

# Fraud & **Financial Crime**

Special report



Sponsored by

**Detica**NetReveal®

# Cause for continued concern

“I trusted some very intelligent people to decide where my money should go,” remarked one comedian recently, “and, apparently, they decided that most of it should go to them.”

Fraud and financial crime generally are rarely out of the news – and there are many reasons why this is so. No economies have yet recovered fully from the financial crisis, which has now moved into a new and more dangerous stage centred on eurozone sovereign risk. Growth remains weak, unemployment is high and financial markets are still volatile. In these circumstances, banks and the individuals who work for them are under severe economic pressure – leading them, in some cases, to break the rules in search of gain. In some cases, this can mean criminal fraud for personal gain; in others it can mean perpetrating or permitting ‘rogue’ trading in search of greater returns for the institution (and, potentially, larger bonuses for the individual).

There is also a delay between perpetration and discovery – the average fraud lasts three years, implying that many of the frauds initiated around the deepest point of the recession in early 2009 have still not come to light.

This isn’t the only reason for fraud to be a growing concern. As participants in our virtual Q&A noted, the growth of online banking, and the rapid development of new types of criminal software, have led to a significant increase in the threat of online attack. Online finance also means that attacks can be completed much faster – real-time monitoring of customer activity could now involve reacting to suspicious actions in milliseconds. And the push for greater convenience has also opened the way for social engineering frauds.

Has the increase in risk led to an increase in vigilance? Not always – in fact, it’s a continuing concern that control and audit functions may be first on the chopping block when budgets need to be reduced. And, partly as a result of this, most frauds are discovered by chance or due to a tipoff – not because fraud prevention mechanisms have worked as designed. In particular, too much attention is paid to external fraud when the more common – and more dangerous – threat comes from within the organisation. Companies need to pay more attention to their employees and corporate culture to keep the new wave of fraud under control.

The results of the *Operational Risk & Regulation/Detica NetReveal Financial Crime Survey 2011* will be published in the January 2012 issue of the magazine.



Sponsored by

**Detica**NetReveal®

WHISTLEBLOWER BOUNTY COULD DETER UK FRAUDSTERS

UK WHISTLEBLOWING REGULATIONS should include a bounty provision along the lines of the one included in the US Dodd-Frank Act, according to legal experts.

“If a potential fraudster knows there’s a danger that his or her activities are going to be exposed by a whistleblower, they are less likely to commit the fraud,” says Vivian Robinson, a London-based partner at law firm McGuireWoods. “They are also more likely to feel there’s a danger of that happening if they know that a whistleblower may be potentially rewarded. I think this would be an added disincentive to people committing fraud.”

Robinson argues that, while including a bounty provision in whistleblowing regulations may make people who were less likely to report a fraud more encouraged to do so, he warns that following the Dodd-Frank bounty provision to the letter – giving whistleblowers 10%–30% of the recovered monies from a fraud – could have risky consequences.

“Initially the US situation struck me as extreme and a recipe for a lot of gold-digging, so I don’t favour that exactly as it is,” says Robinson. “But I do think consideration should be given to the model the UK Office of Fair Trading (OFT) has in relation to cartel offences.”

The OFT’s model allows for a payment of up to £100,000 to be made in relation to information that helps to identify illegal cartels. Robinson feels this could be a sensible model for whistleblowing provisions to follow. “It’s been tried and tested and it has not been disapproved,” he says. “I don’t see why, if one regulator can use it, then another



Jordan Thomas, Labaton Sucharow

shouldn’t be able to.”

Jordan Thomas, partner at US law firm Labaton Sucharow in New York, is even more convinced a bounty provision could be valuable in the UK.

“The problem that law enforcement agencies in the UK and the US have traditionally struggled with is the lack of actionable intelligence,” he says. “The whistleblower provisions, and specifically the bounty provisions, provide a meaningful incentive that will make individuals speak up when in the past they’ve been silent.”

Thomas also believes such a bounty provision to whistleblowing in the UK could have prevented the huge losses UBS incurred from its recent rogue-trading incident.

“It’s hard to imagine that some of the traders in the UBS case who were seeing the size of the trades

and the success or lack of success associated with the trades would not have suspected something was amiss,” he says. “It’s very probable that whistleblower provisions could have exposed this.”

He continues, “In London many of the people who work in the financial sector are paid a great deal of money and it’s a relatively small community. People who have knowledge of misconduct may fear retaliation and so, even if they want to do the right thing, they have practical concerns about the impact on their careers. Without financial incentives, many of these people will remain silent.”

Robinson agrees but is slightly more cautious. “It’s very hard to say whether [a bounty provision] may have prevented the serious cases of internal fraud that we have seen over the last few years,” he says. “But I do believe whistleblowing provisions that have this additional feature to them would be much more likely to cause persons who might not otherwise have blown the whistle to do so.”

The Serious Fraud Office (SFO) in the UK recently released a new service called SFO Confidential, offering an online and telephone facility for would-be whistleblowers. There is no bounty provision involved and the SFO has no immediate plans for one – but says it is engaging with the debate.

“The whistleblowing provisions in Dodd Frank, in particular monetary incentivisation, is not something the SFO has got a view on and it’s not something we do,” a spokesperson for the SFO says. “We are certainly interested in the debate and in principle it’s not totally alien to the UK because of the OFT’s scheme.”

Jessica Meek

GUPTA ARRESTED OVER GALLEON CHARGES

FORMER GOLDMAN SACHS director Rajat Gupta has been taken into custody by the US Federal Bureau of Investigation on charges relating to the Galleon insider-trading case.

The US Securities and Exchange Commission (SEC) accused Gupta in March of leaking details about Berkshire Hathaway’s \$5 billion investment in Goldman Sachs in 2008 to Galleon Group founder Raj Rajaratnam. He also allegedly gave Rajaratnam inside information on the quarterly earnings of Goldman Sachs and Procter & Gamble (P&G) – he was

a director of both companies.

The jury in the Rajaratnam case heard that, in an October 2008 private meeting of Goldman Sachs board members, it was announced the firm had incurred a quarterly loss for the first time in its history. Phone records showed Gupta called Rajaratnam 23 seconds later, at which point all Galleon’s stock in Goldman Sachs was sold.

Rajaratnam used this insider information to trade on behalf of Galleon’s hedge funds. At the time, Gupta was a direct or indirect investor in some of these funds.

Gupta served as a Goldman Sachs board member from 2006 to 2010, and served on P&G’s board from 2007 until he stepped down earlier this year.

The case against Rajaratnam and his associates made use of a substantial amount of wiretap evidence, a technique not previously used by financial enforcement agencies. Rajaratnam was sentenced to 11 years in prison on October 13, the longest sentence ever handed down to an insider trader in the US.

Mhairi Fraser

Reducing fraud in the information age

Technological advances, volatile markets and a continuing economic crisis make for fertile soil for fraud. Whether driven by need or greed, fraudsters keep the world’s financial institutions under constant pressure. It is no longer enough just to investigate fraud after it happens, companies need to work individually and together to address the underlying roots of fraud and prevent it before it happens

What kind of fraud has become more common or more dangerous as a result of technological advances?

**Vishal Marria, Detica NetReveal:** Attacks against corporate accounts have become more common as financial institutions have rolled out web-based cash/treasury management solutions to their business customers. The availability of Trojan toolkits has increased the pool of potential fraudsters who can now readily procure the technology and know-how to commit online fraud. These attacks have become more dangerous because criminals are systematically probing financial institutions to discover weaknesses, which are then exploited for significant gain.

**Daniel Barton, Alvarez & Marsal:** Technology has made many types of fraud easier to conduct and harder to detect. The rise in the use of mobile devices means that not all emails sit on servers long enough to be recorded. For instance, an email sent by Blackberry and immediately deleted will not be on the server during back-up time – usually overnight. The sheer volume of data and the number of transactions makes detection harder, though this can be combatted through smart analysis using a range of forensic technology tools and techniques.

We also have a wider range of electronic data sources including Facebook, Twitter, instant messaging, Blackberry messaging and other social media platforms. Fraudsters are now better connected and more private information is publicly available. And, of course, most companies now have WiFi and other remote connection protocols, which create additional security vulnerabilities. But the technology to fight fraud has certainly improved, with detection and investigation tools becoming increasingly advanced and efficient – we are able to sift through larger and more complex data sets faster than ever before.

The Panel

**Daniel Barton**, Senior director, Alvarez & Marsal  
**Dean Goodlett**, Assistant vice-president and fraud investigations manager in the financial intelligence unit, Rabobank  
**Vishal Marria**, Director, Financial Services Solutions, Detica NetReveal

**Dean Goodlett, Rabobank:** What is not so clear is exactly what is meant by ‘online banking account intrusion’. For instance, when an account takeover occurs, was the enabling factor an actual security breach within the financial institution, a viral invasion of the customer computer system, a fraudulent act by an authorised user of the account, or the result of the negligent use of social media? While the en- result may be the same, each method of entry into the account requires its own solution. I suggest dividing crimes into four categories: internal system intrusion, external system intrusion, abuse of privilege and negligence.

It is important to understand which poses the greatest threat. At present, although external system intrusions are gaining the greatest notoriety, the negligent release of information is driving the greatest number of online banking account intrusions. The number-one cause of account takeovers for 2010 was a change of address, followed by an added signer on the account. In each of these, there is no need for a system intrusion. Searching across social media or dumpster diving can provide all the information needed to telephone that helpful call centre and get the account information changed.



**Vishal Marria, Director,  
Financial Services Solutions,  
Detica NetReveal**

Vishal Marria joined Detica in 2005 and was instrumental in developing the NetReveal financial services solution. He has been deeply involved in creating financial risk strategies and developing solutions to counter a wide range of financial risk including insider fraud, first party fraud, application fraud, rogue trading, counterparty risk, credit risk and compliance. Vishal heads the Detica NetReveal global financial services team and is currently engaged with major banking and insurance companies around the world. He also has extensive experience in financial crime solutions for government and national security.



We are a global society that stores its banking information on the same unprotected system from which we send out our tweets. Perhaps the 'information age' could also be defined as that time in which we divulged too much information.

I cannot conclude without a brief look into what is often considered taboo. We can protect our own systems, we can educate our customers, we can monitor transactions – but how do we prevent attacks from within? This past year has been one of numerous arrests for 'account surfing'. We talk about preventing the negligent release of account information, but what about the merchandising of that information to the highest bidder?

**How can firms co-operate more effectively on fraud prevention?**

**Vishal Marria:** Ad-hoc information sharing is no longer sufficient to fight sophisticated and organised fraud, especially where fraud attacks can be sudden and high-impact. Institutions are beginning to acknowledge that the systematic sharing of intelligence can improve the bottom line for all member banks. While this represents data compliance and competitive challenges, the rewards can be significant.

**Dean Goodlett:** The problem here is twofold. First, while we all talk individually about co-operation, the fact is our organisations are competitors in the marketplace. And second, we are a litigation-prone global society.

Neither of the above is bad in itself – competition keeps us moving forward and litigation keeps us from solving our problems with violence.

However, competition can prevent us from desiring success for those with whom we compete, and litigation can prevent us from sharing proprietary information.

Until we can overcome the problems inherent in both of the above, our efforts at co-operation will be limited to individual case assistance. The exceptions I find to this occur in seminar and conference settings. The actual instruction and panel discussions are invaluable for sharing solutions, and the personal networks established are often a very good manner in which to address a problem without committing the organisation to the issue.

At present, I believe seminars and conferences and the attendant networking are the most viable methods of disseminating information without invoking the restrictions imposed by competition and litigation. In the future, I would like to think we will move to implement a 'clearing-house' concept among organisations, in which questions could be asked and anonymity retained, both by those asking and those answering.

**Daniel Barton:** It is challenging for this to happen effectively in practice. Companies generally want to keep these kinds of issues internal to maintain a positive image for customers and competitors. In relation to bribery and corruption, we have seen some success with companies operating in the same industry in high-risk geographies collectively agreeing not to pay certain types of bribes or facilitation payments. This works if everybody sticks to the agreement, as a level playing field is maintained. Increased anti-bribery action across the world should increase the number of these agreements in the future.

**What are the key points to remember if you are conducting the internal investigation of a fraud?**

**Daniel Barton:** There are three points to remember: control and confidentiality, completeness and objectivity.

Knowledge of the investigation, certainly during the early stages, needs to be kept to a small number of key people. That way, control of the investigation is maintained and work can be conducted to substantiate the allegation without tipping off those that may have been involved. At the outset, you rarely know with certainty who may have been involved or how widespread the problem may be. Working out who can be trusted to assist with information gathering is a risk that can be managed by keeping the group small, senior and ideally two steps away from those that may be involved.

Ensuring you are obtaining all the potentially relevant data is also key. These days most people have a laptop computer, but you need to ask whether the person or people involved also have an old desktop computer that is still in use? It is essential to get the data from the hard drives of both computers. When interrogating financial systems, ensuring that all potentially relevant fields of information are being downloaded prevents either missing information or the need to go back and re-perform the task.

If suppliers are involved, it is important to have all applicable codes and references. There is often more than one code, especially where there are subsidiary companies or the supplier is doing business with the company in different countries.

Sometimes an allegation of fraud cannot be substantiated and, from time to time, has been made with purely malicious intent. Until you can prove what has occurred, the individuals involved should be treated objectively in case nothing is found. But you must always remain vigilant for any other type of fraud or non-compliance. When you commence an investigation you never know where the trail might lead you or what you might find out.

**Vishal Marria:** React quickly, be thorough and ensure you have a full audit trail. An internal member of staff could have high levels of access within the organisation, which could pose serious harm. Do not assume the individual is working alone. Equally, ensure the facts are correct and an intervention plan on a suspected fraud is clearly defined. This plan should allow for regular checkpoints with senior representation that can verify the findings once the suspected staff member is aware of the investigation – a false positive in the findings can have irreversible connotations.

**Dean Goodlett:** The most valuable lesson I have learned from internal investigations is that they are internal. What I mean is the nature of the internal investigation does not just involve interaction with internal situations, personnel and systems. There is also the internal motive side, and that must be considered when dealing with every person surrounding the investigation. The sad fact is that many internal investigations involve employees in addition to those named in the complaint. And, often those unnamed employees will present themselves as the most desirous of 'getting to the bottom of this'. The true goal of their offers of assistance is preventing knowledge of their own involvement or of protecting an associate. By keeping tabs on where you are going with the investigation, they can actually steer your efforts, and thereby manage the risk to themselves or others. Yes, it is risk management and, as such, these additional employees will have already invested heavily in plausible deniability protection.

Everyone involved in an internal investigation will have an internal agenda for why and how they react to the investigation. Do you know what the internal agenda is for each of these people? Then why would you consider revealing information to them?

**What sort of personnel policies do firms need to have in place to reduce the risk of fraud?**

**Daniel Barton:** Companies should undertake effective due diligence and background screening before hiring senior management and key functional employees. This should also be repeated and refreshed on a regular basis. Having everyone sign up to a clear, concise code of conduct and confirming

**Daniel Barton, Senior director,  
Alvarez & Marsal**

Dan Barton is a senior director with Alvarez & Marsal Global Forensic and Dispute Services in Europe. He specialises in fraud, bribery, corruption and regulatory issues, and has conducted investigations in several countries. Before joining Alvarez & Marsal, Dan was managing director in the Tokyo forensic services practice of PricewaterhouseCoopers.



annually that they have read, understood and comply with the policy is also helpful. Standard practices that have been around for a long time, but are not always properly enforced, include rotation of duties and mandatory holiday to be taken each year. However, policies can only get a company so far. Tone at the top and, importantly, tone at the middle are essential for breathing life into policies and turning them into part of the fabric of the business.

**Vishal Marria:** Performing background checks and screening before an employee is granted full information access is essential, even for junior positions that traditionally may have been seen as low-risk. Ongoing monitoring of employees, associates and even suppliers against internal and external watch lists to flag possible connections to known high-risk individuals, should be part of a 'business-as-usual' policy. Many institutions are taking this a step further by analysing the risk associated with the social network of which the potential employee is a part. This significantly reduces the risk of bringing on board a member of staff who is colluding with fraudsters outside of the financial institution.

**Dean Goodlett:** For the most part, organisations are very good at knowing their new hires. Unfortunately, we do not commit to an ongoing programme of knowing our employees. Once they are hired, we move on. But sadly, situations change for our personnel, and all too often fraud is the manifested result.

Ideally, we would continue to monitor our employees for what is occurring in their lives. But, of course, there is the privacy issue and we can all be grateful it is in place. Besides, even if we knew our employees were facing tough times, what would we do? Would we watch them closely, keep them from being placed in tempting situations, spread our processes among multiple individuals, or implement checks and balances to prevent fraud?

Wouldn't it be smarter to just put those practices into place at first? Wouldn't it be wiser to attack our processes and procedures rather than our people?

Obviously, we do need personnel standards. And those standards should reflect a no-tolerance stance towards fraud from the top down. They should clearly delineate those areas in which the employee has no expectation of privacy. They should advise the employee to report suspicious activity. A copy should be reviewed and signed by the employee. But, even with all this in place, shouldn't we also make every effort to fraud-proof our job descriptions?

People change – the best policies are those that recognise this and place due diligence on the processes and procedures conducted by those people.

**Frauds are running for longer and getting larger before detection. Why is this? And what can be done about it?**


**Vishal Marria:** Fraudsters are running sophisticated and complex businesses, and they spend considerable time and effort testing organisations' systems to allow their activities to remain undetected. A typical large fraud may attack an organisation from multiple angles through different lines of business, channels or products. If organisations are not able to leverage their data effectively to realise a single view of the customer across the enterprise, they can miss the bigger picture and are often unable to detect the organised fraud until too late. Organisations must work proactively to leverage their data to protect their businesses – being preventative, not just reactive.

**Daniel Barton:** Conducting regular fraud risk analysis is a good way of ensuring that your controls are being tested and that gaps are spotted, so that fraud can be prevented – or at least made more difficult to commit. Companies should encourage employees to speak up if they become aware of anything that makes them uncomfortable. The employee does not have to make an accusation that fraud has actually taken place – this is the role of departments such as legal or compliance – but they should be encouraged to speak up and should be provided with an easy means of doing so. These means would include confidential telephone lines and email addresses, visible and active compliance representatives, and an open-door policy for all management.

**Dean Goodlett:** Fraud is an ever-evolving issue that has embraced technology for new implementations and for the ability to change its forms. This has enabled fraud to adapt in order to attack new weak points, and to hide until new detection methods are developed. It has also greatly shortened the amount of time necessary to complete the fraud, as transactions are now completed at the speed of the internet. Therefore a new fraud scheme – or, more often, a repackaged old scheme – can involve a great number of internet-speed transactions before a problem is

**Dean Goodlett, Assistant vice-president and fraud investigations manager in the financial intelligence unit, Rabobank**

Dean Goodlett is the fraud investigations manager for the California division of Rabobank. He received his formal fraud training during a 24-year career in Los Angeles area law enforcement investigations, and holds professional certifications from both the Association of Certified Fraud Examiners and the Association of Certified Anti-Money Laundering Specialists.



realised. Add to this the fact the return-on-investment issue prevents most organisations from investing in a solution for a problem they do not yet have or do not think they have. And when the economy is down, what is the first department to be cut?

The point here is that the fraudsters are better prepared, better hidden, have much less exposure time during the enactment, and are very difficult to discover when the decision has been made to not look.

But the greatest problem we face is the attitude of 'set it, forget it'. We put the safeguards in place and then go back to business. Unfortunately for the fraudsters, the pursuit of business endeavours involves looking for new weaknesses. Ongoing vigilance is a must and the effort must be a concerted one. Software updates, staff training, activity monitoring, customer education and constant vigilance must all be in place or else a weak point will be discovered by those who are looking to find it.

We talk much about combining forces globally to attack the fraud issue. I am all for that. But there are better ways to manage the fraud even within our own organisations. There needs to be a concerted buy-in from the entire organisation to cumulatively attack the fraud picture. I am referring to the Financial Intelligence Unit concept, in which all aspects of the fraud picture are combined under one roof. This involves a shared database and communication between all of those offices that are involved in investigations and monitoring, giving a multi-level and cross-channel view of fraud. Something I am looking at today may have been researched in an anti-money laundering investigation three years ago. Without their input, I am duplicating the efforts and may even miss a lead that is sitting dormant in their database. Only by making use of all the available intelligence can we move forward not only in our response to fraud, but also in preventive efforts as we seek to be truly cross-channel and allow for real-time decision-making.

# A many-pronged attack



Roger Aitken explores some of the issues raised by the UBS rogue-trading scandal – from IT deployments to risk controls and systems access – and canvasses industry players on what steps should be taken to prevent it happening again

The latest multi-billion loss to a rogue trader has turned attention to safeguards against unauthorised trades, but even cutting edge technology is not a perfect solution – much of the time cultural and organisational changes can be more effective.

UBS startled the financial markets when it admitted in September this year it had lost at least \$2 billion – an estimate later increased to \$2.3 billion – to a rogue trader on its London delta one desk ([www.risk.net/2110040](http://www.risk.net/2110040)). In a statement issued shortly after the discovery, the bank said: "Following enquiries directed to him by UBS control functions that were reviewing his positions, the trader revealed his unauthorised activity on September 14."

The statement added: "The true magnitude of the risk exposure was distorted because the positions had been offset in our systems with fictitious, forward-settling, cash exchange-traded fund positions, allegedly executed by the trader. These fictitious trades concealed the fact the index futures trades violated UBS's risk limits" (see box).

Though the full details of the fraud have still not been disclosed, it nevertheless underlines the fact that technology, systems and practices need to be aligned across the entire company – between different enterprises, different asset classes, and the front and back offices – to prevent instances of misbehaviour slipping through.

Software and systems vendors are keen to point out the role technology can play in stopping abuse. Wolfgang Fabisch, chief executive at German software provider b-next in Herford, says: "The technology can [help] and it does. When [our customers are] asked 'Why have you been paying for it for 20 years now?', they reply 'We know why we're paying'. This means they find people and processes and fix the hole in the pipeline. Furthermore, systems generally can reduce losses and risk exposure. And knowing a sort of 'Big

Brother' is monitoring what traders are doing is useful – it brings a bit more discipline. However, this requires having skilled staff to operate the systems and train others."

Other vendors argue new families of software will be much more effective in detecting unauthorised trades. In particular, they point to 'complex event processing' (CEP) engines, designed to take in quantities of information from disparate sources – which could include messaging systems and trade databases – analyse it, detect significant underlying events and respond in real time. Users can specify what they want the analytics to monitor, and what action should be taken when it identifies an event – for example, executing a trade when a price falls below a certain level. CEP is a recent development – to work in real time or near real time, it required significant advances in processing power and the availability of large amounts of cheap, reliable solid state memory to store the large amounts of information it uses.

CEP technology is commonly used in algorithmic trading but is now becoming part of the toolbox for intra-day risk systems as well – and could also be used to analyse trade data for signs of unauthorised trading.

Stuart Grant, financial services business development manager covering Europe, the Middle East and Africa for Californian software provider Sybase in London, says: "CEP is going from niche to mainstream. Technology has always tended to have a way of settling into its most obvious use cases. As such, areas such as trading algorithms and market data analytics were the ones that CEP naturally fell into line with. Now it has expanded into other areas of firms' businesses, such as real-time or near-to-real-time risk management and position-keeping."

In particular, Grant says, equities and foreign exchange specialists are seeing rapid take-up of CEP, both in risk management and trading applications.



“Technology is a major part of it in terms of catching rogue trading and other frauds,” says Frédéric Boulier, director of capital markets compliance and anti-money-laundering for Europe, the Middle East and Asia at software provider Nice Actimize in Paris. “When you have such a system in place with people behind the system who examine and deal with alerts, they make additional searches within their databases to decide whether a situation presents a significant issue or not. However, firms need to rely on much more information than that and interrogate it more fully if they want to effectively catch rogue-trading activities.”

As an example of the kind of information rogue-trading oversight programmes need to take in, Boulier points the 2008 Société Générale (SocGen) rogue trading case, in which equity derivatives trader Jérôme Kerviel lost the bank €4.9 billion through a series of unauthorised trades ([www.risk.net/1498128](http://www.risk.net/1498128)). “One of the things that emerged from the Kerviel case at SocGen was that the trader didn’t take any holiday,” he says. “It’s a legal requirement in such global firms to force everyone in the

organisation – compliance officers or sales staff – to take two weeks’ consecutive leave.” Other data sources might be equally valuable in preventing rogue trading. Boulier, a former investigator at the French financial markets regulator, the AMF, adds: “What strikes me is that the *modus operandi* and the way things happened at UBS is like-for-like the same as what happened at SocGen. The UBS trader took bold futures positions and was heavily exposed on exchange-traded futures, covering trades with fictitious over-the-counter transactions and using forward start transactions where the settlement started well out into the future.”

Under pressure of work, Boulier says, middle offices at many major banks prioritise transactions settling over the next few days. If a trader inputs a fictional transaction with a settlement date three weeks away, then cancels it a week later and inputs a new transaction, this might not be detected – unless the bank has made an effort to include non-traditional data sources in its oversight as well.

UBS fraud: rogue trader followed in Kerviel’s footsteps

In September, UBS suffered a \$2.3 billion loss at the hands of a rogue trader – alleged to be exchange-traded funds (ETF) specialist Kweku Adoboli – in an episode with striking similarities to the €4.9 billion rogue-trading loss suffered by Société Générale (SocGen) at the hands of Jérôme Kerviel in 2008.

Kerviel, like the UBS rogue trader, put on large directional trades using equity index futures – in Kerviel’s case, on the Dow Jones Eurostoxx 50, Dax and FTSE 100 indexes; in the UBS case on S&P 500, Dax and Eurostoxx index futures. And Kerviel, like the UBS rogue trader, hid the fact he had gone far beyond his risk limits by logging fictitious offsetting trades – including forwards and warrant trades. Kerviel chose these because they did not require immediate confirmation or daily margin payments, unlike futures trades, and so would be likely to go undetected for longer. The UBS rogue trader might have chosen to use exchange-traded funds linked to equity indexes for the same reason.

If Adoboli was indeed behind the rogue trades, there are other similarities. Both

men were 31 years old. Both had moved to the trading desk after spending some years in the back office – in Kerviel’s case, his back-office experience gave him the knowledge he needed to avoid detection. And both had been breaking risk limits for years before they were detected. According to Adoboli’s charge sheet, he falsified trading records on ETFs almost constantly from October 2008 to September 2011 – he started work as an ETF trader in September 2006.

The bank said the trader confessed “following inquiries directed to him by UBS control functions that were reviewing his positions” on September 14, implying he might have been able to operate for almost three years without detection – or at least without UBS acting to stop him.

In this respect, too, there could be parallels with the Kerviel case: it emerged in SocGen’s own inquiry report that his unauthorised trades had triggered internal alarms at the bank on 93 occasions, but each one had been ignored or discounted by Kerviel’s superiors and SocGen’s internal control functions.

Shortly after the loss was discovered, chief executive Oswald Grubel resigned. Yassine Bouhara and Francois Gouws, co-heads of UBS Investment Bank’s global equities division, left the bank the next month. One of the division’s two chief operating officers, Niraj Gudka, has also resigned. The bank has also promised disciplinary action against several other unnamed employees in the equities business who were involved in the incident, and against “responsible staff in other functions”. Seven front-office staff have been suspended pending disciplinary action – including the other co-chief operating officer of the division, Sethu Palaniappan.

An internal memo from Grubel’s successor, Sergio Ermotti, leaked to press suggested the unauthorised trades did not go undetected. “Risk and operational systems did detect unauthorised or unexplained activity but this was not sufficiently investigated nor was appropriate action taken to ensure existing controls were enforced,” the memo is reported to have said.

Boulier says: “Firstly, rely on more data for your detection. Don’t just look at trades. Look at operations, at systems logs and examine human resources data. There’s a wealth of data out there looking to be leveraged. Moreover, institutions should not be looking at their risk in silos, but need to think about linking the dots.”

Andy Mellor, risk and compliance product manager at technology provider Fiserv in London, says: “There’s no doubt the correct processes need to surround technology, but there isn’t a technological ‘silver bullet’ out there. Technology is there as an essential component of the bigger picture.”



Andy Mellor, Fiserv

Gary Wright, chief executive of London-based research company BISS Research and formerly head of European settlements at Flemings (now JP Morgan), says: “Having the most sophisticated technological systems in place at global trading organisations to detect market abuse, rogue trading and other frauds is all very well and critical to averting damaging financial losses. However, if people and processes are not integrated holistically – across asset classes and silos as well as across the front, middle and back office – failures will ultimately result. Over the years all firms constantly review and update their risk systems after each high-profile case of fraud, yet they still happen. It’s time a broader view of firms’ overall systems and human interventions was carried out.”

He adds that the culture at many leading financial institutions “propagates fraud” as it’s seen as preferable to disclosure. “There’s a deeper malaise in banks that allows such simple covering of positions and the build-up of huge losses created by people who are new to the business and possess limited experience,” he says. “I’ve yet to come across any bank that has a ‘chief rogue-trading deterrence officer’ like a compliance officer,” says Boulier. “I believe there will have to be someone that is only looking for rogue trading within large financial institutions. That individual would be entrusted with the challenging task of putting data together to secure a holistic view of trading risk across an organisation.”

Simmy Grewal, a London-based analyst at Aite Group covering European capital markets and a former Morgan Stanley equities trader, says much of the necessary software is already in place – but only in the front office. She argues risk management tools need to evolve in parallel or even ahead of such developments. “Given firms have the tools at their disposal for trading, I cannot understand why they’re not also deployed for risk management purposes. At the end of the day, the risk management systems should be a step ahead of a firm’s trading systems,” she says.

“Technology is a big part of the puzzle, but not the only part. It surely has to be about the people, organisation, culture and processes that technology can only support,” says Steve Leegood, a director at Bryok, a London-based IT



Steve Leegood, Bryok

consultancy focussed on securities trading venues. “While I do think technology in the front office is certainly cutting-edge in terms of systems being developed and the programming of trading algorithms, it’s not necessarily as true in the back office, where systems have tended not to receive the same investment and have been developed piecemeal.”

Often the back-office systems that arose out of equities trading environments were largely fine, Leegood says, but once firms got into derivatives “those systems that would not necessarily talk to the original systems”.

He also refers to a “detachment” between the back and front office. “With reference to the UBS case, a number of underlying asset classes were being traded. Therefore, one not only has to consider silos across those various asset classes, but also silos existing across the front, middle and back offices ... a matrix of silos.”

Moving personnel from one silo to another can be one of the biggest sources of risk in terms of rogue trading. Reportedly, the UBS rogue trader – like Kerviel at SocGen and Nick Leeson at Barings Bank in 1995 – was able to carry out his trades because he had previously worked in the back office, and knew enough about the details of trade processing and confirmation to be able to conceal his activities. In 2008, the Committee of European Banking Supervisors (Cebbs) spent several months asking European banks about their reactions to the Kerviel case and published the results. First in the list of causes the Cebbs report cited for the losses was “failure to adequately enforce segregation of duties between front, middle and back offices (for example, moving a middle-office worker directly to the front office, covering the same product)”.

But a ban on this sort of lateral movement might not be practical. “That’s a rather difficult one. It’s quite hard to say middle or back-office staff should not be allowed to move roles within trading organisations,” says Grewal. “Certainly there should be elements around the access they’ve had to operational systems before and these should definitely be checked or revoked once on the trading desk. Traders should not have the ability to be able to go through and amend systems and controls. If they have the ability to amend them, that’s frankly questionable and dubious from a risk perspective.”

Terry Gibson, head of product management and strategy at Fiserv’s investment services group in London and formerly head of product management at the Singapore Exchange, agrees: “There should never really be any restriction of staff moving from back-office to middle-office roles and subsequently into front-office positions. Fundamentally, the proper controls and mechanisms must be in place regarding access across those systems, if personnel do transfer. Knowledge is one thing, but being able to execute something – illegally or otherwise – is quite another.”

# Identify and prevent rogue trading

Detica NetReveal's head of investment banking solutions, Laura Houston, explains how the new networked operational risk model can help to reveal fraud

**B**anks have invested a significant amount of time, effort and money into managing large programmes to implement the mandated regulatory changes in relation to managing operational risk. Unfortunately, control failures are still happening, as high-profile incidents at Société Générale and, more recently, at UBS have demonstrated. They prove that typical control environments are no longer sufficient to prevent incidents from happening.

Weaknesses and holes can exist in every control framework, and these can lead to abuse by accident and as a result of malicious manipulation with intent.

## Finding what you know

The primary objective of a control framework is to find behaviours that are known to be associated with high-risk activities. In effect, they apply business rules that generate alerts when a known control is broken. Through the course of business as usual, these control rules frequently trigger on legitimate business practice, and so typically generate huge volumes of false hits.

It becomes very challenging for an organisation to quickly identify the true abnormalities and high-risk behaviours among the high volume of low-risk alerts – the age-old problem of trying to find the 'needle in the haystack'. Furthermore, the time spent moving through this volume of alerts is significant and it soon turns into a process-driven approach rather than one that aims to proactively find the true risks early.

## Searching for what you don't know

Of critical importance in the struggle to detect fraudulent behaviour is the siloed nature of both the control framework and the product areas within an organisation. While a trader may cancel a trade, it may not be known that this same individual has repeatedly made cancellations, they have not taken annual leave in 18 months and they have been logging in at unusual times. Control areas are disparate, the investigations are conducted separately and frequently the only knowledge shared is by word of mouth. How does an organisation begin to identify the unknown without the capability to understand the more complex, repeated and hidden relationships that exist across different product lines, trading functions and systems?

As banks create increasingly complex control models, rogue traders' methods become more sophisticated. Determined fraudsters understand a bank is a potential collection of control holes and weaknesses that can be exploited and, as one opportunity is closed, they will look for alternatives. It appears that, in recent incidents, the traders in question exploited a broad set of weaknesses across various areas of the bank and employed behaviours they knew would allow them to operate undetected. Their activities did raise suspicions but, because they were isolated incidents occurring infrequently across disparate areas of the organisation, they were not considered



significant enough to take further.

BAE Systems Detica, in conjunction with leading investment banks, has developed a sophisticated networked control model to challenge these current weaknesses, enabling banks to take an earlier and more proactive approach to identifying instances of fraud and abuse. This unique model

transforms a bank's approach to managing operational risk through the implementation of advanced technologies, with methods and techniques used that were originally pioneered by secure government intelligence and defence organisations.

The solution, known as Detica NetReveal networked operational risk model (NORM), gives banks the ability to automatically analyse transactional and control data from multiple internal sources, from the front and back office, and across siloed areas to identify anomalous patterns, hidden relationships and changing behaviours at a much earlier stage.

It offers significant efficiency gains through user-friendly investigation tools and significant reductions in false positives through more effective and sophisticated prioritisation, using the following techniques:

- Cluster and peer group analysis – this provides risk assessments of each employee using the holistic and cross-silo view created by Detica NetReveal, identifying individuals whose behaviour stands out from their peer group.
- Social network analysis – sophisticated fraudsters spread their activities across multiple products, portfolios and systems in order to operate 'below the radar'. They utilise and collude with other individuals and external counterparties to facilitate their abuse. The Detica NetReveal NORM solution utilises social network analysis to link apparently unrelated data from across diverse systems to automatically construct suspicious network relationship models for immediate risk assessment and subsequent visual inspection.
- Unstructured data intelligence – analysing the content of 'unstructured data' contained in emails, documents and other messaging systems, providing an invaluable source of intelligence.

It is important to recognise traditional control frameworks deployed in current systems are based on reactive rules and models that largely describe 'the fraud we know'. Sophisticated fraudsters understand and evade traditional detection. The Detica NetReveal NORM solution can transform a bank's ability to manage its operational risk across the organisation by enabling it to proactively reveal fraud that was previously hidden.