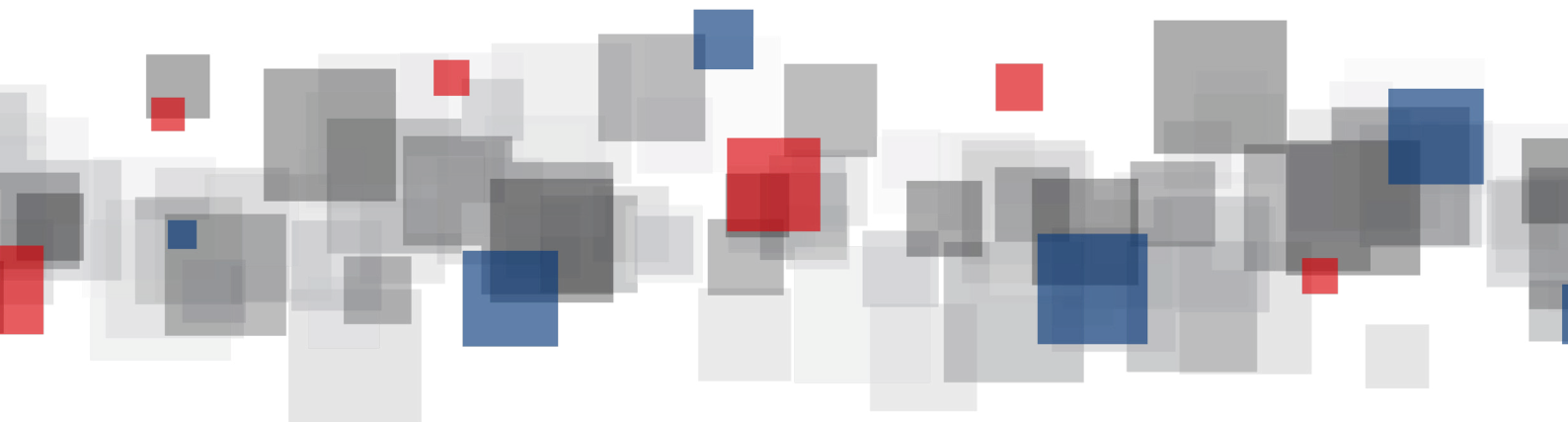
White paper

COMPASS PLUS TECHNOLOGIES

The rise and fall of a fraudulent transaction

How a multi-layered approach can combat the constantly changing threats from financial fraudsters



Executive summary

The financial services sector has undergone a transformation in the last ten years. Customers no longer need to visit their bank – Internet, mobile, and self-service kiosks including ATMs now provide access to services at all times. Whilst cash and cheques still have their place, credit and debit cards are universally accepted, and the mobile phone is moving to take its place as a popular way to pay.

Whilst this evolution has opened up much wider access to financial services, the shift to online banking, e-commerce and mobile wallets has also presented a whole new range of opportunities for criminals. Payment fraud is a global issue, as its perpetrators embrace the electronic age and defraud unsuspecting individuals and organisations worldwide.

The cost of fraud is not simply financial loss. Financial institutions have to bear a number of hidden costs, including loss of customer confidence and damage to their brand and integrity.

This paper explains how fraud happens by looking at the various types of fraud that are prevalent today, the hidden costs of fraud, and how the criminals gain access to the most valuable of assets – customer data.

We track the rise and fall of a fraudulent transaction and examine the ways in which financial institutions can protect themselves and their customers against becoming just another statistic in the ongoing fight against financial fraud.

The methods and mediums in which fraudsters operate are constantly changing. This means that today there is no single line of defence against fraud. Financial institutions must deploy multiple levels of protection that are layered in structure to provide the best defence possible. The integrated deployment of anti-fraud tools as well as proactive and reactive data management and analysis can be powerful weapons in the prediction, prevention and control of fraudulent behaviours.

Fraud overview

The advance of technology and the breadth of access to global electronic communications have created a fluid environment that means fighting fraud is a 24/7/365 challenge.

Thieves adapt – from highwaymen through to hackers, criminals have always employed the most effective means to achieve their goal. The IT-literate criminals of the 21st century are constantly refining their skills.

The proliferation of credit and debit cards and online transactions, the growing popularity of Internet and mobile banking, and the increasing use of the mobile phone as a payment device provide numerous avenues for fraudsters to explore.

Fraudsters operate in a number of ways, and financial institutions and their customers need to be vigilant and aware of the routes that criminals will use.

- **Malware** – also known as malicious software is used by criminals to infect the customer's Internet access device with a Trojan - code that can identify when the customer is using a card for online purchasing, or when accessing a bank account online. Trojans are also being used to intercept and redirect real-time money transfers as well as steal and store a customer's card details.

- **Phishing** – when customers are tricked into disclosing sensitive data either by phone, email, or by entering their card details or Internet banking access codes and passwords on a fake website.

- **Skimming** – the copying of card data during a legitimate transaction, or physical cloning of cards, for subsequent fraudulent use by thieves.

- **Internal fraud** – the skimming of data, including physical cards, by dishonest employees for selling to criminal contacts. Poorly managed access rights can result in an open door to sensitive customer information.

Customers' personal information gained through phishing or malware can be used to break into online bank accounts. Card data obtained by skimming, phishing or malware and Trojans can be used to acquire goods and services in a Card Not Present (CNP) environment. Stolen physical cards, or skimmed (also known as cloned) cards, can be used to buy goods and services as well as to acquire cash at retail outlets and ATMs.

The routes described above are not mutually exclusive. Fraudsters will deploy automated processes and will attack anywhere there is a weak link. For that reason, financial institutions must have multiple layers of protection in place, and implement fraud prevention as an integral part of their overall business and operational strategies.

The cost of fraud

Financial institutions used to regard fraud as an accepted expense – a 'manageable' percentage of the costs associated with day-to-day business operations. Today, taking that approach and simply accepting that fraud happens would see the associated costs escalate rapidly.

Fraud trends vary around the world, and comparable statistics are not available, but the direct costs of fraud alone are damaging and have to be absorbed by financial institutions. CNP fraud statistics are regularly highlighted by the press and phenomenal across the board. However, due to the reputational implications, financial institutions often do not report the number or the cost of these fraudulent attacks. The likelihood, therefore, is that these statistics provide only half the story.

However, the impact of fraud is not just measured in money lost. Fraud can cost huge sums in lost revenue but brand damage is arguably more significant. Brand damage as a result of fraud will significantly impact the financial institution's ability to compete for new business and retain existing customers.

According to Gartner, more than 45 per cent of U.S. consumers have altered their online behaviour because concerns about fraud have made them more mistrusting of email and e-commerce. Financial institutions have to invest in reassuring their customers. One example of this is ANZ bank in Australia and New Zealand, which has invested in a dedicated division that tackles fraud, marketed to customers as the ANZ Fraud Squad.

Published reports on fraud prevention strategies often highlight how victims of fraud behave towards their bank. A surprising amount of of customers are willing to close their accounts depending on the severity of the attack and the banks response and treatment of the customer, demonstrating how easily business can be lost. In the case of compromised cards, even replacing the card may not retain the customer. Card replacements take time and the customer may use that time to take their banking business elsewhere.

Although the cost of fraud is without doubt significant, according to certain sources some types of fraud are falling. This does not mean of course that there has been a reduction in fraud attacks; it means that financial institutions are uniting in the fight against fraud. Complacency is not an option however, as the fraudsters will continue to target the weakest link in the chain.

Overall, it is clear that the implications of fraud go far beyond direct cost.

The layers of fraud protection

Phishing is on the rise. An "attack" is defined as a phishing site that targets a specific brand or entity. One domain name can host several discrete attacks against different banks, for example.

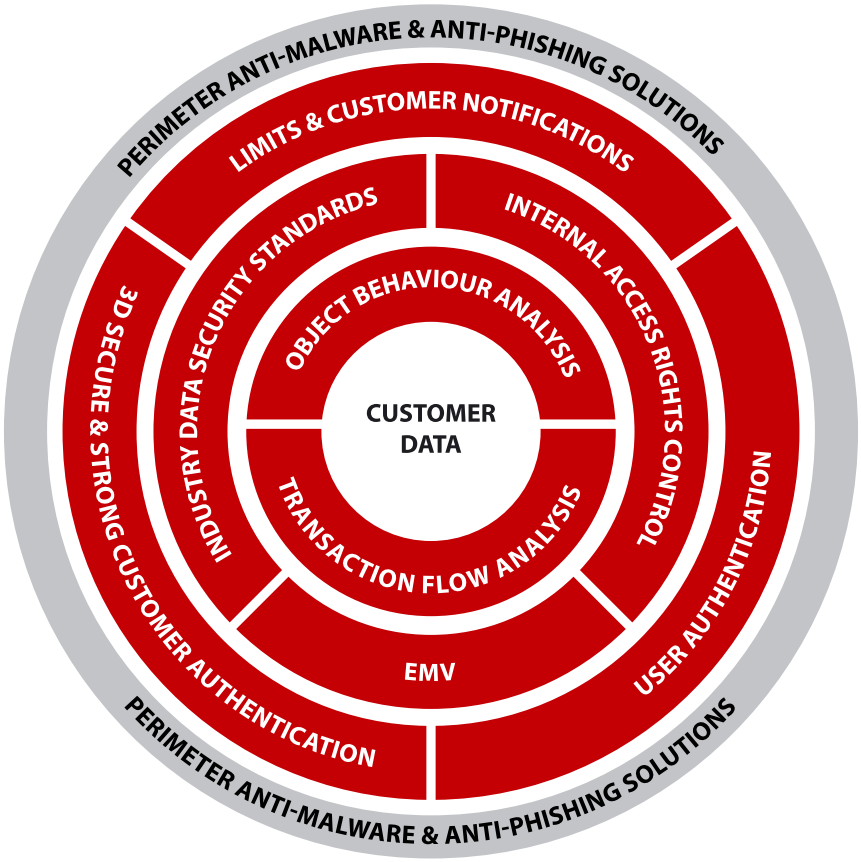
Malware is arguably the greatest concern. According to Gartner, 37 per cent of U.S. banks pointed to malware as the number one fraud threat.

The perimeter

There are a variety of specialist suppliers that can provide browser protection services, security certificates, malware detecting software and anti-phishing solutions. This is the perimeter for fraud defence. These are certainly important in the battle against fraud, however, they only provide a first layer of defence and one that can be successfully negotiated by the fraudsters as the statistics above illustrate. Financial institutions need to ask the question - what happens after the criminal has breached the perimeter fence?

Beyond the perimeter

Financial institutions should take a multi-layered approach to fraud protection that provides a range of measures across multiple channels, transaction types and objects (card, account, cardholder, merchant, etc). Furthermore, these measures should be integrated to create a cohesive strategy that forms the cornerstone of a financial institution's fraud management network. The diagram below illustrates this approach.



Layer #1: User authentication

The first layer of defence beyond the perimeter is to safeguard a customer's account details from malware and phishing attacks, or significantly limit the damage if the fraudster has already obtained these details.

For Internet banking and mobile banking, there are a number of increasingly sophisticated methods of user authentication. We evaluate these below:

- Virtual (on-screen) keyboards prevent malware tracking keystrokes.
- Dynamic passwords – where the user is asked to provide certain characters of a memorable password. However, these are prone to a 'brute-force' attack, especially if it is a simple one word passcode, or of limited characters, where malware will try every possible combination to gain access.
- One-time passcode (OTP) – this is where a password is provided via email or text to the user to provide online access. However, the fraudster could also gain access to email or the mobile phone to steal the OTP.
- Biometrics – where the use of fingerprints, irises, faces and even voice is used to authenticate a user as an extra or alternative layer of security.
- Hardware tokens – these provide an additional layer of security by asking the user to enter a PIN on a device to gain access to the OTP.
- Visa Dynamic Passcode Authentication (DPA) & MasterCard Chip Authentication Protocol (CAP) - this is where an OTP is randomly generated by a crypto-calculator such as a Barclays 'PINsentry' using a customer EMV complaint card and customer PIN. Together they enable the customer secure access to their account online and increasingly via mobile phones and tablets.

DPA/CAP is one of the most sophisticated authentication processes because it requires three key security measures: PIN, OTP and EMV card. It is extremely difficult for all three of these measures to be compromised by a fraudster.

Transaction signing

Should there be a case where the above log-in authentication methods failed, transaction signing (digital signature) can be used to reinforce security. Transaction signing requires the same process as DPA/CAP to embed transactions details, which only they would know, to generate a random one-time digital signature. If hackers attempted to change details, the signature would be void and the transaction would not be approved.

With these procedures, even if the customer's log-in details had been obtained through malware or phishing, the introduction of one-off random passwords, particularly if entered using a virtual keyboard, would typically render the fraudster's information useless.

Proportional security

An approach to user authentication at log-in or transaction signing that financial institutions could deploy is proportional security. Proportional security provides tiered access to a user's account depending on the level of authentication. This means that even if a customer's login details had been skimmed, and the malware detected the input of a random password, there is another level of information required from the customer to access other services available on the account.

For example, financial institutions can require the account holder name, membership number and semi-dynamic password. At this authentication level the customer can only view account details. If the account holder wants to transfer money to existing payees or between their own accounts they would require an OTP. In order to set up a new payee, or transfer funds to a new account the customer would need to use DPA/CAP. In this case, new payee set-up can only be performed on a PC.

Often customers find OTPs and other methods of authentication cumbersome to use, which means services simply won't be adopted. Fraud layers such as proportional security offer high customer convenience with maximum customer security.

To illustrate how these different authentication methods work together in tandem: say that a customer's log-in details have been skimmed by malware but you are protected by an OTP, that information is then rendered useless. However, there are forms of malware that will activate when the customer is successfully logged-in, it can immediately access, set-up a payee and remove funds from the customer account. At this point proportional security becomes invaluable. The financial institution can set strict requirements for user authentication in the case of payee set-up by asking for DPA/CAP, OTP authentication whilst keying using a virtual keyboard.

All of these technologies together will go a long way to preventing a malware-based attack. These procedures are also relatively inexpensive and easy to implement.

Layer #2: 3D Secure & virtual cards

Another layer of fraud security in the online customer not present (CNP) environment is 3D Secure and Virtual cards.
3D Secure provides Internet transaction authentication. Customers need to opt in, and will recognise 3D Secure as the Verified by Visa or MasterCard SecureCode authentication window that appears as part of an online transaction process. The authentication process will either be automatic, or will ask the customer for some further information if the transaction is deemed to need further authentication.

'Virtual' cards also provide an incredibly robust defence against fraud. This is where a one-off 'card' is issued online or at an ATM, with disposable details. Usage parameters are set by the customer – these could include expiry date, number of transactions allowed, single transaction limit, and so on. Provided the usage window is narrow and the limit low, then if the card details are skimmed by malware at the point of transaction, the information will be completely useless. Virtual cards are also cost effective and don't require the issuer, acquirer, card scheme, merchant and cardholder to all adopt the method to implement.

Layer #3: Limits & customer notifications

Let's say layers #1 and #2 for CNP protection have been breached. There is a simple layer, through customer notifications, that can limit fraud.

Customer notifications via email and SMS can be used to alert a customer to account activity and if that activity has not been initiated by the customer, an instant call to the financial institution's fraud department will prevent further unauthorised transactions taking place.

Furthermore, SMS notifications in particular aren't just limited to mobile banking customers and can be used for all types of transactions or for transactions over a certain limit to reduce costs.

Financial institutions should also be able to set and revise usage limits. A sophisticated limit system has an almost unlimited range of configurations based on cards, online transactions and locations in terms of size of spend and frequency as well as type of channel, so an automatic block is invoked if the limit is exceeded. This can range from the basic, how many times your PIN input can fail, to limits based on the number of times you can make withdrawals from an ATM in predefined locations. This layer of protection will at least limit the losses if the customer account is being fraudulently used.

Certain limits can also be controlled by customers via multiple channels, allowing them to reduce the impact of potential fraudulent attacks when travelling abroad.

Layer #4: Transaction flow analysis

Unfortunately, the layers that control access to bank accounts and card holder details sometimes fail. Malware has been successful or a customer has 'surrendered' their account or card details via phishing or skimming. What happens next? The answer to this depends on whether the financial institution has further effective layers of protection in place.

Fraud is an adaptive crime and therefore, as an additional layer of protection, requires special methods of intelligent data analysis for its detection and prevention. Many authorisation systems have their own built-in tools for the implementation of fraud prevention algorithms that are capable of preventing fraudulent transactions at the authorisation stage. However, not all types of fraud can be immediately and definitively recognised and distinguished from unusual cardholder behaviour.

Complete and comprehensive analysis requires vast computational resources that may slow down the authorisation process and exceed the timeout allowed to process a transaction. A good fraud prevention solution needs to complement early online detection and the prevention of potentially fraudulent transactions with statistical post-authorisation analysis of the activity of cardholders, terminals and other objects. This way the transaction flow and object behaviour are both analysed, together arguably offering the strongest layer of protection.

Transaction flow analysis is a methodology using the comparison of the parameters of the current and previous transactions as well as a comparison of the statistical parameters. Each transaction is analysed based on rules and algorithms defined by the bank to detect suspicious transactions. This analysis can be carried out in online and quasi-online mode. The main difference between the two is that online analysis can be carried out at the authorisation stage and offers the option to decline the authorisation, whereas quasi-online analysis is applied to transactions that have already been performed and therefore cannot influence authorisation, although it does help the financial institution take measures to prevent future fraud attempts.

Should a transaction appear fraudulent, alerts are generated and depending on the settings, an algorithm can also trigger system actions, such as an automatic email or SMS notification to a bank clerk, cardholder or retailer, blocking the card, or changing the limits, etc. An immediate system response to suspicious transactions minimises potential damage from fraudulent activity.

Algorithms used for the transaction flow analysis enable the analysis of the details of a particular transaction or several transactions associated with the controlled object, as well as accumulated statistics for all controlled objects, including their risk levels.

Layer #5: Object behaviour analysis

The statistical analysis of object activity (cards, merchants, etc.) enables the tracking of changes in an object's behaviour by analysing its activity over a certain period of time to accumulate statistics. This type of analysis is usually carried out in offline or quasi-online mode at regular intervals.

The fraud system should enable the analysis of activity and the calculation of average indices for both simple and complex objects. Simple objects are cards, accounts, retailers, terminals, countries, BINs, etc. Complex objects are a card and a terminal, a card and an account, a terminal and a BIN, etc. Controlled objects can be complemented with transaction parameters forming even more complex objects for analysis, e.g.: a card, a terminal and a period of time. The analysis of these complex objects enables the full definition of the behaviour model of the controlled object and the detection of signs of unusual behaviour. Each system object is assigned a risk level which can be adjusted in response to the change in object behaviour. This is a convenient and self-learning parameter that can help to decide whether certain transactions are allowed for certain objects.

Layer #6: Internal Access Rights control

There is a further layer of security that must be considered, and that is the protection of data against internal fraud.

Breaches may not all be malicious or intentional, but a system that controls internal access rights to sensitive information, requires permissions from more than one individual to access sensitive information, encrypts all data as a matter of course (including algorithms, rules, etc.) and maintains automatic and detailed audit trails, will provide a strong deterrent to those looking to perpetrate internal fraud.

One overarching safeguard should be implemented: no single staff member should have individual control over fraud systems. For example, algorithm design staff needs to be separate from the implementation staff (those that set up limits, their values, etc). A financial institution can also benefit from giving different access rights to the operators that monitor and investigate fraud incidents.

Layer #7: Payment Card Industry Data Security Standards

There are a number of industry standards that add an additional layer of security for financial institutions. In 2006, card schemes came together to form the Payment Card Industry Security Standards Council, which mandates security standards for payment card processing and management. These include:

- The Data Security Standard (PCI DSS), a set of requirements designed to minimise misuse of payment card data.
- The Payment Application Data Security Standard (PA-DSS), designed to minimise vulnerabilities in payment applications.
- PIN Transaction Security (PTS) requirements that must be followed by device vendors and manufacturers of PIN terminals.

Any organisation which has responsibility for payment card processing must be compliant with the relevant standard or standards, which are designed to prevent, detect and react to fraudulent transactions.

Layer #8: EMV

Physical card fraud – commonly known as skimming - has been reduced by the introduction of the EMV card, a further security layer. EMV has been widely adopted across the globe with varying incarnations from chip and PIN to chip and signature. Dynamic Data Authentication (DDA) EMV cards are more secure than the earlier Static Data Authentication (SDA) EMV card. DDA cards store an encryption key that generates unique data for each transaction that is only valid for one authentication. By contrast, the signature used for SDA cards is the same every time. By reducing static verification methods, it allows card issuers and merchants to diminish the value of stolen cardholder data. The introduction of DDA means that even if payment card data is skimmed, the counterfeit card is useless at the point of sale.

The evolution of fraud: future threats

Fraud patterns and types alter over time, and the fraudsters' ability to create new types of Trojans, new malware programmes and more convincing phishing approaches is constantly changing and evolving. The problem for financial institutions is adapting to new types of fraud that evolve in both sophistication and scale rapidly.

Threats to the security of data are growing at an unprecedented rate. As more and more people are moving to online and mobile banking and making CNP online transactions, fraudsters, who are large scale successful, albeit criminal, business in their own right, are shifting their focus to take full advantage.

The continued advance of the mobile device into the financial services markets is gifting another avenue to fraudsters, as smartphones and tablets are used for Internet and mobile banking, as are mobile wallets, and NFC contactless payments – more often by younger people who may not be as security conscious and actually lean towards convenience over security. Social networks are also being to be used by fraudsters to assume identities and gain valuable personal information.

The proliferation of these new types of fraud is not at the expense of more established practices, any gap in security will be taken advantage of. Devices, channels and fraudulent methods evolve rapidly. This is why a financial institution needs to partner with a specialist vendor that can help it adopt a multi-layer, integrated approach to fraud protection using the latest technology available.

Conclusion

Financial institutions operate in complex and rapidly changing business and technology environments. Just as there is no single type of fraud, there is no single solution to the problem.

Financial institutions must take a holistic approach to securing their systems and data. Fraud happens, but it is imperative that financial institutions stay one step ahead of the criminals by having the intelligence and capability to protect the customer regardless of when and where they may strike.

Of course, fraud costs money, but the indirect cost of reputation damage and loss of customer trust cannot be underestimated. Financial institutions need to understand how fraud happens, and have a robust strategy in place that assumes the worst and can deal with it.

Whether fraud is attempted from outside in, or inside out, financial institutions must plan and implement a multi-layer security strategy to protect and defend customer and card data; to proactively identify and compile fraud activity patterns to predict and prevent future activity, and use real-time monitoring to detect potential threats.

Sophisticated fraud detection software can identify common fraud patterns and then track and block suspicious activity automatically, managing fraud and minimising risk through analytical solutions.

Financial institutions need to seize the initiative and demonstrate that they are ahead of the curve when it comes to fighting fraud. A collaborative, integrated, and multi-level layered approach will enable financial institutions to offer their customers peace of mind, guard against brand damage and fines resulting from data breaches, and ultimately reduce the cost of fraud.

Copyright© 2018 Compass Plus Ltd. All rights reserved