

driving down fraud costs through risk management

Electronic payments processing has been a financial industry success story. Growing transaction volumes and market share are testimony to this, as is its contribution to the profitability of financial institutions. The industry, however, is under threat from fraud — figures show that worldwide fraud continues to rise and will increasingly impact financial institutions unless counter-measures exist. The European Commission estimated that card fraud in the European Union (EU) reached \$943 million in 2000. In the UK, plastic card fraud rose in value by 30 percent between 2000 and 2001 to an estimated total of \$617 million. All fraud erodes margins due to the costs of claims processing, referrals, write-offs and bad debt. Even worse, the brand damage may be more severe than any short-term financial loss. A risk management strategy is essential to successfully address such fraud and thereby contribute cost savings.

Different priorities exist depending on the business objectives and market characteristics, but all financial institutions want to drive down the costs of processing e-payments. Some markets have a large merchant fraud problem, while in others cardholder fraud is a higher priority. Some institutions face both threats and need solutions for each. All financial institutions need a risk management strategy and measures that address multiple fraud types in each market sector. In addition, the industry's trend of adopting Internet-based technologies may contribute to the fraud problem.

Many important factors apply when considering risk management. A risk management strategy must minimize the financial institution's financial liability. To a degree, it is a compromise between security and convenience. A service which is 100 percent secure may be unusable due to high costs or a poor customer user-experience. The introduction of anti-fraud protection must not make the service to the consumer more inconvenient. In terms of a business case, the investment required for adopting a new measure must be lower than the cost of the actual fraud being committed, as otherwise it is unlikely to be sanctioned.

Don't Panic About Security, Just P.A.N.I.C.

Various types of fraud may be committed by numerous entities such as customers, cardholders and merchants. Fraud involving the use of lost and stolen cards, counterfeit cards and identity theft are increasingly common. Furthermore, these crimes can be committed in numerous environments (branch, Internet, cardholder not present (CNP), etc.). Solutions that address these must exhibit the five general characteristics that form the P.A.N.I.C. acronym.

Privacy is the act of keeping information confidential. It can be applied in several ways. For example, in terms of transportation over networks (to prevent a merchant obtaining a card number), or storage on disk files.

Authentication ensures that the entity (such as a merchant) being dealt with actually is who it claims to be. Multiple levels of authentication sophistication are available. One-factor authentication is based on "something I know" (such as a PIN). Two-factor authentication adds "something I have" (such as a payment card). Three-factor authentication includes "something I am" (such as a biometric feature - fingerprint, retina scan, etc.).

Non-repudiation protects against a denial of participation in a transaction (by a merchant or cardholder).

Integrity ensures the recipient receives the data as intended by the sender and can be sure it hasn't changed en-route (such as by a fraudulent merchant).



Checking a transaction against pre-determined conditions that define a financial institution's risk management thresholds.

Individual payment industry elements incorporate one or more of these. However, for an enterprise risk management solution support for all features of P.A.N.I.C. are essential.

How Does the Industry Address Fraud?

The payments industry has evolved over many years to the situation where there are numerous solutions now available. For example, debit and credit cards have been enhanced many times, and now include many security features such as the signature panel (for authentication), magnetic stripe, CVV, CVV2, hologram (for checking) and chip card (privacy and integrity). This illustrates that one item can contain multiple elements of P.A.N.I.C. Other examples of this are discussed below.

Privacy is typically provided by encryption solutions within the delivery channel. The SSL protocol is the standard used over the Internet while in the real world, hashing, message digests, symmetric key (DES, Triple DES) and asymmetric key (RSA, AKDS, PKI) encryption are common.

A consumer's signature and PIN are the two most widely used authentication techniques. These are satisfactory in many face-to-face situations. The rise of counterfeit fraud, however, has resulted in initiatives such as EMV, and the PIN at POS authentication initiative being launched in the UK. Authentication is also a major issue in the CNP environment such as the Internet and Mail Order/Telephone Order (MOTO). The CVV2 feature helps with CNP while e-commerce is being addressed by a protocol being promoted by Visa and MasterCard known as 3D Secure. Reliable merchant authentication is also an important factor and this is typically achieved through password and card verification at the purchase device.

A voucher with the consumer's signature is the basis for recording the agreement to, and participation in, a transaction. Industry initiatives aim to reproduce this in the electronic environment. Techniques such as paper vouchers, PIN, EMV cryptograms, digital signatures, transaction logging and auditing, and the use of trusted third parties as intermediaries can all be used to provide non-repudiation against disputed transactions.

The Message Authentication Code (MAC) is widely used for ensuring data integrity. Other techniques include PKI-based digital signatures.

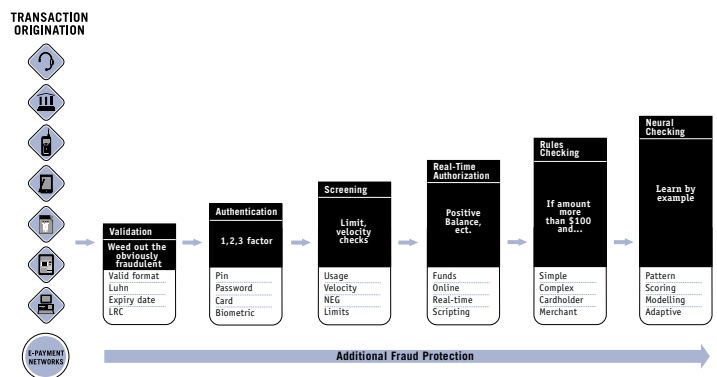
Even though a transaction may satisfy all the above criteria, it is unlikely to satisfy all the fraud management needs of the financial institution. Various checks must be applied before a transaction can be authorized. Examples include limit checking (floor limit), hotlist checking, usage/velocity checking (maximum transactions per period), and complex rules checking (if x AND y then ...). These apply to all the various entities such as the cardholder, merchant, branch, employee, etc.

It is apparent that there are multiple anti-fraud techniques available to a financial institution. The challenge is to incorporate them in a consistent and cost effective way that provides an efficient fraud management service to the enterprise. This is easier to achieve if a framework exists into which these techniques can be incorporated.

Enterprise Risk Management Framework

An Enterprise-wide Risk Management Framework addresses this challenge and, arguably, is essential in minimizing the cost of fraud management. Enterprise Risk Management Framework is a centralized service that delivers consistent risk management across the enterprise. Within the Enterprise Risk Management Framework multiple protection measures exist and are grouped into components. Componentization is the key feature of the Enterprise Risk Management Framework. The framework can evolve from a single component to a multiple component model with the addition of further measures when convenient to the financial institution.

An example of an Enterprise Risk Management Framework containing six components is illustrated as follows.



Component Summary

The validation component eliminates the obviously fraudulent. The authentication component ensures that the entity originating the transaction is whom they claim to be and is recognized and approved by the recipient. The screening component enforces usage and velocity limits and helps control bad debt. The real

time authorization component approves or denies a request based on the most current information being available (such as funds availability). The rules checking component provides a business rules driven service. The neural component provides a “learn by example” service. Following evaluation against the consumer’s traditional usage pattern the transaction is scored and forwarded for further investigation if a pre-determined threshold is exceeded.

Risk Management Componentization

For a comprehensive risk management solution each of the above components should exist at the financial institution. Maximum benefit is only realized, however, when each of the components work together. A transaction typically enters at the validation component and each advance to subsequent component represents an increase in sophistication. Different transaction types will progress to different components depending on their level of risk.

Each component can be considered stand-alone in terms of the protection measures it supports. Multiple technologies must exist in the same component, for example the DES, Triple DES and SSL encryption technologies would reside in the same component. Components must support new techniques as they become market ready. For example, Microsoft’s .NET and the Liberty Alliance solutions should be accommodated by the authentication component.

Componentization of services is a great help when addressing a new threat. A good current example of this is with CNP fraud. Different individual techniques to address CNP can be identified, and this can be simplified if considered within the overall framework.

It is not necessary for each component to support all elements of P.A.N.I.C., but it is important that the overall Enterprise Risk Management Framework does. For example, the privacy of data transmission exists in the delivery channel and is addressed by the validation component. Authentication is a dedicated component. Non-repudiation support such as data logging and auditing is provided by multiple components. Data integrity exists in the validation component, while checking is performed by multiple components.

Customer Segmentation and Personalization

Transactions normally enter the validation component and progress to subsequent components when two conditions

are satisfied. The transaction must pass the conditions set by the component. Second, the financial institution’s customer segmentation rules must define if the transaction is required to proceed to the next stage. For example, for a trusted high-net-worth consumer a four-component profile may be sufficient, but a young consumer who has recently received his first credit card may be required to proceed through all six components. The ability to segment the consumer base and apply different rules depending on the level of risk is a vital factor in controlling costs and providing a good customer experience. Segmentation allows each financial institution to operate at its own preferred level of risk as well as providing a more personalized customer service that leads to increased loyalty.

Interfaces Between Components

While several industry standards exist for individual techniques, in some cases they are absent from components and also from interfaces between components. At most financial institutions a heterogeneous infrastructure is the reality and, therefore, integration must be addressed. Many legacy systems inhibit flexibility and it is in the financial institution’s best interests to remove such barriers by adopting an integrated, end-to-end solution. This must be achieved while continuing to satisfy the continually evolving industry mandates and technologies.

Flexibility and options are highly desirable when considering the types of interaction between components. For example the interface between the real time authorization and rules components may be offline (periodic batch updates) or online (real time, in-line scoring). Additional checking may require additional resources and, therefore, bandwidth and performance become critical elements. This makes customer segmentation even more important.

Consolidation and Centralization

It is essential that individual techniques are only implemented once by being consolidated and centralized. Not only does this provide a more consistent consumer experience but the financial institution is better positioned to react to new threats. For example, should the financial institution come under attack from a new type of fraud, then it is desirable to have the ability to define a new rule once and have it effective across all delivery channels. Speed is vital in this instance, as a quick response can minimize costs. Consolidation also prevents the benefits of a new service not being cancelled out by an increasingly complex and expensive operational environment.

Support Multiple Delivery Channels

The opportunities presented by new delivery channels (Internet, mobile, etc.) means that there is increasing pressure to support them while minimizing fraud and providing a consistent consumer experience. It is most efficient if the additional channels utilize existing risk management services. This is greatly simplified if risk management exists in one place and is accessible to the entire enterprise. It allows existing services such as consumer usage limits checking to apply to the Internet as well as branch and ATM. Similarly, a customer authentication technique can be applied to card issuance as well as during the payment processing.

This also facilitates the migration of existing features into other delivery channels. For example, migrating the established debit card PIN authentication into channels such as the branch and Web, or introducing the plastic card into the e-commerce world through PC based chip-card readers.

Parameterization

Equally important is the need for flexibility by accommodating new business rules through parameters, scripts or configuration changes, rather than software changes. The most flexible solutions support features such as a script-based authorization, the ability to set new limits, to download authorization scripts to EMV cards, and to define additional rules. For all of these a speedy implementation and support is critical.

Conclusion

Fraud is only part of a risk management strategy and consideration must also be given to other security elements. Physical security involving secure operations centers, contingency planning, firewalls, DMZ, secure domains and anti-virus protection must be addressed. Employee monitoring is essential to eliminate the significant proportion of fraud that is committed by staff. Underlying all these is the need for the service to be acceptable in terms of reliability, performance and scalability. All relevant procedures and policies must be in place to support this operation.

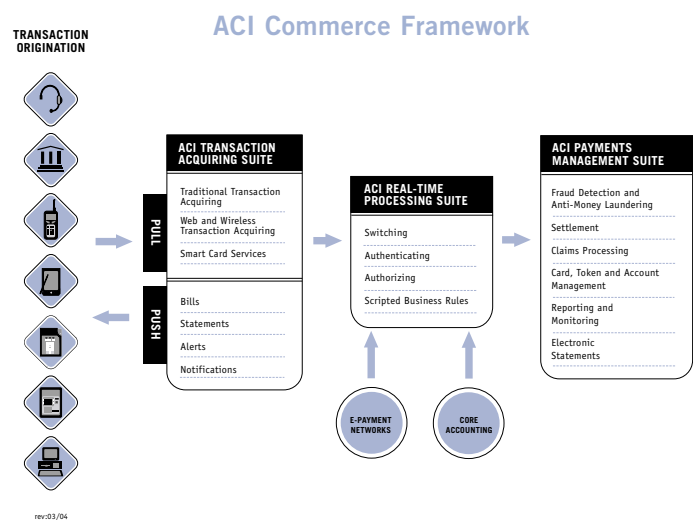
Financial institutions recognize that risk management is mandatory in achieving improved financial performance. Ignoring fraud is not an option and a strategy to address it must be deployed as quickly and cost effectively as possible. The principles of componentization, segmentation, personalization and parameterization, as provided by an Enterprise Risk Management Framework, can help achieve this.

Preparing for P.A.N.I.C. is the best way to avoid panic!

Why ACI?

We make it our business to help customers optimize their return on current investments, transact in high volumes (ACI software processes more than 40 billion transactions in a year), and move forward with new technology. We lead in e-payment processing products and have vast payment marketplace experience on a variety of platforms including IBM zSeries®, IBM pSeries®, HP NonStop™, HP-UX and Sun® Solaris™.

Among software providers, we are unique in our ability to address the breadth of services across the payments value chain — a single source for end-to-end solutions, helping you to simplify implementations and speed your time to market for new services.



The ACI Commerce Framework represents an integrated solution suite that supports transaction initiation, real time processing and back office transaction management.