RACONTEUR on

This is an independent publication by Raconteur Media

21. March. 2011

FIGHTING FRAUD

© Ikon Images / Alamy

BEATING FRAUDSTERS AT THEIR OWN GAME

BUSINESS RESILIENCE Fraud takes many forms and the digital economy has created many new opportunities for fraudsters. But technology is also helping businesses fight back against fraud, which costs the UK economy a staggering £38 billion a year. **Geoff Nairn** reports

While information technology has made our lives easier, it also opens new doors for tech-savvy criminals to commit fraud. Fortunately, technology can also be used to detect fraud by analysing data and searching for patterns of behaviour that betray the fraudsters.

In recent years, the specialist field of forensic accounting has grown in importance. "In the past, we were the poor relation in the accounting profession, but forensic data analytics is now a hot area," says Paul Walker, head of forensic technology and discovery services at Ernst & Young.

His department has grown from just six people three years ago to more than 70 today. Traditionally, the work involves trawling through accounting records and other types of 'structured' data to find unusual patterns that betray many types of corporate fraud.

DATA

The key to detecting fraud is data – the more, the better – and a 70-year-old mathematical principle called Benford's Law. Irrespective of whether it is accounts payable data or voter registrations, Benford's Law, also known as the first-digit law, predicts that real-world data get distributed in a certain non-uniform way. If the suspect data deviate significantly from the expected distribution, there could be a fraudster at work.

In the business world, frauds typically centre on procurement, payroll and expenses. So, when a business suspects fraud, forensic accountants start by analysing the accounts payable data.

Benford's Law is not the only weapon in their armoury, of course, but it can be surprisingly effective. For example, a dishonest clerk has set up a fictitious supplier on the supplier database. Company procedure requires additional authorisation for payments over £10,000, so the clerk ensures all the payments to the suspect supplier are below that level.

That, by itself, is not necessarily suspicious. However, forensic analysis reveals a large number of payments have 7, 8 or 9 as their first digit, eg, £9,450 or £708. Benford's law predicts, counter-intuitively, that the higher numbers should each occur as the first digit around 5 per cent of the time, while the number 1 should be the first digit in 30 per cent of cases.

A quick check then reveals that the address given for the suspect supplier corresponds to a domestic residence rather than a business. The alarm bell rings.

As well as structured data, recent

CONTINUED ON PAGE 03

Distributed in THE TIMES

Publisher
Heather Sophia Athié

Editor
Claire Manuel

Design
The Surgery

For more information about Raconteur Media publications in *The Times* and *The Sunday Times*, please contact Freddie Ossberg
T: 020 7033 2100, E: info@raconteurmedia.co.uk,
W: www.raconteurmedia.co.uk

CONTRIBUTORS

CLAIRE MANUEL
Former editorial director of Newsdesk Media Group, she is a freelance business writer and editor

PETER ARCHER
Specialist writer on finance and business, he was formerly with the Press Association and NBC

ROBERT FOX
A journalist and broadcaster, he is defence correspondent for the Evening Standard

SIMON MICHELL
A journalist and former business analyst and managing editor at the Jane's Information Group

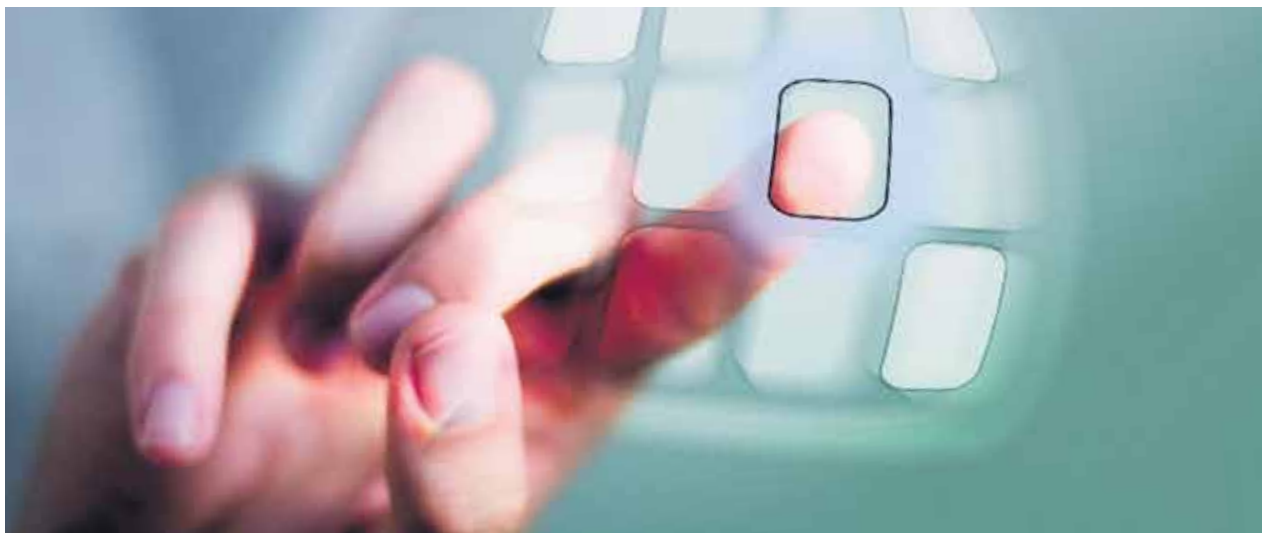
IAN WELSH
A specialist on responsible business and sustainability issues. He is editor of Ethical Corporation magazine

MICHAEL DEMPSEY
Journalist and media trainer who has worked for the BBC, the Financial Times and numerous publications

GEOFF NAIRN
A freelance journalist specialising in IT, telecommunications and, most recently, cleantech and sustainability issues

ROBERT SCHIFREEN
A former computer hacker, Robert is a well-known writer, broadcaster and trainer specialising in IT security issues

GUY CLAPPERTON
Author, broadcaster, speaker and journalist. His latest book, This Is Social Media, is about to go into its second edition



USING TECHNOLOGY TO BEAT FRAUD

CONTINUED FROM PAGE 01

years have seen a tremendous growth in the amount of unstructured data stored in organisations, particularly in regulated industries where e-mails and telephone conversations are now preserved as a matter of course.

Unstructured data pose particular challenges for forensic data analysts. Mr Walker admits that searching though archived phone conversations or e-mail records to find evidence of fraud can be like trying to find a needle in the proverbial haystack.

Nevertheless, it is often the only way to uncover the more sophisticated types of fraud and other 'non-compliant' behaviour, such as price-fixing, blackmail or bribery.

"Our software is able to look for certain words in a dialogue that indicate non-compliant behaviour," says Mr Walker.

SOFTWARE

Advanced data analysis technology is also being used to help businesses fight against fraud perpetrated by their customers.

For the financial services sector, FICO, a US software company, sells predictive analytics software that can flag potentially suspect card transactions in real time.

The software uses neural networks – modelled on the workings of the brain – to analyse transactions against profiles and known fraud patterns. It condenses the historical transactional data of a cardholder down to a few variables that are then used to analyse every transaction in a few milliseconds.

Brian Kinch, FICO senior partner, says the software in effect learns about the cardholder behaviour in a bid to reduce the number of false positives – legitimate transactions flagged as possibly fraudulent.

For example, if a cardholder frequents casinos and often makes several withdrawals of cash from casino ATMs, FICO's software learns this behaviour and knows not to challenge the withdrawals. For cardholders who don't visit casinos, such behaviour is highly suspicious.

One of the biggest problems facing financial institutions when it comes to fighting fraud is that of information silos. At most banks, the fraud management systems have developed in isolation, with one system for monitoring credit cards, one for debit cards, another for online banking and so on.

Fraudsters know this and so they typically spread their attack attempts across different channels in the hope of remaining undetected for longer.

"Multi-channel attacks are what banks fear most," says Duncan Ash, marketing manager for financial services at SAS, a leading vendor of business intelligence software.

HSBC, Britain's biggest bank, uses SAS software to monitor all the credit card transactions of its customers in real time. It is now moving towards a more comprehensive solution that can monitor additional channels and so protect against multi-channel attacks.

"Sometimes there are subtler threats that, when viewed separately, can appear benign. But when you bring them together, you can spot fraud earlier," says Derek Wylde, head of group fraud risk at HSBC.

He gives the example of a customer's credit card, which is used shortly after their debit card and followed by activity on the internet banking channel. Viewed in isolation, the activities are not suspicious, but the three activities happening within a short timeframe is suspect.

Data analysis is a vital weapon in the battle against fraud

> The key to detecting fraud is data – the more, the better

ADAPTING

When fraud management procedures tighten for one industry or fraud type, fraudsters are adept at switching to a new target. The changing nature of fraud also mirrors the ups and downs in the UK economy.

In 2007, application fraud was all the rage as fraudsters took advantage of the UK's credit boom to apply for loans they had no intention of paying back. As much of this business is done online, or through third-party agents, lenders rarely meet the applicants face-to-face.

"Today, there is a lot more remote interaction in financial services so it is very difficult to know your customer," says Brian Kinch, who was head of customer account fraud at LloydsTSB before joining FICO.

This problem particularly affects the insurance sector, with the growth of online operators and aggregator websites that let people 'plug and play' with their personal data to obtain a better quote. "Insurance fraud has always been there of course, but it has been getting progressively worse," says Mr Ash of SAS.

When the credit crunch started to bite a couple of years ago, the era of easy credit came to an end. Instead of trying to create new accounts, fraudsters switched to hijacking existing ones using cashpoint scams and online phishing attacks.

As banks got wise to these attacks, the fraudsters switched to identity fraud as a way to obtain products and services that were not subject to as strict an approval process as credit applications.

Identity fraud used to be relatively minor in the UK, but it now accounts for almost half of all frauds and costs the UK economy more than £2.7 billion a year, according to the National Fraud Authority.

"Identity fraud is the modern-day equivalent of Dickensian pickpockets," says Richard Hurley, communications manager for CIFAS, the UK's fraud prevention service.

ANALYTICS

The fraud landscape is constantly changing. The recession has seen the growth of first-party fraud, in which customers with a good credit history suddenly decide to stop paying off their debts. This behaviour is difficult to detect until it's too late, but Mr Kinch says it is an area where data analytics can help.

"Analytics shows us that there are certain characteristics that are common to these customers," he explains. For example, they will take all the products on offer when they open the account and will try to accumulate as much credit as possible before disappearing.

New types of fraud are emerging all the time. One of the most unusual insider frauds involved a Sainsbury's IT manager who stole more than 17 million Nectar points, worth £80,000, using a series of fake accounts. He was jailed earlier this month. The explosion in social media is also attracting fraudsters, both as a new channel to deliver scams and as a rich source of personal information.

The ingenuity of fraudsters knows no bounds and modern technology has made their task easier. But the good news is that technology can also be harnessed as an ally in the battle against fraud.

FIGHTING FRAUD TOGETHER

Fraud can happen to any organisation. No-one is exempt and every organisation is vulnerable, both to external attacks from customers intent on committing fraud and to internal fraud committed by staff.

To successfully counter fraud, organisations must first acknowledge this unpalatable fact. The next step is to introduce a comprehensive fraud strategy. CIFAS, the UK's fraud prevention service, offers some guidelines based on the experiences of its more than 250 member organisations.

Every organisation, both public and private sector, must have an anti-fraud policy and philosophy embedded and endorsed by its senior management. A lot of fraud can be checked through rigorous verification. Know your customer, know the application and check the application and the supporting identity documents.

Share data if a fraud has happened. If your organisation has been victim of a confirmed fraud, it is important to share data on the fraud through a recognised body such as CIFAS. The bigger the store of confirmed fraud data, the more useful it will be to predict future frauds. The same fraudsters will attack more than one organisation in more than one sector.

Data security is paramount. A comprehensive data security strategy needs to take all aspects into account: from staff recruitment to applications for services. Fraudsters can target them all.