Alerting business to threats from fraud and corporate crime

COMMERCIAL CRIME International

December 2011

9/11: 10 years on

AML and terror finance rules tougher but risks remain

The September 11, 2001, terrorist attacks thrust anti-money laundering (AML) and counter terrorist financing (CTF) initiatives into the spotlight as the United States embarked on its 'war on terror'. A decade later, tremendous progress has been made in tracking and seizing dirty money. But globally, regulations could be improved, risks abound, and money launderers and terrorist groups strive to stay ahead of the authorities, experts warn. **Paul Cochrane** *reports from Beirut.*

As Dr Tony Wicks, an AML expert at US-based NICE Actimize, a financial crime, compliance and risk management solutions provider noted to Commercial Crime International: "September 11 was a major milestone associated with the [anti-money laundering] industry generally. There has been significant change and scope in regulations, as well as in the understanding of the causal link of following the money, of what happens with proceeds of crime and TF."

He added: "If asked 10 years ago about money laundering, most people didn't know what you were talking about. A good point is that today people know about the concept although maybe not the full ramifications and the law."

Progress has been made in large part due to close coordination between governments and the financial industry to tackle ML and TF through improved due diligence by financial businesses worldwide, implementing 'know your customer' (KYC) procedures, and the improved filing of suspicious transaction reports to the authorities.

A major motivation has been fines for non-compliance, in particular those imposed by the US Treasury's Office of Foreign Assets Control (OFAC). "What's interesting over the last 10 years is the way regulators are managing the problem. Wind the clock back before 9/11, OFAC was levying fines, on average, of less than $10,000, and typically levying around 400 penalties a year in the early part of the last decade," said Malcolm Taylor, manager director of Accuity, a global AML screening data provider.

"Wind the clock forward and look at 2010, there were only 24 similar penalties but the average amount was closer to $10 million. So the regulator has dramatically increased the size of the penalty whilst at the same time significantly reducing the number of institutions being penalised. The focus has clearly

continued on page 2/

The Director, staff and everyone at ICC Commercial Crime Services would like to wish all our members a very happy holiday.

We look forward to helping you stay one step ahead of the fraudsters again in 2012.

In This Issue of CCI

AML and terrorist financing - from page 1

shifted to the larger institutions where the regulator perceives there to be a bigger risk."

Indeed, American bank Wachovia had to forfeit $110 million in 2010 for having inadequate AML mechanisms in place; and in 2009, the UK's Lloyds Banking Group was fined $350 million by the US authorities for ML-related misdemeanours regarding clients in Iran and Sudan.

The MENA experience

The long arm of the US authorities has also resulted in countries upping their enforcement and bringing banks into AML and CTF initiatives. In the Middle East and North Africa (MENA) region for example, a Financial Action Task Force (FATF) style regional body was established in 2004, MENA-FATF.

"Laws and implementation have improved in the MENA for two reasons. One, the Arab countries have a vested interest as they are directly affected by terrorist groups and two, international pressure. Although the main issue holding everything back is widespread corruption," said Mohammad Baasiri, third vice governor of the Central Bank of Lebanon and a major figure in establishing MENA-FATF.

While the value of the penalties has increased, so have the number of terrorist entities and 'sanctions programmes' (collection of financial punishments) published on the OFAC website. A decade ago there were around 500 terrorism related entities, but today there are more than 11,000 on the OFAC list, a twenty-fold increase, said Taylor. "The number of OFAC sanctions programmes has grown by nearly 70% over the same period," he added.

Yet while the US has updated its lists, there has not been the same level of focus internationally, for instance on United Nations terrorist and sanctions lists. So banks have been able hide behind UN sanction screening lists, claiming they are looking for internationally named entities but not monitoring outside these lists.

"What we have seen is there hasn't been enough updating, lists remain old, and the terrorists have changed their methods and their sources," said Rohan Kumar Gunaratna, director of the International Centre for Political Violence and Terrorism Research in Singapore.

Into this vacuum has stepped companies that list entities suspected of being associated with ML and TF, politically exposed persons (PEPs) and terrorist groups. They provide more extensive data for the private sector than governments and international bodies. Taylor gave the example of Accuity as offering such a service.

Disparity in global standards

Another problem addressed by these private actors is that while the US, Europe and other jurisdictions have adopted tougher regulations, as well as overhauling laws and approving new reforms such as the US Foreign Corrupt Practices Act and the UK Bribery Act, the playing field internationally is uneven. "Asia is playing catch up, and as we see more western banks invest in Asia many larger institutions are having to raise the bar to achieve a common AML standard across their global operations," said Taylor. "But there are still a lot of tier two and three institutions that have inadequate screening systems in place, so there is a lot of catching up to do, even in developed economies. There is a disparity on a global scale and it will take time to close the gaps."

Indeed, Gunaratna said in the coming years it is "crucial for western nations to not only feed and enhance AML and CTF capabilities in the global south – as 95% of terrorist organisations are located there – but that these capabilities grow with the range of threats. I think Africa is a new group area for extremism and terrorism, and specialists in TF and ML will need to look at new actors that may emerge."

At a business level, experts say that companies have to understand areas of geographical risk and the potential compromising relationships of their clients, to avoid falling foul of launderers and terrorist financiers seeking alternative means of circumventing the law and screening processes. A balance has to be sought between assessing risk, not scaring away clients, and investing the appropriate amount to carry out effective due diligence, hopefully in a client-friendly manner.

"The amount of regulations are not going away and the expectation is that the bar will be raised," said Tony Wicks. "The challenge for companies in the current economic climate is the cost of implementing control systems. What we will see is the increasing use of technology to implement those systems on a cost effective basis, but also increasing customer-centricity related to those systems."

Be aware:
as this photo of 419 fraudsters at work shows, not everyone will be taking time off for the holidays.

Urea scam prompts bribery investigation

PAKISTAN's Federal Investigation Agency (FIA) is reportedly about to start prosecuting those believed to be involved in a Rs27 billion ($308m) embezzlement scandal at the state-owned fertiliser distribution company.

The scam allegedly involved officials at National Fertilizer Marketing Ltd (NFML) taking bribes in exchange for a multi-tiered scheme that involved obtaining government subsidies to import fertiliser, not delivering it to government warehouses as promised, and then illegally shipping the fertiliser to Afghanistan; in the process creating an artificial shortage in the local market (from which those behind the scam also profited).

Investigators allege that between June 2008 and December 2010, about 78,000 bags (50kg) of fertiliser worth about Rs27 billion were moved illegally by about 10 people, with the cooperation of NFML officials. Reports also suggest that the fertiliser scam may be just the tip of the iceberg, and allege that about 2.5 million tons of urea, worth $1 billion, was imported by several companies in the past year at the behest of state-owned companies but that about 40% of it has yet to be delivered to the government's warehouses.

The scandal came to light when the FIA received a complaint in April 2010 claiming that a number of officials and others received Rs390 million in bribes to allow the smuggling of fertiliser imported at Karachi to Afghanistan via Chaman. The fertiliser had been meant for several government storage facilities.

Bank was complicit in grain fraud says US

PARIS-based BNP Paribas SA is being sued by the US government over allegations that the bank aided a grain export fraud scheme involving commodity payment guarantees provided by the Department of Agriculture.

It is alleged that a corporate banker in BNP's Houston office helped with a scheme that defrauded the Agriculture Department of at least $78 million through deals he made with four US grain exporters.

Officials said the banker knew the exporters were secretly controlled by the same foreign businessman, who owned the companies importing the shipments into Mexico. The Agriculture Department's Supplier Credit Guarantee Program prohibits payment guarantees on commodity sales between a US exporter and a foreign-owned importer controlled by the same person or group.

"Because the US exporters and Mexican importers were under common ownership and/or control, which fact defendants knew, none of the commodity sales between these entities were eligible for SCGP payment guarantees," Assistant US Attorney Michelle Zingaro said in the complaint.

When the Mexican importers defaulted on payments for dozens of grain shipments from 1998 to 2006, BNP and Jovenal "Jerry" M Cruz, its former trade finance manager, "presented or caused to be presented false or fraudulent claims to the USDA," she added.

The complaint alleges that the US shipping companies assigned their falsely obtained export guarantees to BNP, along with the payment obligation from the Mexican importer. In exchange, BNP provided the US exporter a line of credit up to the amount of the guarantees, minus the bank's fee.

"By financing these transactions, BNP earned fees in exchange for providing a line of credit to US exporters that was fully secured by the United States," the government said in the complaint. "Cruz solicited and received payments of kickbacks and/or bribes" from others in the alleged conspiracy "for BNP's role in financing the scheme through expanding lines of credit from BNP to the US exporters based on ineligible commodity sales to the Mexican importers," it added.

Mr Cruz, who has pleaded not guilty, will go to trial on the case in February. Meanwhile, three other people charged in the scheme have pleaded guilty and are awaiting sentencing.

Alba alleges fraud

ALUMINIUM Bahrain (Alba) said recently that it would take legal action to recover losses stemming from alleged fraudulent contracts involving businessman Victor Dahdaleh. Alba gave no estimate of the company's losses, but said to date it had recovered more than $30 million from European companies.

Alba said it had filed a civil suit seeking damages against Dahdaleh, Alcoa, and a group of other related individual and corporate defendants in the US.

Britain's Serious Fraud Office (SFO) arrested Dahdaleh in October in the UK and charged him with corruption offences relating to contracts for the supply of intermediate product alumina, shipped to Bahrain from Australia, and for the supply of further goods and services to Alba.

The SFO said Dahdaleh was alleged to have paid bribes to officials of Alba in connection with contracts with US company Alcoa Inc. He said the (5-year) investigation into his affairs was flawed and that he would be contesting the charges.

More assertive investors may be key to halting rise in fraud

10 years after Enron, WorldCom and Tyco International, corporate fraud is still flourishing as much as ever. There's been a great deal of regulation, oversight and tighter controls introduced in the interim, but it seems that criminal behaviour within companies continues despite the threat of stiffer penalties, and investors continue to be the main victims. **Rodrigo Amaral** *attempts to explain why this is, and show stakeholders what they can do to identify wrongdoers before it's too late.*

Jérôme Kerviel, Bernard Madoff, Satyam, Parmalat and America's HealthSouth Corporation all demonstrate that fraudsters do not stop, even when the economy is thriving. The evidence suggests that corporate frauds are a more widespread problem than generally perceived and, worryingly, that they are as hard as ever to spot.

More evidence that corporate fraud is on the rise is provided in a recent study from Kroll and the Economist Intelligence Unit, where companies in the financial sector reported that fraud cost them an average 2.7% of revenue in the past year. At 18% of all companies interviewed by the EIU, the cost reached 4% of revenue. More worryingly, only 27% of 1,200 firms surveyed said they were prepared to comply with legal requirements that could help them to combat fraud in a more effective way, such as the UK Bribery Act or America's Foreign Corrupt Practices Act.

In a bid to provide perspective, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), an American corporate governance association, has analysed the fate of companies that American authorities have investigated for fraud. Unsurprisingly, COSO found that they are more likely than clean firms to suffer falls in their share price or go bust. And whilst investors may have the satisfaction of seeing the culprits sent to jail, this is scant compensation for the billions of dollars they inevitably lose when major corporate frauds are exposed.

Investors' holdings can be affected by corporate fraud in many ways and they will not always be aware that it is even taking place, as companies are often not required to report irregularities they discover themselves, as long as it does not materially affect shareholders' interests. But even low-value frauds perpetrated by employees who merely want to fund a more luxurious lifestyle can reveal deeper problems in a company that could result in severe losses.

Moreover, while investors cannot be expected to stay abreast of every occurrence in the corporate behemoths in which they put their money, experts still insist they have a part to play, by putting pressure on firms to install effective systems to curtail fraudulent activities - particularly in hard times when corporate misdemeanours not only grow in volume, but also become harder to prevent.

Risk factors

Certain factors can conspire to increase the risk of corporate fraud. Employees have incentives to stray, especially if they sense their jobs could be at risk. Even when employees have a firm position in a company, the pressure to perform in a challenging environment can lead managers to misrepresent their numbers. If they need to reduce costs and maintain profits in tough times, companies often choose to axe departments that do not produce revenue - departments that can include monitoring activities such as internal audit and risk management. At the same time, the

Incidence of types of corporate fraud by region

Corporate fraud by region	All respondents	Africa	Asia-Pacific	Europe	Latin America	North America	Middle East
Theft of physical assets or stocks	28.8	38.5	25	23.5	25	22.5	10.5
Internal financial fraud or theft	22.9	22.3	24.7	18.2	23.5	25.6	26.3
Management conflict of interest	20.8	27.7	23.9	19.2	20.6	15.2	22.8
Vendor, supplier or procurement fraud	19.6	30.8	24.7	14	22.8	12.5	24.6
Internal financial fraud or theft	19.1	32.3	22.1	16.3	17.6	13.5	19.3
Corruption and bribery	18.9	37.7	24.4	13.7	22.8	6.6	21.1
Financial mismanagement	15.7	32.3	20.7	11.7	8.8	10	12.3
Regulatory or compliance breach	11	9.2	14.4	9.8	11.8	9.3	7
Intellectual property theft, piracy or counterfeiting	10.2	7.7	11.2	7.8	6.6	13.8	12.3
Market collusion	9.1	13.8	10.6	9.4	6.6	5.5	8.8
Money laundering	3.7	13.1	2	2.9	2.2	3.1	3.5

Shows the perceived prevalence of different types of corporate fraud in various regions, as a percentage of 1,200 survey respondents. Source: Kroll/Economist Intelligence Unit

growing sophistication of financial arrangements used in business transactions, coupled with complex IT systems, has made the job of ill-equipped fraud-busters more complicated.

On the other hand, the difficulties that companies face during a period of crisis often help to uncover irregularities, especially those that might not be noticed during a boom. It is certainly true that frauds are more readily detected during an economic downturn when scams become more visible.

With the average time between a fraud starting and it being detected put at 3.5 years, according to KPMG, the cases coming to light now might be only the tip of the iceberg. Companies may still be failing to spot many of the frauds committed by employees, executives, business partners or third parties. And experts say that more often than not firms prefer to keep fraud cases hidden from the public if they are not legally forced to disclose them.

In defending such actions, companies might argue that, for investors, many cases of fraud are of little interest if they do not involve large amounts of money, as frauds like accounting gimmicks or misappropriation of funds do not have a significant effect on the firm's bottom line, and therefore have arguably no direct impact on its share price. The argument goes that such cases would have a negative impact on the reputation of the company, so the best solution is, whenever possible, to deal with small-time crooks internally and with discretion. The definition of a small-scale fraud is subjective, however. For example, KPMG reported a case in India where a trader in a minerals firm siphoned $25m to his own account by colluding with clients of the firm. But that sum was not deemed worth the trouble of taking the perpetrator to court.

Rising amounts

The frauds that are investigated, however, are sufficiently numerous to establish that fraudsters are not only more active, but are stealing larger amounts. COSO studied frauds involving financial reporting in America between 1998 and 2007. It found 347 alleged episodes of fraudulent reporting, compared with 294 in the previous 10-year period. In total, the companies involved in frauds misreported or misappropriated $120 billion, or an average of $400m a case. In the 10 years to 1997, the average value of the frauds was a mere $25m. The authors of the report did however say that their latest research included the mega frauds of the early 2000s, which could have skewed the differences.

The COSO study also provided an idea of how generalised the problem is. Companies involved in financial reporting frauds ranged from start-ups with no assets or revenues to industrial behemoths with assets of more than $400 billion and revenues of over $100 billion. Cases were identified in a wide spectrum of industries, involving both listed and unlisted companies. Among those that are publicly traded, COSO identified a higher incidence of stocks sold in over-the-counter markets rather than exchanges among the companies where frauds were reported.

Detecting fraud

If any company can be a target, it should be assumed that anyone can be a perpetrator, and ignoring red flags is the one thing all firms can ill afford to do at a time when corporate fraud is on the rise.

As CCI showed in October (page 3) many of the signs of fraud are common sense. But in reality, most of the clues are likely to be found by the number-crunchers and compliance officers that work in internal audit and risk management departments, especially at large, multinational corporations. In general, the bigger the company, the more exposed it is to fraud. So the best way to keep everybody on track in a multinational giant is to ensure internal controls are efficient. Sections of annual reports that deal with internal and external controls should receive special attention from shareholders, for all their lack of glamour and

continued on page 6/

Size of the problem

Corruption and corporate fraud is costing companies and governments about $40 billion dollar a year and is increasing globally says a recent joint World Bank and United Nations report.

The World Bank report highlighted 817 'corporate vehicles' that were implicated in 150 corruption cases worldwide and involved about $56.4 billion over the last few years. Most large-scale corruption cases involve using legal entities to conceal ownership and control corrupt proceeds, the study released by the Stolen Asset Recovery (StAR) Initiative of the World Bank and the United Nations Office on Drugs and Crime, said.

In the report titled, Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets, it suggests policymakers need to take steps to improve transparency to reduce opportunities for wrongdoing.

The study explains how corrupt public officials and their associates conceal their connection to ill-gotten funds by exploiting legal and institutional loopholes that allow opacity in companies, foundations and trust-like structures. The report also identifies weaknesses in company formation, registry, auditing and lack of proper identification in offshore registries that helps people set up shell companies and use front men to channel money.

Continued from page 5

yawn-inducing terminology, and investors must check whether companies are putting together robust compliance and audit programs. If they are not, that is a problem.

Clearly, it is not easy to define the total characteristics of a system that is good at spotting and preventing fraud. The ability and eagerness of external auditors to identify illegal practices at their clients have often been questioned, and ill-intentioned top managers may change their auditors when they want to make their own lives easier. At the same time, internal controls are only as strong as company boards allow them to be, and are likely to be weak if irregularities are brewing in the top echelons of a corporation.

The fact is that, despite the influence of senior management, internal staff are almost always best positioned to detect irregularities. When they speak out, results can be swift. But in many companies denouncing irregularities is not possible for staff members who fear for their jobs. Firms have attempted to set up anonymous hotlines to minimise this problem, but cultural factors mean that such measures are not always accepted by workers, and much of the information collected can be unreliable. Yet companies may have few alternatives if they want to uncover the enemy within their ranks. According to researchers, fraud detection takes place less because of the action of interested parties, such as investors and auditors, than through information disclosed by employees, the media and industry regulators.

And the challenge becomes even bigger as companies focus on their international operations. Some of the markets most coveted by multinationals, such as the Brics (Brazil, Russia, India and China), are seen by many analysts as soft targets for corporate fraudsters, with lax prevention and control systems at the corporate level, and ineffectual justice systems that fail to dissuade potential perpetrators of criminal deeds.

Helpful legislation?

Legislation to help fight corruption, such as the UK Bribery and Foreign Corrupt Practices Acts, also complicate the situation, as American and British companies can no longer claim that they are not responsible for fraud at foreign subsidiaries. This makes it more urgent for firms to invest in the prevention of fraud and the spreading of compliance practices to their units all around the world.

Investors also need to be aware of the possible consequences of mis-steps in foreign markets by companies they hold a stake in. Even minority shareholders are not absolved from doing whatever they can to combat fraud and corruption, according to the new UK Bribery Act. And those with a place on the board have an obligation and a responsibility to try and make the board understand the implication of something that might be happening.

With the spectre of corporate fraud hovering over business, it may be that in the future an increasing number of investors will try to use their own means to tackle it.

This article is an edited version of the original by Rodrigo Amaral that was posted on Fundweb in October.

An example

An American man was sent to prison for four years last month after he admitted embezzling about $1.2 million from a natural gas supplier he was employed by as a comptroller and financial officer.

In this role, his duties included issuing the payroll, paying outstanding amounts and receiving payments to the company. But between 2004 and June 2011, he twice a month issued himself an unauthorised cheque from the company's corporate bank account held at a First Commercial Bank. He forged the name of the company's owner on each cheque and submitted them for payment. He then altered the company's accounting ledger by replacing his name with the name of a company to falsely reflect that company had received the cheque as payment. Finally, upon receiving bank statements for the corporate account, he altered the statements to remove his name and replace it with the name of the company he had falsely entered on the company's internal ledger.

Fraud cost organisations 2.1% of earnings in the past 12 months, which is equivalent to a week of revenues over the course of a year, according to the Kroll Annual Global Fraud Report.

However, fraud remains predominantly an inside job, according to the report, and insider jobs increased this year. The 2011 figures show that 60% of frauds are committed by insiders, up from 55% last year.

Steps to assist fraud detection

COMPANIES must ensure their owners and boards of directors are actively involved in creating and maintaining an environment that is not conducive to fraud says *Tracy Coenen, a forensic accountant and fraud investigator with Sequence Inc in the US, and author of Expert Fraud Investigation: A Step-by-Step Guide and Essentials of Corporate Fraud.* This involves active oversight of daily operations, continuous monitoring of the potential red flags of fraud and swift action when fraud is discovered.

Executives have the means to commit and cover up the largest frauds, she continues. They have access to the information and computer systems, they have power over all employees and they have access to the money. The finance function is riddled with fraud risks and the company's executives are in the best position to take advantage of those risk.

Creating and maintaining an ethical corporate culture is the most basic step to preventing internal fraud. Companies establish a culture that values honesty by creating a code of conduct that is practical and is enforced. This means that from the top of the company, all the way to the bottom, the rules governing ethical conduct are front of mind and are adhered to by all employees and members of management.

Ethical behaviour must be a non-negotiable standard within the company, and no one should be exempt from the rules. The code of conduct also should include guidelines and mechanisms for reporting suspicions of unethical behaviour. It must be clear that there will be no retaliation against employees who report co-workers, managers or executives.

Hiring

Hiring the right employees is another major component of reducing fraud. Information on job applications and resumes should be verified and references should always be checked. While it may seem unlikely that these sorts of checks will uncover any damaging information, it is still important to do the work in case something is amiss.

Background checks, as permitted by law, are important. The more sensitive the employee's position, the more thorough the background check. Court records - including civil, criminal and bankruptcy - can give important clues to a potential employee's background.

Checks and balances

Internal controls are needed to ensure fraud does not occur or that it is detected quickly if it does occur. True fraud prevention goes beyond simply complying with whatever regulatory mandates a company may be subject to. It requires the creation of policies and procedures specifically designed to address fraud risks.

If procedures are properly designed and implemented, there will be natural checks and balances between employees. Such procedures include segregation of duties, whereby accounting procedures are divided between employees so that no single employee monopolises a process.

For example, the process of recording sales, billing customers, collecting customer payments and updating customer accounts should be divided between several people. This way, if someone tries to steal funds or manipulate accounting records, it will likely be caught by another employee who is recording or reconciling transactions in another part of the process.

There are many standard control procedures that can prevent and detect fraud, and they aren't necessarily expensive to implement. Establishing these procedures will help increase the chances that fraud will be stopped. As an added benefit, the perception that fraud is being prevented and detected further helps deter employee fraud.

Fraud happens

Despite the best efforts of management, fraud will occur in companies. When it happens, hopefully companies have procedures in place to catch the fraud early. It is essential that companies swiftly, certainly, and fairly deal with instances of fraud. Those responsible should be held accountable so other employees know there are consequences for unethical behaviour.

SFO hotline offers new option to report corporate fraud

THE UK Serious Fraud Office (SFO) is encouraging whistleblowers to flush out corporate wrongdoing with a new service designed for company insiders who are not personally victims of fraud or corruption.

The SFO said that individuals with inside knowledge of suspect business practices could call the new "SFO Confidential" hotline or fill in a new online form. The new hotline will complement its national fraud reporting service for victims.

"Company executives, staff, professional advisors, business associates of various kinds or trade competitors can talk to us in confidence," said SFO Director Richard Alderman. "I have set up a special team to make the SFO readily accessible to whistleblowers, with trained staff sympathetic in dealing with any anxieties people might have about coming forward."

Preserving funds abroad – Europe to the rescue?

As anyone who has ever been involved in court proceedings knows, winning before the judge is pointless if you cannot recover the money. In this article, **Joseph Kean** *from the Dispute Resolution Team at Mundays Solicitors LLP in the UK, discusses how a new proposal from the European Commission may make retrieving funds from accounts across Europe a lot easier in future.*

About the author:
Joseph Kean, Partner at Mundays LLP, became a solicitor in 1990 and throughout his career has practiced in commercial litigation and arbitration, working in a wide variety of industry sectors, including aviation, construction and technology. For more tel 01932 590 500 or email joseph.kean@mundays.co.uk

Mundays is a leading regional practice which provides quality advice to corporate and private clients. It specialises in Banking, Construction, Corporate & Commercial, Dispute Resolution, Employment, Family, Insolvency, Private Wealth, Property, and a wide variety of industry sectors.

For creditors or those who have lost money through fraud or corruption, obtaining a court judgment is only the start. More important is the question of how you actually recover the money. You may be able to trace funds into the defendant's bank account, but will those funds still be there when you come to enforce your order? The position is even more complicated when the funds are held in multiple foreign jurisdictions.

The European Commission's proposal

To address this problem, the European Commission (one of the European Union's (EU) governing institutions) recently proposed the introduction of a special procedure (known as a European Account Preservation Order or "EAPO"), effective in European cross-border civil and commercial matters. The proposal would enable claimants, in certain circumstances, to obtain a court order 'freezing' money held by a defendant in bank accounts across Europe, and restricting the account holder's dealings with those funds, including preventing them from making payments and other transfers. In this way the EAPO would provide a safeguard and could prove very effective at prompting early payment by a debtor-defendant. Currently the availability of such orders is a matter for local procedure, which differs widely throughout EU member states. The proposed EAPO would provide a "one-stop-shop" in European cases.

(Note: *the EAPO procedure would not apply to bodies such as the Serious Fraud Office, Financial Services Authority etc, who already have their own tools and established international networks and procedures).*

The UK Government has decided not to opt into this proposal for now. Nonetheless, and even if the UK ultimately stays out of the regime, UK companies undertaking litigation in European courts and those with bank accounts in other EU countries will need to take careful note of EAPOs, if and when they are adopted by the other EU states.

How will an EAPO work?

Under the proposal, an EAPO will be available to a claimant who is suing a defendant in one EU state, where that defendant has bank accounts in other EU states. For example, a claimant suing a debtor in Germany could apply in Germany for an EAPO to freeze the debtor's bank accounts in France, Spain and other EU states. It will be available both while a case is proceeding through the courts of an EU state (a "pre-judgment EAPO"), and once a judgment has been obtained from an EU court (a "post-judgment EAPO").

For a pre-judgment EAPO the claimant will need to show that his claim is well-founded and that there is a real risk that without the order, the debtor would remove or transfer the funds held in his bank accounts, frustrating enforcement. However, the only condition for a post-judgment EAPO is that the claimant has obtained an enforceable judgment in one EU country that he wishes to enforce in another. Once issued, EAPOs will be automatically recognised and enforced in another EU state without any special procedure being required, and a defendant's right to challenge the order is limited.

An EAPO will be served directly on the bank holding the relevant account which must then be 'frozen', preventing the defendant transferring or withdrawing the funds. Moreover, EU states will be required to establish

a mechanism to help claimants obtain information about a debtor's accounts held in their territory.

Benefits to creditors

A major difficulty for those attempting to recover assets obtained by fraud or other corrupt activity is that the perpetrators of these crimes are often based in many jurisdictions, with funds spread over several countries. Under current rules, separate applications must be made in each country where a bank account is held, resulting in many different procedures, the need to take advice in each jurisdiction, increased costs and time delays. The ability to obtain just one order which can then be enforced across Europe could clearly be of great assistance to those seeking to recover funds internationally.

In addition, applications for an EAPO will be made to the court "without notice" to the defendant, who is only informed once the account has been frozen by the bank. This preserves the surprise effect of the measure and prevents the debtor from emptying his bank accounts in advance. This will be particularly important when dealing with fraudsters and other criminals.

Potential difficulties with the proposal

While the EAPO would provide a welcome enforcement tool for claimants, the current proposal has been widely criticised as failing to protect defendants, which is one reason why the UK Government decided not to opt in at this stage. For example, as there is no need when applying for a post-judgment EAPO to show that assets are at risk without the order, a defendant who is willing and able to pay the judgment debt may nonetheless find his bank account frozen without notice, with all the potentially serious consequences that may have for trading.

In addition, there are a number of other safeguards missing that UK litigants are accustomed to seeing in measures of this kind, including:

♦ no obligation for the claimant to make full and frank disclosure to the court when applying for an EAPO

♦ an absence of effective provisions to provide security to protect a defendant should they ultimately successfully defend the claim

♦ uncertainty over the amount of funds that would be exempt from being frozen, to ensure the livelihood of the defendant and his family or to allow a company to continue its ordinary course of business

♦ the potential impact on banks and other account-holding institutions, who may find themselves devoting more resources complying with EAPOs served on them and providing account information to claimants.

What do you need to do?

As things currently stand, and as the UK has opted out of this proposal, EAPOs will not be obtainable in support of claims brought in the UK, nor will they be enforceable against bank accounts held in the UK. However, in modern business, commercial organisations, including fraudsters, maintain financial accounts in many jurisdictions. Businesses litigating in the courts of other EU states, as claimant or defendant, will need to take relevant legal advice on the applicability of EAPOs to their situation. The proposal is still some way off becoming law. However, it is clear that, if passed as currently drafted, the Regulation will have a considerable impact on recovery of money judgments in European cases.

UK SME's urged to check address

THOUSANDS of small UK firms have fallen victim to corporate identity fraud in the past year, raising the threat of their finances being "crippled", new research has revealed.

More than 15,000 small businesses claim to have fallen victim to corporate identity fraud over the past year, according to the report. Crimes were often the result of fraudsters changing a firm's office address by submitting a false form to Companies House, said life assistance firm CPP recently.

Most companies were unaware of this loophole, mistakenly believing details of documents sent to Companies House were checked, said the report. A CPP identity fraud expert said: "Small businesses are particularly vulnerable as they often don't have the systems in place to protect themselves or the resources to draw on if they do become a victim."

Links:

The proposed EU Regulation: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0445:FIN:EN:PDF

The UK Ministry of Justice's consultation: http://www.justice.gov.uk/consultations/european-asset-preservation-order-cp14-11.htm

The Government's statement to Parliament, 31 October 2011: http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm111031/wmstext/111031m0001.htm#1110311000006

Protecting against corporate espionage

How do you protect against a sophisticated, motivated criminal who has targeted your company's trade secrets? These types of people know that information comes in many forms, not just electronic. They are trained to exploit any vulnerability and they need to find only one. **Michael Podszywalow** *a member of ISACA and the founder and senior security consultant for SpyByte LLC explains.*

Corporate espionage is on the rise for multiple reasons: the down economy, frequent job changes, and even governments that boost their economies through the acquisition of trade secrets. Stealing information is one of the oldest forms of gaining a strategic and competitive advantage, and the only thing that changes are the techniques used.

According to security expert Ira Winkler, information exists in four dimensions: paper, visual, oral and electronic. Professional spies can obtain information through any of these dimensions, so deploying security technologies alone will not sufficiently secure your company. An effective information security program must protect the four dimensions of information using physical, logical and operational security measures.

The Professional Attacker

A professional attacker can be almost impossible to stop using traditional security measures. Ultimately, the attacker's goal is to launch a "precision strike" against the company and avoid detection at all cost.

To be able to detect and defeat an attack, it is critical that security professionals to put themselves in the shoes of a criminal and think like they do. Sophisticated criminals often take the path of least resistance to get what they want. They are trained to take advantage of whatever vulnerabilities appear. Doing this will allow you to see your exposures and determine the best countermeasures for your organisation.

Protection

In today's regulatory environment, information security managers must comply with industry-specific, state, province and federal regulations (regulations that often focus on customer information and privacy). But security programs that focus on privacy-related compliance requirements do not sufficiently protect a company's assets. Your company is not secure just because you have checked off the items on the compliance list, so consider the following:.

Step 1

The first step to effective defence is to identify: 1) information that, if lost, would critically harm the company, and 2) the value of that information to your company and its competitors. These are your "crown jewels" and should merit the best defences. Information security managers must be able to identify company intellectual property (IP), the location where the IP resides, and the value of the IP, so they can protect and control who has access to this information. Then perform a risk assessment to identify existing security vulnerabilities to those crown jewels.

As a side note, it is also important to establish a comprehensive list of data items your organisation owns or processes, including an inventory of all IP that could affect revenue or reputation. Examples of such information may include: copyrighted material, patents, trademarks, operating procedures, user manuals, policies, memos, reports, plans, contracts, source code, recipes, manufacturing plans, chemical formulas, design drawings and patent applications.

Step 2

Once you fit your crown jewels into your security program, you must determine how to protect against the low-tech attack vectors. One way to do this is through an effective, incentivised and targeted security awareness program coupled with regular enterprise-wide security testing. Employees respond better to carrots than sticks. If you properly train and incentivise security awareness, you will gain a strong defence.

Step 3

The third step is to simulate an actual attack, which often occurs as a "blended threat," in your enterprise security testing. This testing should focus on all types of information, regardless of its form. You should implement testing along several attack vectors in a holistic approach, for example, combining a network pen test with physical and social engineering assessments. Those results will give you a better idea of your attack defences.

And finally

In some places of the world, people think that, if you fail to protect your information, it is up for grabs. They will view you as an easy target that should have had better protection in place, not as a victim who suffered criminal damage through espionage. Today, there is no universally adopted legal definition for a "trade secret," so countries treat theft of IP very differently.

To protect yourself, you must begin to view your organisation from an attacker standpoint and realise that no company is 100 percent secure. A determined, skilled and highly motivated attacker is almost impossible to stop, but you can put measures in place that make your company less likely to be a victim.

Online Social Networks – Launch pads for Malware

The advent of social networks has turned the online world into a virtual society. And whilst social networks serve as seamless communication channels, they are also an ideal launch pad for malware infections. There has been a tremendous increase in the dissemination of malware infections through social networks. But the security and privacy mechanisms of social networks have proven insufficient to prevent exploitation. **Aditya Sood** *and* **Richard Enbody** *explain the dangers.*

Aditya K Sood *is a senior security researcher and PhD candidate at Michigan State University. He is also a founder of SecNiche Security Labs, an independent arena for cutting edge computer security research.*

Richard J. Enbody*, Ph.D, is associate professor in the Department of Computer Science and Engineering at Michigan State University (USA).*

Social networks hold a plethora of personal information on the users that form the network. Individual connections between users collectively form a web of connections. To build each link between users an implicit trust is required between the two users and implicitly across the entire network. Any information provided by an individual user through chained connections becomes a part of the full network. If an attacker is able to exploit one user in the social network, they have the potential to be able to push malicious content (such as malicious URL's) into the network. The connectivity of the network enables the spread of the exploitation. That is, the attacker exploits the weakest link in the chain. This exploitation process is aided by the inability of users (and their stored objects) to determine the legitimacy of content flowing through the social network. The infection process begins with the exploitation of human ignorance and curiosity followed by spreading of the infection through the trust upon which the network is based.

In order to start the exploitation process, an attacker can pick any issue that affects human emotions to drive the user in a social network to follow the path generated by the attacker. Topics such as weather calamities, political campaigns, national affairs, medical outbreaks and financial transactions are used for initiating infections. Phishing and spamming are used extensively for spreading messages on these topics with malicious intent. Basically, it is a trapping mechanism used by attackers to infect an entire online social network.

Exploit Mechanisms – The Art of Infection

Since social network exploitation begins by exploiting an individual user's trust, curiosity, or ignorance common attack strategies have emerged: One of the simplest infection techniques is the injection of malicious URLs into a user's message wall. Since it can be difficult to differentiate between the legitimate URLs and illegitimate ones, even a careful user can be tempted to click on the link. Unfortunately for the user, clicking the hyperlink can result in automatic download of malware from a malicious domain through the browser.

- Browser Exploit Packs (BEP) hold a number of browser-based exploits that are bundled together to customise the response to a victim. When a user visits a malicious domain, the BEP fingerprints the browser version and the related environment of the user machine. Based on this information, a suitable exploit is served to the user which exploits the integrity of that particular browser.
- Drive-by-Download attacks are triggered by visiting a malicious page. They exploit browser vulnerabilities in plugins and built-in components. Successful exploitation of the vulnerability results in the execution of shell code that in turn downloads the malware into the system. A variation of the Drive-by-Download attack is the Drive-by-Cache attack that can exploit browser cache functionality in order to execute malware.
- Malicious advertisements (malvertisements) are yet another technique to spread malware infections through online social networks. When an attacker injects the malicious link in a user message board, it is linked to a third party website which has malicious advertisements embedded in it. These advertisements are further linked to malicious JavaScripts that are retrieved by the browser, which executes the malicious content in the context of running browser with the user's privileges.

The biggest problem with the online social networks is that they do not have sufficient built-in protection against malware. For example, current

continued on page 12/

social networks do not scan the URL's and embedded content coming from third party servers such as Content Delivery Networks. Therefore, there is no mechanism to detect the authenticity of URL's that are passed as message content among the user objects in the online social networks. In addition, it is easy to upload malvertisements, and social networks fail to raise any warning. Online social networks are not harnessing the power of Safe Browsing API's from Google or similar services to instantiate a verification procedure before posting a URL back to a user profile. Lack of such basic protections is a key factor in making the social networks vulnerable to exploitation. Finally, many social network users are not knowledgeable enough to differentiate between real and malicious entities. Ignorance not only results in exploitation, but also greatly impacts the overall security of online social networks. Because of the high connectivity and need for trust in a social network users are particularly dependent on the built-in security features of online social networks, but the security features are not tough enough to thwart many malware attacks.

Conclusion

Robust security and privacy mechanisms are indispensable for safe online social networking. Built-in security is necessary because attackers exploit the trust, curiosity and ignorance to garner maximum profit. User awareness regarding security concerns is important but can only spread gradually, so social networks should be proactive and develop more sophisticated and stringent mechanisms to thwart malware infections. Safe and secure transmission of the information and robust user's privacy should be the paramount concern of the social networking companies.

Cybercrime

EDF fined for hacking Greenpeace

EDF, the French energy firm, was recently fined Euro 1.5 million by a Paris court for spying on Greenpeace. It must also pay Greenpeace Euro 500,000 in damages. Two EDF employees were jailed, along with the head of the company they hired to hack into the environmental charity's computers.

EDF was charged with complicity in concealing stolen documents and complicity to intrude on a computer network. It was claimed the company had organised surveillance not only of Greenpeace in France, but broadly across Europe since 2004. And it was stated that in 2006, EDF hired a detective agency, Kargus Consultants, run by a former member of France's secret services, to find out about Greenpeace France's intentions and its plan to block new nuclear plants in the UK. The agency allegedly hacked the computer of Yannick Jadot, Greenpeace's then campaigns director, taking 1,400 documents.

At the trial, EDF said it had been victim of overzealous efforts, and had been unaware anyone would hack a computer. But Greenpeace UK's executive director, John Sauven, said: "The evidence presented at the trial showed that the espionage undertaken by EDF in its efforts to discredit Greenpeace was both extensive and totally illegal. The company should now give a full account of the spying operation it mounted."

Whilst anti-nuclear activists are reportedly furious at what EDF did, a security expert has commented that the only real surprise is that this sort of trojan-assisted industrial espionage has not reached the courts before.

Philip Lieberman said that the case is notable because the saga started more than five years ago. And, he wondered, how many other cases of trojan-assisted industrial espionage have been carried out in recent years. What does this case tell us? Quite simply that trojan-assisted infections are almost certainly an integral part of the modern-day private detective's IT arsenal when conducting industrial espionage," he said. And we should ask whether terrorists are using the same techniques to assist their campaigns.

COMMERCIAL CRIME International

Published monthly by Commercial Crime Services,
Cinnabar Wharf, 26 Wapping High Street, London E1W 1NG, UK.
Tel: +44 (0) 20 7423 6960 Fax: +44 (0) 20 7423 6961
Email: ccs@icc-ccs.org Website: www.icc-ccs.org
Editor: Andy Holder Email ajholder@gmail.com

ISSN 1012-2710