-effective technology platform that exceeds these requirements, which can be summarized as follows:

- System agility and operational efficiency to minimize cost and maximize fraud detection
- Scalability and performance to address fluctuating business challenges
- Application availability to protect customer loyalty and brand image
- Superior transaction processing heritage

The same benefits that characterize PRM—system agility, operational efficiency, scalability, high performance, a proven track record, and excellent return on investment—also apply to the System z platform. This chapter describes specifically how the key features and strengths of System z map to the demands of ACI Proactive Risk Manager.

# System agility and operational efficiency to minimize cost and maximize fraud detection

An “agile system” is one that is fast, adaptive, and efficient. These qualities can be achieved by the tight integration and optimization of PRM on IBM System z, which maximizes the use of the available data resources, allows efficient access to associated application systems, and exploits the technology benefits of the hosting System z platform. Specific examples of this synergy follow.

- Collocating PRM scoring and authorization engines on System z effectively eliminates network latency and costs. High volume systems can waste precious time waiting for data transfer, shrinking the effective analysis window, whereas with zero latency on the mainframe, the client can experience increased throughput potential along with increased range of real-time processing capability. This increased potential can also provide a wider processing window to handle all the rules the client needs to process in their response time window.
- Taking a broader perspective, another major advantage of IBM System z is the tight integration of data among multiple applications using shared resources such as memory, buffer pools, and databases. All inter-process communications are achieved through the use of the internal messaging queues. This is an important example of how BASE24-eps and PRM leverage the sharing and availability capabilities of the System z Parallel Sysplex® clustering technology. Shared messages are not sent over an external network link, but travel over internal memory within the same logical image (LPAR) or pass among other logical images using the memory speed HiperSockets™ virtual TCP/IP connections, thereby reducing or eliminating inter-process latency.
- Today, many financial institutions run their enterprise-wide core banking transaction systems on IBM System z. PRM and core banking systems can both benefit from the data synergy and collocated access to customer operational databases on IBM System z, which results in immediate data availability, enabling analytics to be performed on the data more quickly. Moreover, operational failure exposures associated with data passing and synchronization between system images are eliminated.
- As financial institutions further optimize their risk detection rules and build more advanced fraud detection systems, more connections are needed to related backend “systems of record” application systems for access to transaction information and account demographics such as names, addresses, and account limits. Some clients preload static files for this access while others are moving to real-time access using an enterprise service bus as a connection point among applications. Because these related backend systems and their interface programs are also collocated on IBM System z, the entire enterprise fraud system shares and leverages the mainframe resource sharing and reduced latency advantages, thus increasing the potential transaction processing capacity while improving the holistic view of risk analysis. This can also apply to “add in or tie backs” where PRM passes information back, such as a card block, a status on a card, or a transaction release.
- Enabling you to use your computing capacity in an optimized manner, is a key architecture design point of IBM System z. Because waiting on disk and network I/O has the single biggest impact on overall solution scalability and throughput, collocating the database with its using applications reduces disk I/O wait time and eliminates costly network latency. Delays in accessing memory is the second most significant factor impacting performance. IBM System z provides superior internal memory bandwidth to reduce I/O demands and improve application throughput. The net result is immediate data availability for improved credit risk analytics, fraud detection, and enhanced customer management, and the elimination of many operational failures associated with data synchronization between systems.

- An important part of the value proposition of the IBM-ACI Worldwide strategic alliance is the integration of every aspect of the retail payment operations on IBM System z. Unlike a distributed platform, IBM System z provides the unique capability of combining switching, routing, and risk analytics on a single platform, as shown in Figure 4 on page 13. PRM and BASE24-eps, when collocated on the same System z, leverage the IBM Coupling Facility to share the data and message passing queues among Sysplex images. Collocating PRM and the data on the same system as BASE24-eps can enable fast and real-time detailed analysis of transactions to be performed before the final authorization is transmitted. Also, additional rules and models can be applied to the real-time transaction to detect fraud. In addition, there is incremental value in integrating payments and fraud management together on a single platform, as shown in Figure 5 on page 13 where the linked tables not only eliminate most file transfer (simplicity) but also facilitate real-time analysis (risk reduction).

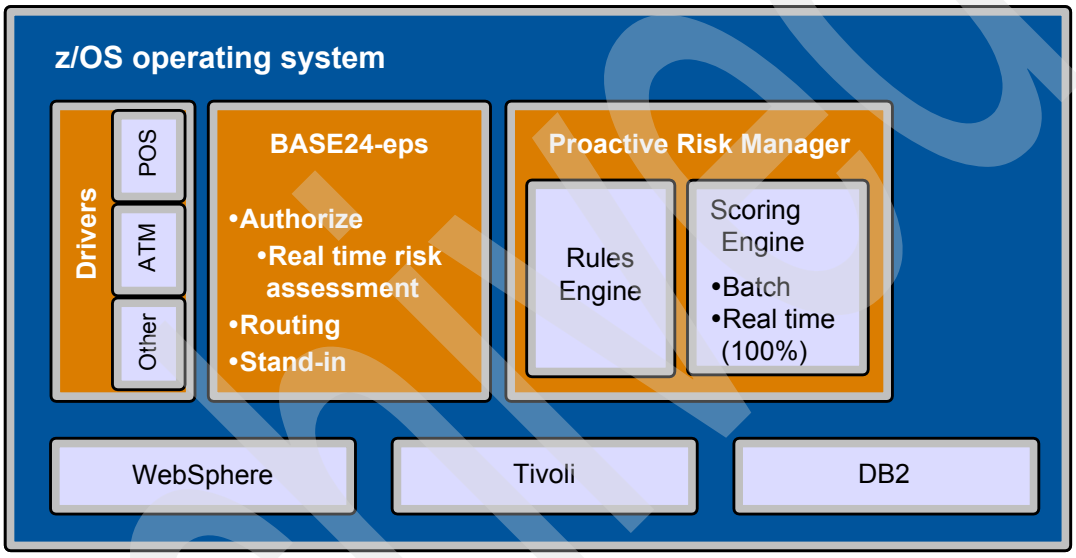


*Figure 4 Integrated payment architecture on System z*

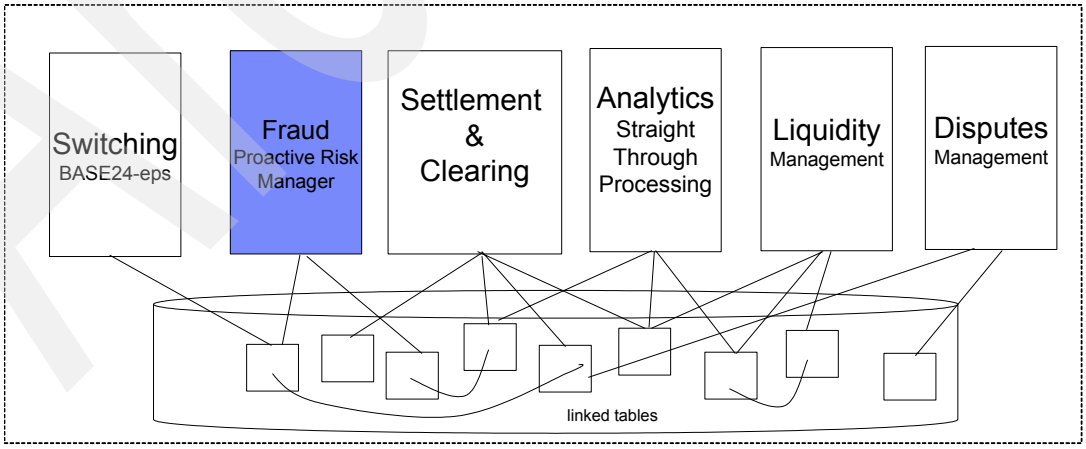


*Figure 5 Sharing data between processes on the same system*

- While maximum benefit is obtained by having BASE24-eps on System z as your payment engine, you might also be able to use other payment engines or deploy BASE24-eps on

another platform and still receive benefit. For clients currently operating on BASE24 “classic” who require enterprise fraud monitoring with PRM (Figure 6 on page 14), there are benefits from connecting the BASE24 classic payment engine to PRM on IBM System z. When using this configuration, PRM retains collocation access to clients’ and “system of record” databases, and the financial institution still exploits, the advantages of the System z data sharing, high availability, and information management middleware capabilities. The resource sharing capability and scale of the IBM System z enable the client to begin migration to BASE24-eps on System z and benefit from the advantages of collocation with PRM.

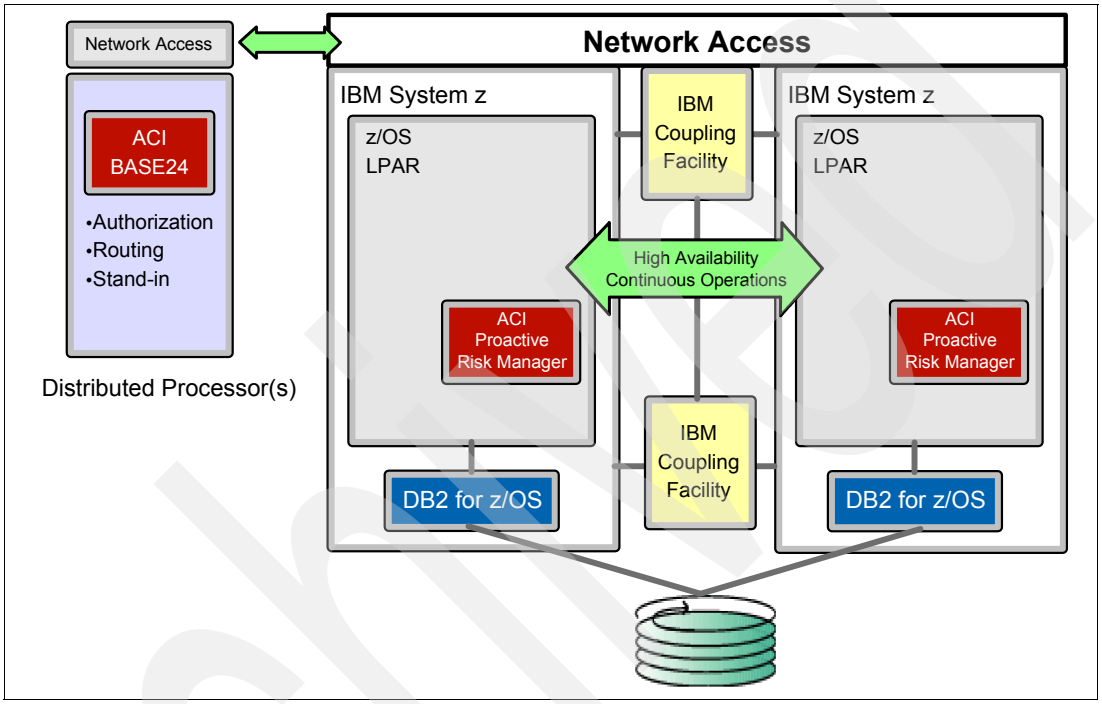


*Figure 6 BASE24 classic on a distributed environment, and PRM on System z*

- ACI PRM uses IBM DB2® database products for storing its own data. In most large financial institutions business data for most channels is kept in DB2 databases on IBM System z. When combining the performance of IBM System z with PRM and a DB2 database, financial institutions are positioned to carry out data analysis and data mining to explore new sources of fraud risk. The enhanced performance achieved by running PRM and DB2 on the same physical system reduces I/O latencies significantly by utilizing memory-to-memory transfer of data at the same time that analytics are being performed on the data. This fast and efficient processing, illustrated in Figure 7, reduces the standard window of time to authorize a valid transaction.

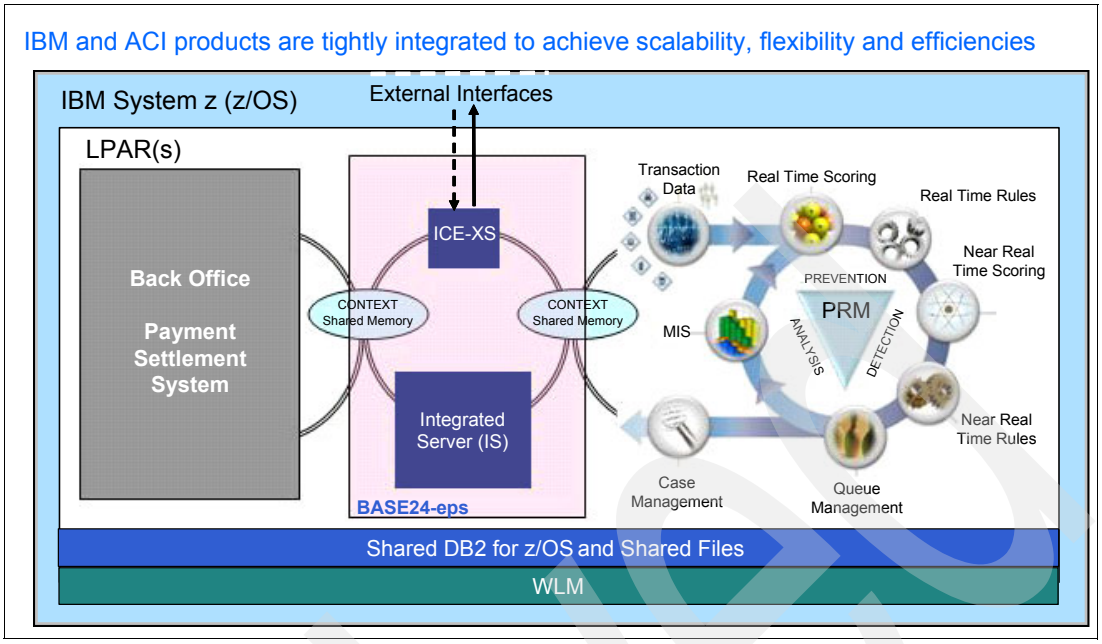


*Figure 7 Advantages of data co-location: Data synergy*

- Because the goal is to get the most complete view of related information possible to assess risk, the additional ability to integrate batch processing into the PRM process can help maximize enterprise fraud detection. IBM System z can prioritize and assign resources for the batch workload to meet critical batch windows that are synchronized with real-time and near-real-time priorities so that these processes operate as a single entity. When analysis of daily, weekly, monthly, or quarterly activity is required, the IBM System z batch capability provides reliable, high-performance access to massive DB2 database content.
- Incremental workloads or new applications can easily be added to an already running System z configuration. IBM System z is built to share many different workloads on one physical machine and balance these workloads according to Service Level Agreements (SLAs) agreed upon with the Line of Business organizations. Leading edge virtualization capabilities on System z, along with dynamic resource allocation, provide financial institutions with the flexibility to direct processing capacity to specific business applications when and where it is needed. This is especially important in financial environments, where a higher number of transactions can very quickly lead to changes in business operations because of increasing fraud analysis and detection.
- The ability to create virtual machine images which comply with EAL5 security facilitates rapid development, migration, and deployment, with extremely secure isolation between independent workloads supporting reduced exposure to internal risk of fraud. This prioritized resource sharing of System z for migration/development/test/production usage eliminates the need for multiple servers, software, networking, support staffing, and facility investments, and the associated costs, and can help fraud managers implement whatever range of system extensions are deemed necessary to improve risk analysis.
- With energy prices and consumption constantly rising, the cost of meeting the total energy requirements of data centers becomes an increasingly significant component of the IT budget. Limited and expensive space in data centers and the propagation of hotspots also can constrain the IT budget. Financial institutions can achieve energy and space savings by consolidating applications running on low utilization (white space) distributed servers and moving them to a centralized System z. In addition to the cost savings from reduced energy consumption and space requirements, consolidation also saves money by

enabling reductions in network infrastructure, system management staffing, and software licensing costs.

- The System z heritage of managing shared resources among multiple diverse workloads makes it feasible to leverage the investment in an existing System z installation by adding appropriate incremental resource to support PRM. This would complement the data sharing and inter-process latency mainframe advantages while eliminating the possible need to acquire an entirely new IT server, software, facilities, and operations staff. With a balanced system design supporting utilization rates of up to 100%, System z is an attractive platform for workload consolidation at a low cost of ownership.

## Scalability and performance to address fluctuating business challenges

Speed and efficiency are critical to stopping fraud in real time; high performance and scalability are required to respond to changing fraud detection transaction volumes. The following examples illustrate how the scalability and performance characteristics of IBM System z support and enhance PRM in providing financial institutions with the flexibility to quickly react to new threats.

- Testing at volumes greater than the majority of the largest institutions today, ACI Worldwide and IBM conducted a series of tests at the IBM Poughkeepsie Benchmark Center to demonstrate the performance characteristics of the PRM product on a single System z using single and dual PRM image (LPAR) configurations and also to determine the MIPS (capacity) per transaction for sizing. The benchmark results showed that PRM running on System z can handle extreme peak transaction processing requirements for both real-time and near-real-time processing, thus allowing the financial institution to determine the level of real-time monitoring needed to achieve its business goals and be prepared to support a dramatic increase in scale. Performance and scalability were close to linear while the cost per transaction remained low and constant. The CPU cost per transaction (measured in MIPS) remained virtually constant as volumes increased, indicating the financial institution can have the confidence of a predictable cost per transaction combined with the computing power and scale to meet their growth requirements (as shown in Figure 8 and Figure 9). Total cost of ownership (TCO) per transaction becomes even lower with higher transaction volumes because support costs for System z are fairly constant as volume grows. The financial institution can run at sustained high utilization rates of over 90%, thus maximizing the cost efficiencies of the System z platform.

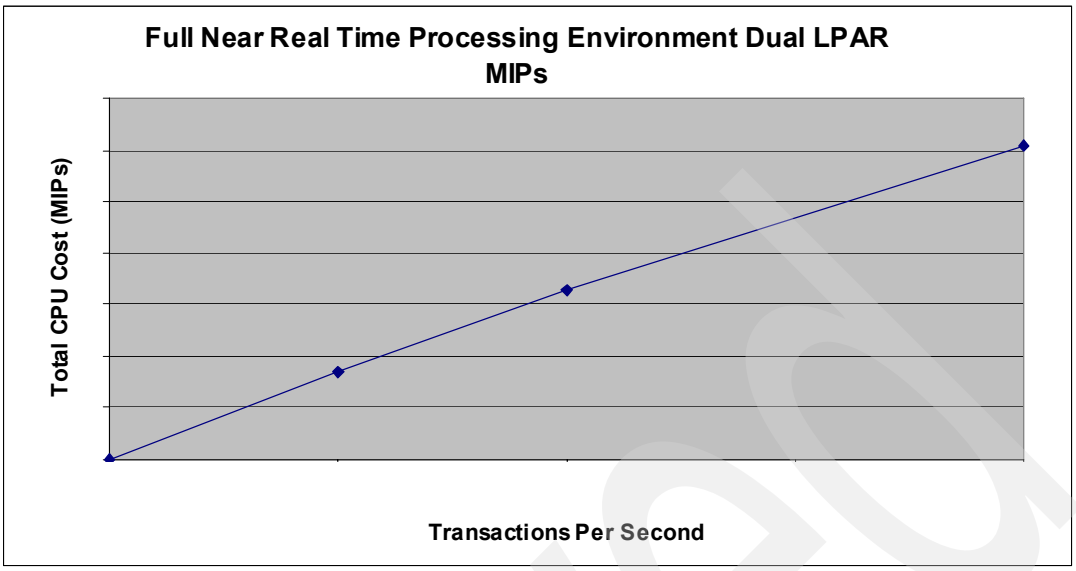


*Figure 8 Full near real time processing benchmark results in a dual LPAR*

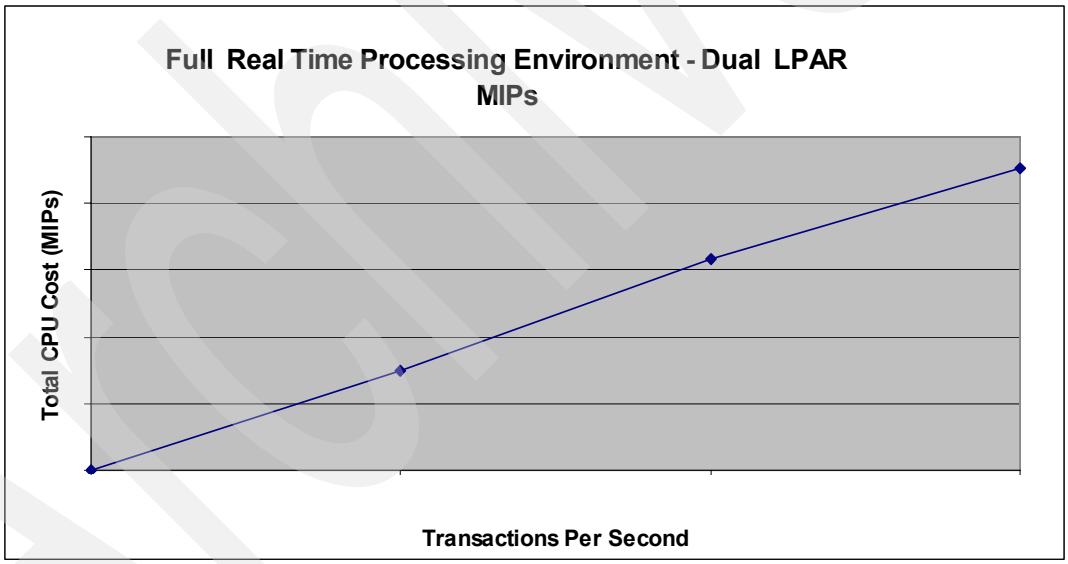


*Figure 9 Full real time processing benchmark results in a dual LPAR*

- The fraud manager has more flexibility in rule writing because the financial institution can increase the length of time historical transactions are stored in the highly scalable DB2 on z/OS® database. Thus the financial manager can increase the suggested real time “short window” retention to a longer period. This provides an extended analysis window which, in turn, means a deeper analysis of historical behavior is possible. Additionally, horizontal capacity scaling can be added non-disruptively by exploiting DB2 on z/OS data sharing and Parallel Sysplex. Unlike partitioned databases required for very large databases on distributed servers, DB2 on z/OS does not require repartitioning to add images. In addition, hot spots in processing due to data affinity are avoided because of the Parallel Sysplex “shared everything” design, which allows workloads to be executed anywhere within a Sysplex.

- The financial institution should have the flexibility to adjust the amount of real-time transaction monitoring that is done, thus avoiding the need to buy excess server capacity for “just in case” peak processing and ending up with unused and costly server white space. The System z “just in time” capacity lets the financial institution dynamically and non-disruptively upgrade processor capacity to handle traffic spikes and to assign the additional capacity to the fraud process. This additional capacity can be a temporary cost, paid for in daily increments or extended into a permanent capacity upgrade at the user’s discretion. These Capacity on Demand options to permit “just in time” dynamic addition of computing power and memory can respond to transaction and workload fluctuations, with a variable cost structure, without service interruption. This feature helps when you need capability to analyze a higher percentage of transactions in real time or when more models and rules need to be applied to the transactions to detect fraud patterns.

## Application availability to protect customer loyalty and brand image

Cybercrime respects no borders and never sleeps; fraud attacks can be initiated from anywhere in the world 24x7. At the same time, application availability can represent the financial institution's face to the outside world. An enterprise-level fraud solution needs to protect the institution and its customers without compromising system availability, business continuity, and disaster recovery if warranted, so the financial institution can ultimately meet its responsibility to its customers and shareholders. PRM on IBM System z can deliver exactly that combination of continuous availability and constant fraud protection, as shown in the following examples.

- The PRM and System z solution can meet specific high availability requirements, ranging from a single site up to a multi-site “Active-Active” configuration with immediate Disaster Recovery. Supported configurations included a range of multiple PRM images sharing the DB2 database on a single redundant System z machine (Figure 10 on page 19), up to dual physical machines in different data centers, each with multiple PRM images operating as a single entity leveraging the System z Parallel Sysplex clustering technology sharing the DB2 database and message queues (Figure 11 on page 20). These configuration options for high availability and disaster recovery are also valid for the combination of ACI BASE24-eps and ACI PRM. This is a striking difference when compared to an Intel®-based PRM configuration, which could require many application and database server images and their associated latency, operational complexities, and staffing costs, and delivering a fluctuating and increasing cost per transaction.

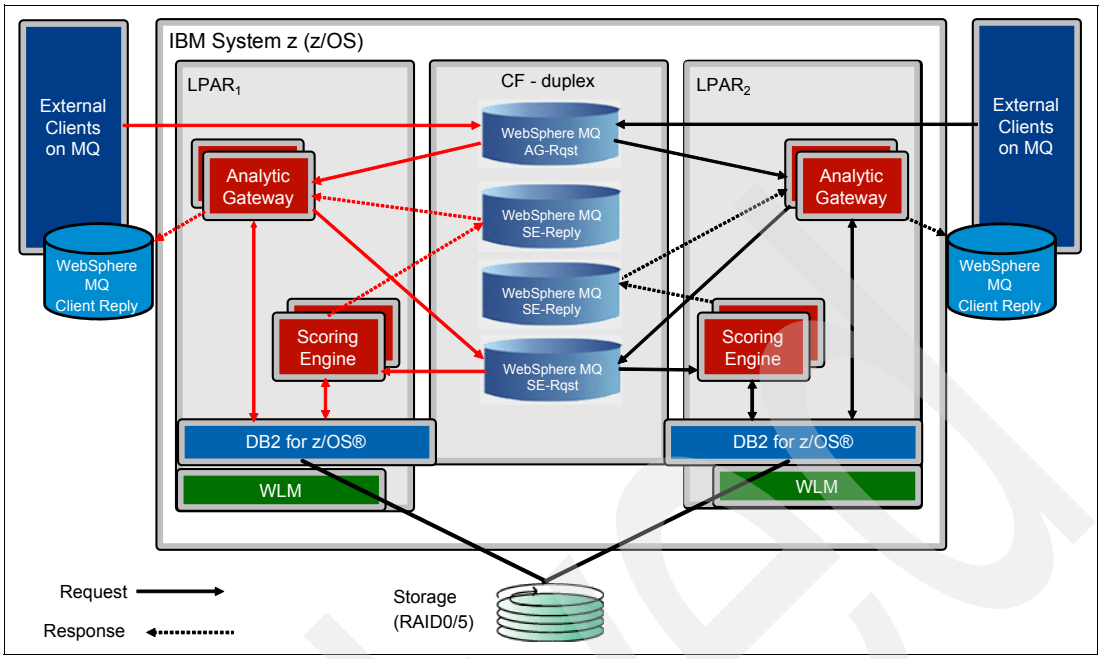


*Figure 10 Single site Parallel Sysplex*

- PRM on z/OS with DB2 is the only platform on which system-wide clustering can provide continuous availability for PRM. Failover techniques on other platforms claim the ability to mask or minimize the impact of unplanned outages, but DB2 on z/OS with Parallel Sysplex, as shown in Figure 11 on page 20, is designed to also support continuous operation through scheduled events such as hardware and software maintenance or replacement, eliminating exposure to reduced service or fraud detection levels. DB2 also provides the ability to reorganize files and journals online, thus eliminating the need to interrupt real-time fraud processing for scheduled database maintenance activity such as incrementing database table space to support additional traffic. These continuous operation features are critical for effective 24x7 enterprise fraud management.

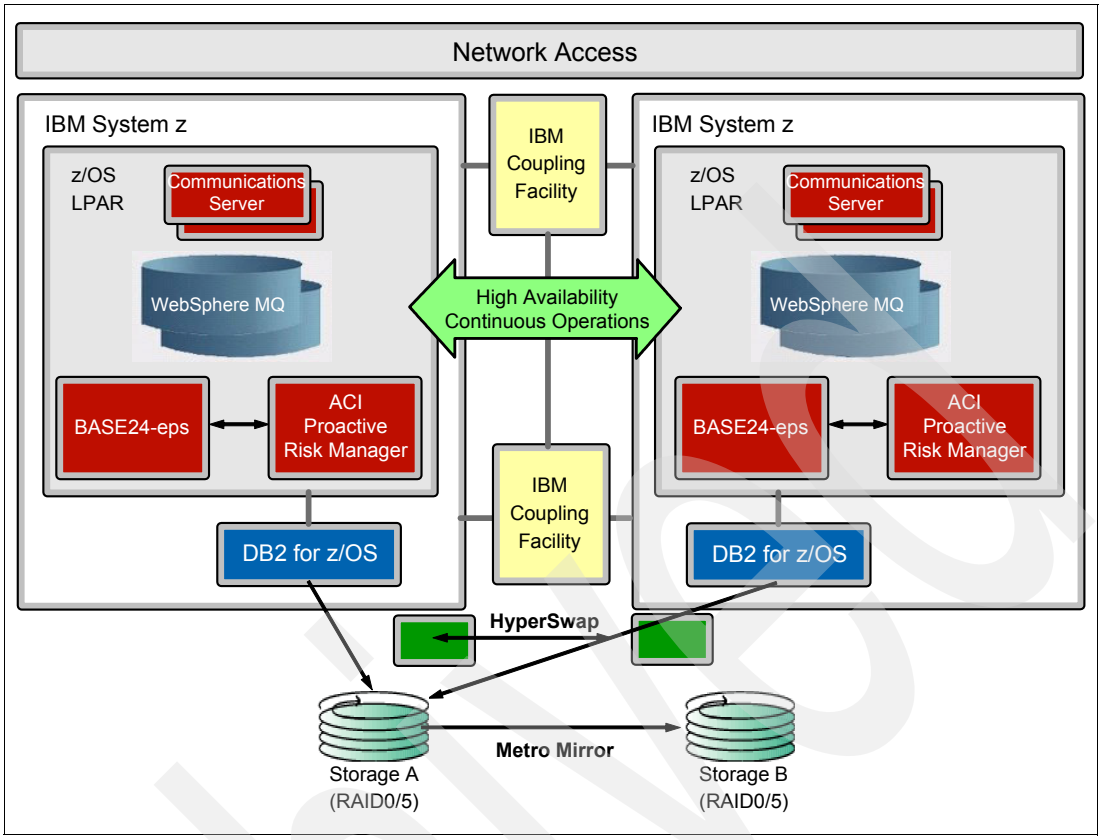


*Figure 11 BASE24-eps and PRM co-located on System z*

- DB2 for z/OS (the PRM data store) has multi-level security, providing different access levels/lists support that can be applied to data at a row level; this granularity reduces the potential for employee fraud and cover up.
- The z/OS encryption facility encrypts data at rest, the IBM TS1100 tapes support data encryption for archive and tape interchange data, the IBM DS8000® System Storage™ encrypts data on disks and the on chip cryptographic functions, and Crypto Express co-processors of System z provide a sound foundation for data protection.
- Running an ACI payment engine on System z, such as BASE24-eps, authorization latency is reduced since the applications take advantage of System z integrated cryptography, eliminating the need for external network-attached encryption devices.

## Superior transaction processing heritage

Nothing speaks louder than a recognized industry reputation for technical innovation, product excellence, customer satisfaction, and the ability to deliver on commitments. The following examples illustrate how ACI Worldwide and IBM have earned their preeminence in providing service to the financial sector.

- ACI Worldwide and IBM have joined forces to create a strategic framework for electronic payments powered by IBM System z technologies. As part of the ACI Worldwide and IBM strategic alliance, ACI Worldwide has optimized the next generation of their strategic retail payments and fraud applications on the IBM System z platform. The two companies have partnered to re-engineer and optimize the PRM and BASE24-eps products to leverage the

IBM System z capabilities. IBM System z is the reference platform for these ACI Worldwide products.

- System z has long been known for its exceptional total cost of ownership benefits and operational characteristics of large volume transaction processing, large scale database management systems, and unparalleled system security and reliability. The proven System z infrastructure can support extremely high volumes with integrity. For example, the Financial Network Services (FNS) core banking benchmark achieved 9445 transactions per second against a 380 million account DB2 database.
- There are System z customers with Parallel Sysplex clustering who have been operating without disruption for over a decade—despite changing hardware infrastructures and implementing multiple software and application upgrades. IBM continues to improve the performance and scalability of the System z mainframe so technology keeps pace with changing business requirements. These unparalleled strengths enable financial institutions using System z to analyze a higher volume of near-real-time transactions and a higher percentage of transactions in real time.
- ACI Worldwide currently has over 2500 institutions protected by PRM. A number of processors around the world are utilizing PRM to protect against and manage fraud on behalf of other financial institutions, and half of the top 20 global banks utilize the solution. More than 800 customers around the world rely on ACI Worldwide solutions to process payments, manage risk, automate bank office systems, and provide application infrastructure services.

## Benefits summary

The implementation of PRM functionality combined with the strengths of IBM System z provides financial institutions the ability to address the trends and challenges they are facing in today's volatile payments environment. With PRM on a System z, financial institutions can take an enterprise view of payments transactions to quickly address potential threats and comply with increasing worldwide government regulatory requirements, while reducing their cost per transaction.

Combining the industry leading workload management, resource sharing, availability and high performance transaction processing pedigree of System z, with its integration efficiencies to leverage coexisting application and database assets, the PRM solution becomes the obvious choice to provide better informed, cost-effective, real-time multichannel enterprise fraud protection that the financial sector demands.

ACI Worldwide and IBM are ready to help financial institutions fight fraudulent activities across all payment channels with proven solutions such as PRM running on IBM System z. The goal is not just to combat fraud, but to reduce operating costs while providing analysts with the tools to help the financial institutions mitigate fraud risks.

# Experience the solution now

It is said that seeing is believing. A quick way to start seeing the power of an IBM System z based PRM enterprise fraud solution is to talk to your ACI Worldwide or IBM representatives. They can provide literature, an onsite demonstration, and a video discussion to help you learn more about this solution. They can also arrange to have you attend a “Smart Bank” showcase and assist you in locating and accessing additional resources.

## Video

The video *Improving Speed & Efficiency in Payment Fraud Management* can be viewed at the following Web site:

http://www.aciworldwide.com/igsbase/igstemplate.cfm?SRC=DB&SRCN=&GnavID=79

Industry experts from featured analyst firm Gartner, Inc., ACI Worldwide, and IBM examine the growing importance of speed and efficiency within fraud management and provide insight into how leading financial institutions are managing fraud and risk across the enterprise in real time.

## Onsite functional demo

A collection of business scenarios based on various integrated combinations of BASE24-eps and PRM is available as an onsite demonstration. The demo lets you view transaction transaction progress using the application’s user interface screens. The demos are globally remote-accessible. The application code is running on an IBM System z10™ in the IBM Montpellier, France, executive briefing center using a fully functional configuration, so you can experience the solution at your own facility.

The demo scenarios include:

- Scripted authorization
- Role of scripting in fraud management

- Card status changes with real-time update to BASE24-eps
- User-defined limits with temporary increase period

Additional capabilities can be shown using the product's desktop user interface.

## Customize your own demo

Working with your ACI Worldwide and IBM alliance team, you can request the use of a sandbox environment where you can try out minor customizations to address your particular needs and to demonstrate additional product functionality not included in the general purpose product demonstration scenarios. The sandbox provides a fully operational environment with the operational characteristics, supporting data, and traffic generation capabilities equal to those of the ACI Worldwide product demo environment.

A sandbox environment is available via a remote connection from anywhere in the world. The testing period is usually up to a three weeks per project, but longer periods are negotiable. This is typically a customer funded engagement and is staffed by ACI Worldwide, IBM, and customer resources who use the sandbox to build a more tailored demonstration to match specific requirements. A sandbox could also be used for things like training or for services projects to help expedite the installation process.

## Witness production volume operation by attending a Smart Bank showcase

The Smart Bank showcase is a combined briefing and live data center-scale demonstration where you can view the integration of the BASE24-eps payments engine with PRM fraud detection in both real time and near real time, running at production scale on an IBM System z10 Enterprise Class. The showcase also shows connection to backend core banking systems for authorization, in high availability scenarios, and demonstrates capacity upgrade on demand, which provides increased flexibility to handle traffic spikes and changes in processing requirements based on business needs.

This demonstration showcase is a sample implementation to simulate a real customer payment environment using integrated ACI BASE24-eps and PRM with multichannel input, including batch, into PRM as the enterprise fraud solution. The showcase extensively uses Tivoli® monitoring solutions integrated with ACI User Interface statistics to provide a single view of the integrated solution infrastructure. The basic concept behind this implementation is to provide customers with a live view of the capabilities of ACI Proactive Risk Manager on System z in a high availability configuration running at production level transaction volumes.

It is also important to note that customers can implement such a configuration to monitor the transactions and prevent fraud today. The Smart Bank showcase implementation is one of the many real customer integration scenarios that can be used to rapidly deploy such a solution at a financial institution. The ACI Worldwide and IBM strategic alliance can provide seamless collaboration services to help customers accelerate the selection and implementation of an enterprise-wide risk management framework to prevent fraud as soon as possible.

Clients attending a briefing have found this demonstration to be particularly helpful in understanding the functionality of ACI payments engine and ACI Enterprise Fraud Management software, and the value of the underlying System z infrastructure.

IBM's Global Services organization represents a key value-add in offering customers end-to-end total solutions including consulting, legacy systems integration, custom capabilities, and ongoing support for large-scale processing needs. This complements the application-level services ACI Worldwide provides to implement PRM. Together, ACI Worldwide and IBM offer an unparalleled comprehensive solution in the e-payments space.

## Customer success story

Westpac New Zealand chose ACI Proactive Risk Manager for Enterprise Risk on the IBM System z to strengthen its fraud detection and prevention capabilities and to protect against the rapidly rising volume of fraudulent activities occurring worldwide. Westpac New Zealand implemented real-time rules to monitor potentially suspicious transactions within the authorization process, thereby identifying and preventing fraud. Westpac is one of New Zealand's largest full-service banks and has been operating in New Zealand for over 145 years. The bank has 1.2 million active customers, almost 200 branches, and over 500 ATMs nationwide. Further information is available in the press release link at:

http://www.ibm.com/press/us/en/pressrelease/27828.wss

## Additional resources

As leading technology providers of financial services solutions, IBM and ACI Worldwide offer expertise in protecting financial institutions and their customers from fraud. The solution brochure *IBM and ACI Worldwide - Providing Enterprise Fraud Solutions for Retail and Wholesale Payments* provides additional background on an enterprise approach to fighting fraud, the importance of real-time fraud detection, and highlights of IBM and ACI Worldwide enterprise fraud solutions. It can be found at:

http://www.ibm.com/industries/financialservices/us/detail/resource/M833021I37699B40.html

ACI Proactive Risk Manager has been optimized for System z. This powerful combination enables banks to take an enterprise view of payment transactions with the flexibility to quickly respond to new sources of potential fraud. Banks and other financial institutions will be able to monitor transactions in near real time even as transaction volumes grow. Selected high priority transactions can be monitored in real time to further reduce the risk of fraud losses. The solution brochure *Improving Payments Fraud Detection and Prevention: ACI Proactive Risk Manager with IBM System z10* provides additional information on the benefits of the mainframe for enterprise fraud detection and prevention. It can be found at:

http://www.ibm.com/common/ssi/fcgi-bin/ssialias?infotype=PM&subtype=BR&appname=STGE_ZS_ZS_USEN_&htmlfid=ZSB03024USEN&attachment=ZSB03024USEN.PDF)

IBM announced the System z Solution Edition Series to help customers deploy new enterprise workloads such as electronic payments. This program reflects an ongoing strategy to enable customers to run a much wider range of their business activities on System z while taking advantage of the powerful reliability, efficiency, transaction processing and management capabilities of the platform. Further information on these offerings, including the System z Solution Edition for ACI, is available in the press release at the following Web site:

http://www.ibm.com/press/us/en/pressrelease/28181.wss

# Summary

The financial impact of fraud is increasing for banks worldwide. Fraud attacks and data breaches are costly, not only in terms of reputation and loss of revenue, but also in the administrative costs of restoring customers' accounts and reporting exposures to regulatory agencies. Banks are also required to keep an increasing amount of capital reserve for fraud losses. All of these issues are placing a greater internal focus on enterprise risk management.

Fraud is becoming a growing concern for financial institutions and an adequate enterprise-wide solution is required to deal with this issue effectively. Fraud detection needs to be near real-time and complex analysis across multiple channels needs to be done on a continuous basis. This IBM Redguide™ positions ACI Proactive Risk Manager (PRM) solution to address this issue and reduce enterprise fraud across all payment channels, and achieve operational cost reductions by implementing the solution on the IBM System z platform.

This guide also helps you understand the current worldwide payment channels changes, trends, and challenges, including the importance of accepting that fraud losses are becoming a key concern for financial institutions due to large sums of money already lost because of fraudulent transactions.

## Other resources for more information

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this guide:

- *A Guide to ACI Worldwide's BASE24-eps on z/OS ,* SG24-7684
- *z/OS Parallel Sysplex Configuration Overview*, SG24-6485

These Web sites are also relevant as further information sources:

- ACI Worldwide landing page with additional resources on payment fraud management

  `http://www.aciworldwide.com/enterprisefraud`

- Improving speed and efficiency in payment fraud management, an ACI Worldwide and IBM webcast featuring analyst firm Gartner.

  `http://www.aciworldwide.com/igsbase/igstemplate.cfm?SRC=DB&SRCN=&GnavID=79`

- Fraud Management at Retails Banks and Credit Unions: The Vendor Landscape - A new Report from the Aite Group - As fraud becomes increasingly multichannel, financial institutions are using solutions from multiple fraud management technology vendors.

  `http://www.aitegroup.com/reports/200904151.php`

- The Fortent Financial Crimes Survey Findings 2008 - This report presents the findings of the 2008 survey carried out among senior compliance officers, representing financial institutions around the world. The purpose of the survey was to identify key areas of concern among executives who are responsible for overseeing their institutions' compliance with Bank Secrecy Act/Anti-Money Laundering (BSA/AML) laws. The survey also addressed the impact of the current economic climate on the compliance function.

  `http://www.http://www.fortent.com/knowledge_center/articles.php`

- EAL-5 certification information

  `http://www.ibm.com/systems/z/advantages/security/ccs_certification.html`

## The team that wrote this guide

This guide was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO).

**Alex Louwe Kooijmans** is a project leader with the International Technical Support Organization (ITSO) in Poughkeepsie, NY, and specializes in SOA technology and solutions on System z. He also specializes in application modernization and transformation on z/OS. Previously he worked as a Client IT Architect in the Financial Services sector with IBM in The Netherlands, advising financial services companies on IT issues such as software and hardware strategy and on demand. Alex has also worked at the Technical Marketing Competence Center for zSeries® and Linux® in Boeblingen, Germany, providing support to customers starting up with Java™ and WebSphere® on System z. From 1997 to 2000, Alex completed a previous assignment with the ITSO, managing various IBM Redbooks® projects and delivering workshops around the world in the area of WebSphere, Java, and e-business technology on System z. Before 1997 Alex held a variety of positions in application design and development, product support, and project management, mostly in relation to the IBM mainframe.

**Rob Haake** is responsible for product marketing for ACI's financial crime management products. Rob also serves as the President of the Americas ACI Customer Exchange (ACE) Risk Advisory Committee. Rob joined ACI Worldwide in May 2008 and has over eight years payment industry experience. Prior to joining ACI Worldwide, Rob led channel and product marketing efforts for First Data Corporation's national financial institutions segment. Rob holds an MBA from Regis University and a Bachelor of Arts from Creighton University.

**Jim Goethals** is currently an infrastructure architect with IBM in Raleigh, North Carolina. He has worked at IBM for 40 years, 26 of which were in product marketing, where Jim was responsible for multiple IBM hardware and software products. His current position in the IBM Banking Center of Excellence deals with retail payments and core systems transformation to help clients accelerate their move to smarter banking on a dynamic infrastructure. His other areas of expertise include networking and transaction processing on large systems.

**Ethel Richardson** has over 25 years of experience with IBM mainframes. She is a graduate of Vassar College in Poughkeepsie, New York with a Bachelor's Degree in Mathematics. She also holds a Masters Degree in Systems and Information Science from Syracuse University in Syracuse, New York. Ethel has contributed to several publications related to the financial services sector and the value of the mainframe.

**Dino Quintero** is a project leader with the International Technical Support Organization (ITSO) in Poughkeepsie, NY. His areas of expertise include continuous availability planning and implementation, enterprise systems management, virtualization and clustering solutions.

Thanks to the following people for their contributions to this project:

Ella Buslovic, Emma Jacobs, Alison Chandler
ITSO, Poughkeepsie Center

Andy Brown, Michelle Weatherhead, James Kueffner, Lori Morehead
ACI Worldwide

Stephane Faure, Robert Easter, Ken Muckenhaupt, John Crooks, Michael Onoufriou, Lorilee Lang
IBM

# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
*IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-4545-00, was created or updated on September 16, 2009.

# Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at
http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

| | | |
|---|---|---|
| DB2® | Redbooks® | System z® |
| DS8000® | Redguide™ | Tivoli® |
| HiperSockets™ | Redbooks (logo) ® | WebSphere® |
| IBM® | System Storage™ | z/OS® |
| Parallel Sysplex® | System z10™ | zSeries® |

The following terms are trademarks of other companies:

PRM is a trademark of ACI Worldwide. ACI and ACI Worldwide are registered trademarks in the United States, other countries or both.

Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.