

## Protect Yourself Against The Fraudster

---

*With ambitious and ever-evolving techniques, the financial criminal remains a frustrating and slippery adversary. Are banks and other financial institutions using adequate anti-fraud methods to safeguard their revenue and reputation?*

By Johann Grennepois

### Introduction

The financial criminal is a fearsome character within today's society: fraud is estimated to cost UK businesses £14bn per year. Results from a recent study reveal that more than one in 10 UK consumers have been the victim of identity theft and fraud. Issues around fraud and security have plagued the UK's financial services industry for the past decade.

With domestic and international unauthorised transactions on the increase, the harmful impact of fraud on the revenue and reputation of financial services firms is gathering pace. Negative publicity, increased operating expenses and loss of income have forced both small and large players to seek and implement strategies to detect and deter organised theft and other fraud.

Yet, even with heightened financial crime vigilance and counter-measures, difficulties emerge in a climate where sophisticated and strongly integrated systems are being used by fraudsters today. Banks and other financial institutions need equally comprehensive systems and processes to protect the industry and the consumer from today's organised financial crime.

### Fraudsters' methodology

Predicting the future guise of financial crime in the UK is impossible without first understanding what makes certain activities more appealing to the perpetrators. Typically, fraudsters prefer activities and channels that enable access to assets through minimal effort, with few obstacles and large gains. Rather than going for a small quick win, fraudsters are focusing on how best to gain valuable information on people and processes. For example, knowing which call centre positions have access to customer details or what answers are needed to pass a lending scorecard can open up a repeatable source of income. A large value scam is likely to be quickly spotted and closed down.



Furthermore, if caught, the fraudster is likely to face a severe sentence. Even though the smaller, repeatable activities quickly result in large losses, it is difficult for an organisation to link them all to one person and thereby to make the crime large enough to interest the police.

Today's fraudsters operate with increasing sophistication and are highly organised. They seek to exploit the vulnerabilities within organisations' processes. Increased speed and automation of banks' decision-making processes have benefited fraudsters, who often manipulate credit scoring and behavioural tracking systems. In addition, the slow evolution of decision-making processes enables fraudsters to perfect their craft through trial and error.

It is also important to comprehend the fraud techniques that have been used to target financial institutions and their customers. Understanding and quantifying the problem is the first step towards effective prevention. Trojans, skimming, phishing and sleeper fraud demonstrate the speed with which fraudsters are innovating, much to the frustration of the UK's law enforcement community and financial services industry.

Fraud against financial services companies takes two forms:

- First-party fraud – where the fraudster opens a new account with their own or with forged details.
- Third-party fraud – where a third party executes a transaction pretending to be a genuine customer of the bank.

## Sleeper fraud

First-party fraud is a major concern for financial institutions. It is more complex to detect than third-party fraud, as its effects – losses – are often hidden within a financial institution's bad and doubtful debt charges, and so can fall into the crack between credit risk management and fraud prevention. 'Sleeper' fraud, where fraudsters open new accounts with the intention of taking funds at a later date, appears to be on the increase worldwide. Analysts predict that sleeper fraud losses to US banks will hit \$2tn by the end of 2005. The UK will undoubtedly continue to follow.

The typical perpetrator will first endeavour to open a current account. Cash will then be deposited into the account, and the money withdrawn at an ATM shortly afterwards. These actions will be repeated for several months and, in this way, the fraudster simulates normal banking activities that are likely to see the perpetrator fast-tracked for other applications. When the fraud finally happens it is likely to run into many thousands of pounds, across loans, credit cards, overdrafts and multiple cheques all for the guarantee limit.

Early profiling identified, amongst other things that many fraudsters were "paid in cash". Whilst such profiles had some initial success in preventing losses the fraudsters quickly moved on again.



The more sophisticated sleeper fraud now involves using the façade of a legitimate business enterprise to engage in fraudulent activities. The 'company' will make regular payments to fake employees to imitate salaries, which will be then paid back to the company one way or another to simulate revenue and on-going cashflow. In this way, both the company and its "employees" appear to be good customers allowing them to obtain large unsecured loans.

The combined losses on business and personal accounts typically run into hundreds of thousands of pounds. Furthermore, in many cases the fraud also goes beyond the financial services industry and impacts include insurance, telecoms, retail and benefits fraud. Again, this activity was initially easy to spot as the company's bank accounts were held at the same institution as those of the "employees". Now, however, fraudsters are opening bank accounts with a variety of institutions to help them to simulate a legitimate business.

Counter-measures include behaviour recognition systems which can identify typical sleeper account practices. Neural networks have enjoyed some initial success in this area. However, with their performance being so similar to regression models, in reality all they are doing is correcting misalignment in the original risk scorecards.

To find the optimal solution the problem needs to be approached from many different angles. For example, not just at the account or customer level, but also investigating transactions across accounts, or by sales channel, branch, ATM and employee.

## Skimming

Card skimming, which provides the raw ingredients for counterfeit card production, occurs at ATMs and retail outlets. It is the fastest-growing fraudulent activity in the UK, and the most common type of third-party fraud. Losses accelerated from £8m in 1995 to £130m in 2004. Banbury, Oxfordshire's pretty market town, was recently labelled the 'skimming capital of Britain', after trade body APACS revealed that all 28 of its town cash machines had been targeted by fraudsters.

Fraudsters typically attach reading devices known as "skimmers" to ATM card entry slots or swipe it through a machine in a bar, restaurant or petrol station in order to read the magnetic strip data from inserted cards. The information collected can then be burnt onto a blank card or sold on to large producers of counterfeit cards. The fraudster can then either go on an immediate spending spree or withdraw money from the account with the 'cloned' card. Under the Banking Code, the cardholders will be fully protected, with the financial costs incurred being refunded by the banking industry.

To tackle the skimming issue as well as fraud on lost or stolen cards, the chip and PIN system was rolled out across UK businesses and retail outlets in 2005. The data encrypted on each card's



microchip is better protected from fraudsters than that recorded on a magnetic strip. In response, fraudsters have stepped up their efforts to gather PIN codes. The latest high-tech method involves a miniature wireless camera hidden near the ATM, typically in a leaflet holder attached to a wall, to overlook the PIN pad. The footage is sent to a portable computer nearby.

In response, companies like NCR and Taiyo are developing anti-skimming devices that shut down the ATM or cards that use magnetic fields to prevent reading devices from scanning encrypted data. Such systems are starting to be used by UK high street banks in an attempt to eliminate the ever evolving skimming problem. This cat-and-mouse game still has a long way to go.

## Conclusion

Fraud management should be recognised as a discipline distinct from credit risk management. Fraud management benefits from some of the methods applied in the wide field of risk management but is rarely matched in terms of complexity, pace and sophistication. Whilst new technology can be beneficial, it can be hard to recoup large investments with the fraudsters adapting so quickly.

Adopting a more integrated approach towards fraud is necessary as the identification and prevention of the problem requires a multi-faceted methodology. A top-down, goal-driven anti-fraud strategy providing strategic direction combined with a bottom-up, data-driven approach delivering detailed insight will have a more aggressive and effective impact.

Integrating strategies such as manual inspection and data validation to the approach will strengthen the search for the solution that gives the best financial performance, given the customer service, cost and time constraints. Fraud prevention has come to the forefront of priorities for UK banks and financial institutions. Organisations are acutely aware of the growing threat that fraud poses to their businesses and they are rapidly rethinking their fraud management strategies.

Successful implementation of effective prevention strategies will be a source of competitive advantage for financial institutions that can stay one step ahead of financial criminals. Conversely, a poor fraud prevention strategy may well leave you in the unenviable position of being top of the fraudsters' hit list.