Strengthening the defences

In an interactive webinar sponsored by Wolters Kluwer Financial Services, *Operational Risk & Regulation* convened independent industry experts from Aviva, FinCEN and Wolters Kluwer to discuss the challenges that fraud – be it internal or external, high- or low-tech – presents to financial institutions and how these firms and law enforcement agencies are working to stay on top of financial crime

Regulators and financial firms around the world are not only ramping up their anti-fraud efforts, but are also thinking more strategically about how fraud can be prevented as well as detected.

Fraud is on the rise. According to a recent study, 43% of companies suffered one or more frauds in two years that had a significant impact on their business. Furthermore, a report from the Association of Certified Fraud Examiners (ACFE) in the US last year looked at approximate known fraud cases, saying US companies lost, on average, 7% of their annual revenue to fraud. In the UK, the National Fraud Authority in January said that UK fraud loss is £30.5 billion. Private sector fraud was estimated at about £9.3 billion, and public sector fraud was estimated at £17.6 billion.

The Panel

John Flynn, Head of financial crime, Aviva
Anthony Harris, Senior advisor, Regulatory Policy and Programs, Financial Crimes Enforcement Network (FinCEN)
Nona Tiedge, Assistant director, Office of Regulatory Analysis, Regulatory Policy and Programs, FinCEN
Guy Sheppard, Product manager, Risk, Anti-fraud and Compliance, Wolters Kluwer Financial Services
Tom Leuchtner, Director, Financial Crime Business Unit, Wolters Kluwer Financial Services

Why fraud is on the rise

"Fraud happens generally because there has been a failure of internal systems and controls," says John Flynn, the head of financial crime at Aviva, speaking at the *Fraud and Financial Crime* webinar recently hosted by *Operational Risk & Regulation* and sponsored by Wolters Kluwer Financial Services.

"Most controls in companies are designed to be accounting controls," he says, "how we measure the flows of money inside and out, so they are not necessarily controls that prevent fraud." He adds that, according to a recent ACFE report, 78% of victim organisations modified their anti-fraud controls after discovering they had been defrauded, "which is telling you that the controls weren't in place first of all."

Flynn says, "Many companies have an anti-fraud policy and they display it very proudly. The anti-fraud policy says 'thou shalt not commit fraud' and then no further action is taken, but that will not protect you. You have to think a bit more about fraud risk management and how you will protect against it."

A good anti-fraud strategy is "dependent on who you are," he says. "Aviva is a large insurance company active in 28 countries with varying types of operating structures and different types of environments that we operate in, which means that there is no single anti-fraud risk method that will protect and manage your fraud risk. You have to make it bespoke for your company and for the risk and environment that you face."

Flynn also points out that fraud impacts all aspects of the company, not just the person or department that can be responsible. "If you think about your vast controls – from your HR recruitment policy to your system access control on computers and your payment processes – they are all fraud controls. The problem with a lot of firms is that fraud is considered in isolation and that certain people or the fraud team are considered responsible for managing fraud. It's a responsibility throughout the whole of the company and you have to get that attitude right through the company."

"You've also got to then think about how you focus within an organisation," says Flynn. "If you focus from the top down, you focus on the strategic risk only, then you generally miss the tactical and operational risk areas. If you focus from the bottom up, then you can lose sight of the bigger objective. So you have to have balance and approach it from various different angles."

What components are needed in an organisation to prevent fraud? "You need a prevention team to identify the risk, who can implement the strategy, and ensure that there is a commensurate control framework in place. That's very important to get the right understanding of risks."

When it comes to preventing fraud, it is important to focus on ensuring that a control framework is robust. For example, he says, look at a firm's employee exit procedures and controls. "When people leave the company, make sure they leave as they're supposed to, and not with your laptop, phone, Blackberry and information." Data loss is another significant area of concern, and the number of cases of this will continue to increase, he says.

Another area in which Flynn says to review the controls is malpractice reporting processes – he advocates having an independent malpractice reporting line. "This is vital in information being reported," he says. "Quality assurance is part of ongoing risk management; tested to see if it is effective, and its effectiveness can be monitored. Any internal fraud that I've been involved with has tended to involve some password or ID sharing among

SAMPLE C
not for reprod

John Flynn, Head of financial crime, Aviva
John Flynn is the head of financial crime at Aviva, where he is responsible for providing global oversight of the financial crime policy, a role that involves setting the strategy and risk appetite for the group. This is achieved by delivery of the policy and standards throughout the group, which currently consists of 28 territories. He reports on the effectiveness and risk to the Group Risk & Regulatory Committee. In the last year, Flynn has implemented an Aviva-wide programme introducing anti-bribery and corruption controls and procedures as a consequence of Aviva listing on the New York Stock Exchange in 2009.

COPY
duction

employees. It always happens. Any large internal fraud that we've had has always involved multiple IDs being used. There are lots of areas you can cover under internal fraud, but you have to understand the controls and identify the different departments, what area it is going to occur in, and generally, when something has happened, the controls have been overridden."

"Secondly, you need a reactive investigation team who are there not to solely reactively investigate," says Flynn. "Within Aviva we have a 'zero tolerance' attitude to fraud so, if you commit fraud within Aviva, we will seek to prosecute you and take away any of the ill-gotten gains that you may have taken from us." Flynn adds, "If you suffer an internal fraud, please go after the person. Don't just dismiss them from the company. Go after them to seize the assets, either through a civil case or a criminal prosecution if possible. It sets a very positive message throughout the company, and it sends a positive message that we want to build the company we want it to be."

Firms also need to be more sophisticated and proactive about detecting fraud, using tools such as data mining. "Lastly, to complement both of those prevention and investigation teams, you need a development team," he says. "These are the people that are going to happen in the future – what lessons have we learned and how do we feed that back into our strategy, what's going to come up and really hurt us soon? Because the fraudsters are continually changing, you need to be continually learning, developing control weaknesses and learning lessons."

Ultimately, however, there needs to be somebody who is responsible for fraud – some place where the proverbial 'buck stops'. "Often when fraud – and especially internal fraud – occurs within an organisation, nobody takes responsibility," says Flynn. "You need to identify people all the way through your organisation who have responsibility for fraud. In order to do that, they have to understand what guidance, prevention and investigation are available. You can't make somebody responsible or try to implement the policy, or make them responsible without giving them some guidance on what they should be doing."

But perhaps the most important aspect of a fraud strategy is obtaining senior management engagement and awareness of the risks. "If you haven't got senior management on board then it's going to be very difficult, and they will be forced to make some hard choices about how to deal with fraud," says Flynn.

Helpfully, fraud is on the radar screens of senior management and the boards of many organisations because of the rise in activity in recent years. Certainly within general insurance and possibly within life insurance, "we're seeing an increase in fraud in the UK of anything from 15% to 25% in the last year," says Flynn. "We are seeing an increase in people claiming to insurance companies who will drop the claim when challenged. There is greater investigation being undertaken by the companies into fraud, trying to manage our costs. Yes we are seeing an increase in fraud and, given the economic climate, it is likely that we will continue to do so."

Regulators are also responding to concerns about the global rise in fraud that is both a cause of and the result of the current economic crisis. For example, in the US, the Financial Fraud Enforcement Task Force, an inter-agency group led by the Department of Justice, was recently created by an executive order by President Barack Obama to strengthen efforts to combat financial crime. Just a few weeks ago, representatives of the Financial Fraud Enforcement Task Force met in Miami for the first in a series of mortgage fraud summits – a location that was selected largely because of analysis that identified the Miami/Fort Lauderdale area as being ranked first in the nation for the number of local subjects named in Suspicious Activity Reports (SARs) filed by depository institutions concerning suspected mortgage fraud.

The *Bank Secrecy Act* – a force to be reckoned with

The analysis work on mortgage fraud was completed by the Financial Crimes Enforcement Network (FinCEN). This US regulatory body is the administrator of the *Bank Secrecy Act* – the principal anti-money-laundering and counterterrorist financing regulatory regime in the US. The *Bank Secrecy Act* is becoming a powerful anti-fraud tool for US regulators and law enforcement. Record keeping and reporting requirements cover a wide variety of financial sectors, including the deposit institutions, securities firms, mutual funds, futures firms and money services businesses, such as money transmitters and currency dealers, as well as insurance companies, casinos and card clubs and dealers in precious metals, stones and jewels.

In the US, as is the case elsewhere, financial institutions are required to file SARs. "In addition to their role of spotting money laundering and terrorist financing, SARs also provide information on numerous kinds of fraud, including cheque fraud, mortgage loan fraud, consumer loan fraud, wire transfer fraud, commercial loan fraud, credit card fraud, as well as debit card fraud," says Anthony Harris, senior adviser in FinCEN's Regulatory Policy and Programs Division.

"Mortgage fraud is a very important issue within the US," says Harris. "It is a particularly invidious crime that has robbed many homeowners not just of the roof over their head but often their savings and security. Mortgage fraud we have found is also tied to other serious crimes such as identity theft, money laundering and others. One of the greatest obstacles we have faced is that there is always a new scam, a new angle and new opportunities for criminal actors. Mortgage loan fraud and its close cousin loan modification fraud are prime examples of fraud opportunities in all economic conditions."

Last year the Obama administration announced a new initiative led by FinCEN to combat fraudulent loan modification schemes and co-ordinate ongoing efforts across a range of federal, state, civil and criminal enforcement agencies to investigate fraud and to assist in enforcement and prosecutions. As part of this project, FinCEN also issued an advisory to alert

Anthony Harris, Senior advisor, Regulatory Policy and Programs Division, Financial Crimes Enforcement Network (FinCEN)

Anthony Harris is a senior advisor in FinCEN's Regulatory Policy and Programs Division. In this role, he supports the associate director in executing the division's regulatory functions associated with FinCEN's responsibilities as administrator of the *Bank Secrecy Act* (BSA). Harris previously served in the Regulatory Policy and Programs Division's Office of Compliance, working with regulatory agencies on initiatives to strengthen BSA compliance. In this capacity he has represented FinCEN in interagency initiatives related to BSA examination procedures and training. Prior to joining FinCEN in 2003, Harris was an examiner with the Federal Deposit Insurance Corporation.

Nona Tiedge, Assistant Director, Office of Regulatory Analysis, Regulatory Policy and Programs, FinCEN

Nona Tiedge joined FinCEN in November 2002 as a senior intelligence research specialist, and was selected as assistant director for FinCEN's Office of Regulatory Analysis in December 2004. She manages a staff of 25 intelligence research specialists responsible for providing analytical support to FinCEN's four Regulatory Policy and Programs Division offices and federal and state regulatory authorities. Tiedge served as co-chairman of the *Bank Secrecy Act* Advisory Group's Suspicious Activity Report (SAR) feedback sub-committee. Prior to entering federal service in 2002, Tiedge spent 17 years as a bank vice-president, Corporate Bank Secrecy Act compliance officer and bank fraud investigator at a large south-eastern depository institution.

US financial institutions to the risks of emerging schemes related to loan modifications. The advisory identifies red flags that indicate a loan modification or foreclosure rescue scam may warrant the filing of an SAR by a financial institution, and it requests that the financial institution include the specific term foreclosure rescue scam in the narrative sections of relevant SARs. Including this term will allow law enforcement to more easily search for and identify fraudulent activity when reviewing SAR information, which in turn assists in focusing their investigative resources. Non-US institutions may also find the red flags in this advisory of interest.

FinCEN has a longer history of tracking mortgage fraud than many organisations. "In mid-2004, as our analysts prepared to publish issue three of *By the numbers* for SARs filed through June of that year, we noted a significant increase over the previous reporting period for the number of depository institution SARs involving mortgage fraud," says Nona Tiedge, assistant director at the Office of Regulatory Analysis, Regulatory Policy and Programs at FinCEN. "We began closely monitoring this activity and have since published six analytic reports describing our findings from analysing mortgage loan SAR data, with our most recent report released just last month. You can find those reports on FinCEN's website."

"The filing trend shows a significant increase in SARs reporting mortgage loan fraud beginning June 2003," says Tiedge. "In fact, reports grew by almost 93% between 2003 and 2004, and the upward volume continued through 2009, although the percentage of growth decreased between 2006 and 2008, compared to previous years, but showed a slight increase in 2009. Of course, as you know, this period I have described is the period of the mortgage crisis in the US."

Flynn agrees the fraud-risk triangle – which is a triangle with motive, rationale and opportunity on the three sides – has become even more apparent in recent years. "The crisis has impacted the rise of fraud. People, because of the opportunity – we have seen reductions in staff and size of companies – are rationalising it by saying they need this money to survive or to maintain their lifestyle. Therefore, if the motive is to maintain a lifestyle, or quite often greed, then we will see an increase in fraud."

Internal fraud – cause for concern

Fraud at financial institutions – and concerns about fraud – is on the rise, according to a poll conducted during the webinar. Almost 36% of respondents who attended the webinar said internal fraud was their biggest concern. This was followed by money laundering at nearly 18% and customer ID theft at around 17%.

Today, fraud poses significant problems for financial firms. "The effect on profitability, now that financial services firms have to be so much more cost-competitive and now that the competition for new customers has risen, has been driven so much further up," says Guy Sheppard, who oversees Wolters Kluwer Financial Services' financial crime solutions in the UK and the EU. "These losses must be prevented, and they can no longer be dismissed as this 5%–7% cost of sale. A lack of controls will lead to significant expenditure in managing this loss. For example, this can be through a large regulatory fine now that the UK Financial Services Authority has begun to get more aggressive in going after prosecutions. As well, the sheer practicalities of calling in a consultancy at a significant amount of expenditure per day, per hour, and then the cost of the systems a firm will have to implement to comply after the fact," means an ounce of prevention is worth a pound of cure.

What should financial services firms be doing to combat the rising threat of fraud? There is little doubt that having effective financial crime controls is becoming an increasingly costly business. Says Sheppard: "It can be extremely challenging to keep pace with all the financial criminals. We hear all the time about our friends in West Africa and various 419 scams, and about some of the more sophisticated and better-thought-through schemes that constantly keep financial crime professionals on the hop. These include 'spear-phishing' and some of the gas-station-related frauds that have become prevalent in the US."

Sheppard notes that the current difficult economic environment is also leading to an increase in both internal and external fraud – sometimes via unexpected ways. He says: "I have seen my customers expanding aggressively into emerging markets, which is fantastic from a commercial perspective because it means new customers. But these new customers also often provide much higher risk than the traditional customer base, and the data driving informed decision-making as to whether it is good business or not is often very sparse."

SAMPLE
not for repro

Tom Leuchtner, Director, Financial Crime Business Unit, Wolters Kluwer Financial Services

Tom Leuchtner is the director of the Financial Crime Solutions Group at Wolters Kluwer Financial Services, which currently serves the banking, securities and insurance industries in North America, the UK & Europe. He brings more than 20 years of experience to this role, including an extensive background in software technology from his work at Lotus, Netscape and numerous tech startups, serving in advisory and board member capacities. Leuchtner also has significant experience in the private equity sector, with more than five years of venture capital and advisory experience. He delivers a wealth of experience gained while managing the Paris-based Netscape EMEA product management team and as the founder and chief executive officer of a tech consultancy based in the Netherlands, and is a member of the Association of Certified Fraud Examiners.

Guy Sheppard, Product manager, Risk, Anti-fraud and Compliance, Wolters Kluwer Financial Services

Guy Sheppard oversees Wolters Kluwer Financial Services' financial crime solutions in the UK and the EU, working with customers to ensure that the acute needs and challenges of UK and EU customers are met. Sheppard's previous experience includes developing commercial-grade counterterrorist finance programmes alongside the Metropolitan Police's Counter-Terrorism Command, managing an online information and listings business in Shanghai, as well as establishing a public sector risk and security division within LexisNexis Butterworths to address the data and technology needs of UK law enforcement and security service agencies.

COPY
oduction

Unfortunately, he notes, these rising threats are coming at a time when risk and compliance professionals are under increasing cost pressure. Says Sheppard: "We are assisting customers in writing business cases that successfully argue the point that technology can provide additional financial benefit on top of the reputational risk prevention that might not interest a 'pounds and pence' or 'dollars and cents' financial manager."

"With most of the customers I am speaking with, there is always the 'return on investment' discussion," says Tom Leuchtner, director of the financial crime solutions group at Wolters Kluwer Financial Services. "Certainly it's an important discussion to have. Reputational risk is a difficult thing to quantify, so invariably the dialogue moves towards developing a strategic approach to fraud."

Indeed, the positive side of this need to justify investment in fraud-detection and prevention software is that business lines are gaining a greater understanding of how risk and compliance departments can help them improve the way they engage with clients, and also restructure the cost base around a firm's anti-fraud initiatives. Says Sheppard: "We are constantly getting into deep conversations with members of data or IT security functions, as well as the more traditional risk and compliance departments. There is more of an expectation now that effective financial crime control will rely on sophisticated technology, as well as the internal know-how deployed through that technology. Firms can make head-count savings through reducing the manual review workload and improving their detection and customer profiling."

Leuchtner adds: "What we have seen over the past few years, on financial crime in general, is a drive to leverage the investments institutions are making in their anti-money laundering as well as anti-fraud efforts. Typically, the processes used to sift through transactional analysis, behavioural monitoring, profiling and working a case are all very common activities across anti-money laundering and loss prevention fraud groups. We are seeing a migration towards a combined set of processes and infrastructure."

Another change that is happening at firms – although it is a difficult one – is the move from a detection strategy to a prevention strategy. Says Leuchtner: "This does not have to mean a prohibitive investment in technology. Customers have said they have found the move less difficult than it seems."

According to Leuchtner, profiling is an early aspect of moving to a preventive strategy. "The big challenge is that, by definition, firms are looking at transactional activity, which is by definition historical. The money has left the building. The challenge we face is how to predict when a major loss event is going to occur. Some of it is science and some of it is art. One of the foundational components is profile – looking at the historical activity, comparing current activity in real time to the historical activity and trying to assess whether this current activity is in line with typical behaviour."

This work can be with respect to a customer, an account or an employee, he says. "Traditional systems employ behavioural monitoring through looking at system logs. We advocate a different method, which is to monitor behaviour through network analysis. The other piece is that, as you think about employing some technology, the comprehensive approach – cross-system and cross-channel analysis – comes into view and is achievable. As you're thinking about analysing across different systems, it's important to think about how to unify processes and methods, not only around the technology but around investigations, reporting and auditing, as well as unifying systems to help you look at consolidation of vendor spend and IT project."

Leuchtner says the typical process for moving to a common framework around financial crime control is to look at where the highest risk area is first. "Our customers and prospects are looking at treasury and cash management, online banking, e-payments, wire, automated clearing house or electronic cheques," he says. "Typically, they don't have these kinds of monitoring systems in place, so what they'll do is look to drive their financial crime framework – a product or technology – into place and then leverage that investment they've made. Boards today won't approve these kinds of investments unless there is a clear return on investment."

To view and listen to the entire webinar, visit www.risk.net/media-centre