

The Goldfinch Report

Risk and Security

Published by *Paycre8*

Written By Peter Goldfinch

About the Author:



Peter is one of the founders of Paycre8 and has been writing the Goldfinch Report for approximately 3 years.

He has been working in the payments industry for over 20 years and as a consultant completed assignments for clients in 20 or more developed and emerging markets.

Many would consider Peter to be a technology oriented professional but he also has a strong business background.

This report is an opinion piece and is not intended to do more than reflect Peter's views at the time of writing. The subject matter often relates to current experiences resulting from his consulting experience. The purpose is to generate debate

There is no payment system that is completely secure nor is there one that does not represent a risk to its provider or users. Protection is derived from increasing the barriers and therefore the degree of difficulty for any 'would be' fraudster. Fraudsters will always attack the softer targets first.

Those who commit fraud come in different forms from the organized criminal groups to the amateur who is less motivated by the financial rewards and more by the challenge of breaking a security method. The perpetrator of fraud will not necessarily be external to the organization. The internal threat from disgruntled staff is just as significant.

The organized criminals will seek out the opportunities delivering the maximum return for the least effort. A method of committing fraud generally occurs in one country, (and one payment service) and then moves onto the next weakest country or application. By keeping a global watch there is the potential to take defensive action ahead of an attack. But somebody always needs to be first.

A disgruntled staff member who is able to access unprotected personal customer data can then pass this onto the organized criminals or use it themselves - In effect stealing another person's identity. Technical staff may be able to patch software for accessing data or manipulate processing to move funds to alternative accounts.

The providers of payment services often find it difficult to stay ahead of organized crime and therefore must be quick to react when a new method of fraud becomes evident. The in-house opportunists can be addressed through adherence to the PCI/DSS standards - deployment of sound key and data management practices, strict access controls supported by audit logs plus software change management and testing procedures. Segregation of tasks is critical.

The Goldfinch Report: *Risk And Security*

Published by *Paycre8*

Written By Peter Goldfinch

through examination of current industry developments and directions. The author hopes you enjoy reading these reports.

About *Paycre8*:

The three founders of Paycre8 have been working in the payments industry for collectively over four decades. Most of this time they have worked as consultants, designers, integrators, developers and project managers on various project internationally. They have experience in a wide range of payment channels, instruments and networks, normally working at the leading edge.

The demand and referrals from old clients plus a passion for the creative aspects of the industry motivated the three founders to build what they believe is a unique and niche consultancy practice.

But risk is not only an issue of fraud. Poorly designed and constructed systems can operationally fail especially when under stress due to high transaction loads. Such failures can result in accounts being incorrectly updated as transaction reversal and recovery processes fail. In simple terms a system lacking in processing integrity represents a risk.

A payment system that is exposed to fraud, subject to delinquent behaviour by customers or lacks integrity and robustness will cost its providers/owners in terms of reputation as well as financially.

Within the mobile payment sector we are hearing a lot of negative comments concerning regulators. There is some justification for this but it must be recognized mobile is a new payment channel and the first where banks have not lead the deployment. The promoters are largely ignorant of the risks and ramifications of what they are trying to achieve especially if they get it wrong. Essentially regulators are finding they are outside their comfort zone.

In general the failure of one element of a country's Payment System can flow through to the other elements causing systemic failure, leading in the extreme case to the melt down of an economy, the old domino effect. This generally results from depositors losing confidence with the overall banking system and withdrawing their deposits in cash, for example, the Northern Rock situation in the UK. Central Banks and governments need in these situations to act quickly to stop other financial institutions being effected as per the recent credit crisis.

For the industrialized countries the payment systems are more tightly integrated and failure of one element will flow through the complete system with a greater effect than in an emerging economy where integration is not so tight. But regardless of the status of an economy people's behaviour is unpredictable, when losing their savings. The impact of failure will be as severe at the social and political levels as it will be at the economic level.

The Goldfinch Report: *Risk And Security*

Published by *Paycre8*

Written By Peter Goldfinch

Paycre8 - Value

statements:

Purpose – to provide payment system advisory services to an international client base. Clients who currently operate payment systems or who are investigating starting up electronic payment services.

Vision - By providing fast responsive, informed expertise, and consistently high quality service, *Paycre8* aims to build an international reputation for excellence.

Mission – To be recognized as the foremost group of experts in payments.

So how do you design a secure payment system to mitigate the risk?

The primary objective is to authenticate the transaction initiator as the account owner or the person with permission to access the targeted funds.

A payment system is a chain. The number of links will depend on whether the system is open or closed, whether a single transaction is required to pass through multiple switches and network links to reach the customer owning institution or whether a transaction is simply on-us. The weakest link inclusively from the point of acceptance through to the owning institution is where the attack is most likely to occur.

In general terms the industry through evolution has in the last 2-3 decades developed two models. One is the proprietary debit card (non-repudiation) model and the other the card schemes request and response model. The card schemes when it comes to ATM support use the non-repudiation model.

The primary difference between these two models are:

- The non-repudiation model has been based on technology and transaction limits to support primarily cash withdrawals and debit account access.
- The card schemes traditionally have relied on business processes rather than technology. The chargeback facility is the foundation of their historical processes. The payment risk through a series of ever evolving rules is spread across the four parties - cardholder, merchant, acquirer and issuer.

With the growth of the 'card not present' transaction market segment (e-commerce) card schemes are increasingly utilizing technology. The mitigation of risk is covered through:

- Utilizing credit-scoring techniques to ensure cardholders fit a certain profile.
- Behavioral profiling to determine if a transaction has a high probability of being fraudulent.

The Goldfinch Report: *Risk And Security*

Published by *Paycrest*

Written By Peter Goldfinch

Paycrest - delivers a range of payment advisory services:

- Market Surveys and Analysis
- Requirements Definitions
- Solution Development
- Business Planning
- Business Modeling
- Process Planning
- System Design
- Solution Evaluation and Selection
- Project Directorship
- Project Management
- Specialist Project Resourcing
- Business Training
- On-Going Business Reviews and Audits

- Processes to monitor merchant transaction behavior.
- Implementation of 3D secure methods.
- The issuance of chip cards and also the concept of chip with PIN.
- In those countries reluctant to go with chip, PIN on magnetic stripe cards has been introduced at the point of sale.

How does all this impact mobile payments?

The author's view is that mobile is just another payment channel and should utilize the methods that have been developed successfully for other channels, specifically those developed for the non-repudiation model and deployed by ATM systems. For mobile to be globally successful across all market segments it needs to be the strongest with respect to security.

Technically it has this capability.

The only serious breaches of security in respect to ATM have occurred at the device itself. This is where magnetic stripe readers have been attached to the card acceptance slot to capture magnetic stripe details along with hidden cameras to record PIN entry. A similar attack has occurred in Australia recently with respect to EFTPOS devices.

The mobile handset has advantages over an ATM and the EFTPOS device, being associated with an individual. Or more correctly the SIM card is linked to one individual. Further in terms of a payment system the handset is both the payment instrument and acceptance device. This means the ATM and EFTPOS issues will not occur with mobile, at least not in the same manner.

To make a mobile payment service secure the following points need to be taken on board:

- Industry strength security is required from point of acceptance. This can only be achieved by using the security features of STK.
- Both the PIN block and the message (containing the PIN block) need to be encrypted using either 3DES or PKI or a combination of both. If 3DES then the keys should be unique to each SIM.

The Goldfinch Report: *Risk And Security*

Published by *Paycre8*

Written By Peter Goldfinch

Contact *Paycre8*:

info@paycre8.com

- Avoid holding any meaningful data on the handset/SIM using pseudonyms for card or account selection.
- Ensure all individual SIM keys are secured by the systems security service engine using a secure key storage facility.
- All encryption/decryption/zone key translations and PIN authentication to be done in tamperproof hardware security modules.
- The SIM/STK initialization process must be conducted in a secure environment where encryption keys are not exposed.
- PIN keys must be appropriately managed in accordance to industry best practice.
- Transaction monitoring and limits on activity are needed to be in place to ensure a security breach is detected quickly and the damage is limited.

These measures will lead to and an extremely secure system similar if not improved on ATM security.

Why is this approach so rarely implemented?

- Cost and associated logistics. A SIM replacement program is often necessary and although this may seem an overwhelming task, if planned and executed well it can be achieved with the minimum amount of pain.
- Mobile payment services are rarely developed by payment specialists. Payment specialists who have only worked in the card scheme environment are also unlikely to be fully exposed to the technical solutions available.
- Mobile Network Operators seem unable to co-operate with banks and other parties. They want to own it all and are likely to miss out in the long term.

The last point is critical. The mobile operators have two strengths to offer mobile payments. Firstly they have the greatest reach in terms of customer penetration and secondly they control the SIM real estate.

Many mobile payment providers and banks are looking for non-SIM based security options. They are clearly dissatisfied with the level of MNO co-

The Goldfinch Report: *Risk And Security*

Published by *Paycrest*

Written By Peter Goldfinch

operation. Many of the criticisms leveled at banks are now being leveled at mobile operators. Therefore banks in particular who are able to both measure and manage risk are exploring and in some cases implementing mobile handset memory security based on one-time passwords, derived encryption keys and multi-factor authentication methods.

So what is the general state of mobile payments from a risk and security perspective?

The solutions that have been delivered range from being text based with a password through to full STK deployment. In effect no security through to non-repudiation level security. The middle ground seems to be USSD or WAP deployments where security at its best is similar to Internet security. Internet level security will not allow mobile to achieve its full potential. Banks will use mobile only to the level they use the Internet today. These two payment delivery channels will then develop in tandem, and without telecommunications companies participating. Mobile network operators will and are being marginalized as both handset and network capacity improves. Mobile operators need to change their strategy and move away from the stance that they own the end-to-end payment services. Yes they may gain some initial traction but with poor security and inexperience in risk management they are easy targets for fraudsters and they will be attacked. The banks need to be convinced high level SIM based security can be delivered across a mobile service. This has been achieved and is operational today. Combine this security with other risk management techniques relating to usage monitoring and limits then the risk of attack or the impact of an attack will be reduced significantly. Regulators will become more comfortable with mobile. Customer confidence will grow.

This will only happen if banks and mobile operators are able to work together. A significant trend in industrialized countries has been for banks to out-source or sell off their payment delivery channels to service providers.

The Goldfinch Report: Risk And Security

Published by *Paycrest*

Written By Peter Goldfinch

The mobile payment delivery channel can be owned and operated by mobile operators but there is a requirement for the systems and processes to meet bank and regulator security and processing standards.

It is important to remember mobile payment services are still in their infancy. The threat of a major security breach on one of the high profile MMT deployments will have a catastrophic impact that will take many years to overcome. But it is due to happen. It is like waiting for the earthquake, you need to prepare.