

How Teamwork Can Beat the Fraudster

Ben Poole

Treasury departments and banks are facing increasing regulatory requirements to minimise financial crime. How can they balance compliance with the needs of the business and what tools are at their disposal?

Methods of payment and banking are becoming more sophisticated, as seen in the latest automation, electronic peer-to-peer payment networks and methods of identity authentication, among others. This is a world that is trying to combine the speed of product delivery with security enhancements-so when the regulator imposes tougher standards in the area of financial crime, it is no wonder that some corporates and banks can feel somewhat overwhelmed. As corporate banking channels become more advanced, so do the methods used by financial criminals. So how can corporates and banks satisfy their business partners and the regulators at the same time?

Risk to SMEs

One of the most basic preventative measures for all organisations is to acknowledge the fact that they are at risk from financial crime-that applies as much to a small local company as it does for a multi-billion dollar multinational. The risk can sometimes be greater for small and medium enterprises (SMEs), as they are more likely to operate on very tight margins and will not have a reserve of funds to fall back on if they are affected by fraud.

Smaller companies don't often have a qualified IT administrator, which can leave their network open to attack from malevolent outside influences. Barry Schofield, from Investigator Limited, notes in his article Corporate Espionage - The Risk For SMEs that SMEs may also think that purchasing a software product will fulfill all of their network security needs, but they end up "trying to use complicated and hugely technical enterprise security products that simply weren't designed with them in mind". Without knowing how to use the solution that has been purchased, there is a strong likelihood that these companies will have problems dealing with corporate espionage going forward, as well as struggling with using the solution itself.

Just as some SMEs may lack the structure to effectively cope with the more technical elements of financial crime prevention, they are also more likely to lack a clear policy on how to handle internal data, no matter how unimportant it may seem at the time. As Schofield notes: "Companies produce their own newsletters, policy-meeting minutes and so on, filled with project data, details about people, company status updates and other information. It is important to realise that, although information on a computer can be extremely important, the same piece of information written on a napkin is just as valuable." The message is: all data, no matter what format it is stored in, needs to be protected.

Compliance Concerns

As well as taking control of financial crime issues, companies also face a whole slew of government compliance issues and regulations. As new and revised regulations are implemented, it is important

that organisations of all sizes keep up to date with what is required of them. If they do not, they can expect to be penalised by the regulator, as well as possibly leave themselves open to fraud.

Recent research in the UK, conducted by credit research firm Experian, found that 51% of corporates are at risk of receiving a fine because they are not adequately complying with anti-money laundering (AML) legislation. A large cause of this is the revisions that are about to be implemented in the UK's AML Directive. In his article, *Reconciliation: The Transaction Challenge For Financial Institutions* Experian's Tony Pullen explains that from 15 December 2007, businesses will be required to authenticate the identity of all shareholders, where they are beneficial owners, in addition to directors and proprietors. On top of this, companies will also be expected to monitor their relationships with business customers and employ a risk-based approach to areas of due diligence and corporate threat assessment. The Directive is also reclassifying which corporates should take on greater AML responsibilities. As Pullen from Experian explains, this will include, "any organisation that accepts cash payments of €15,000 (around £10,500) or above, as well as casinos, lawyers, estate agents and accountants, regardless of the level of one-off cash payments they accept."

Clearly, the regulators are trying to come down hard on money launderers with this revised legislation, but some say this regulation goes too far. If CEOs feel that their company is spending too much time trying to comply with bureaucracy, there is a danger that they will either relocate to a much less regulated region, or just sell up and move their capital out of the industry altogether. This is certainly the view of many people in the gambling industry, according to Warwick Bartlett, from Global Betting and Gaming Consultants (GBGC), in his article, *Regulation and the Gambling Industry: Post 9/11*. Set against the backdrop of the terrorist attacks in New York on 11 September 2001, Bartlett argues that regulations brought in to prevent terrorist financing and money laundering are going beyond that remit by over-regulating and interfering with legal business transactions and operations-in some cases as a way of protecting domestic business against outside competition.

An example of 'over-regulating' that GBGC's Bartlett cites in his article is the establishment of the UK's Gambling Commission. The gambling industry in the country is not happy with the Commission, seeing its establishment as an indirect accusation of poor AML practice within the industry. "Nothing could be further from the truth," argues Bartlett. He adds, "No one has been arrested, I know of no one who has been accused. However, those that are supposed to know better have foisted upon the industry a Gambling Commission that will cost £14m in direct costs and at least double that amount in general compliance costs." The tone of this argument reflects how badly mistreated this industry feels and it is an example of how problems can arise when regulators and industry do not work together. Bartlett later notes that, out of 2,800 gambling websites, only 14 have applied for licences in the UK. While it is too simplistic to put this solely down to the Gambling Commission, it is clear that any corporate is going to think twice about establishing a business in a place where it feels stifled by compliance.

The topic of government working with industry in the fight against financial crime is something that the UK's Attorney General, Baroness Scotland, covered in her recent speech published on gtnews, *The UK's Response to Global Financial Crime*. She describes how financial information, generated and stored by industry, can aid criminal prosecution by allowing law enforcement to:

Look backwards: by piecing together how a criminal conspiracy was developed and implemented and the timelines involved.

Look sideways: by identifying or confirming associations between individuals and activities linked to conspiracies, even if overseas-often opening up new avenues for enquiry.

Look forward: by identifying the warning signs of criminal or terrorist activity in preparation.

Cross-border Co-operation

Contentious cross-border compliance issues are also highlighted in the article from Bartlett at GBGC. He specifically picks out the US as an example of this. In the US, online gambling is illegal-but online gambling websites do exist and are accessible to US residents. In this instance, US authorities have prosecuted directors of online gambling sites using regulations such as the Wire Act and, more recently, the Unlawful Internet Gambling Enforcement Act (UIGEA). This is despite the fact that these companies are not registered in the US and are mostly trading on the major stock exchanges such as the FTSE 100. Authorities in the US justify this as an attempt to remove the supplier of the product that is illegal in the US – the online gambling companies. This could well be the case, but it also leaves them open to the accusation of protectionism. GBGC's Bartlett argues that their motive "will no doubt change when the timing is right for their own Las Vegas-based companies to move into this lucrative industry." He also notes that there is currently a Bill being debated in the US Congress that aims to partially legalise online gambling in the country – and while this may just be coincidence, it doesn't take too much of a mental leap to link these two moves. If this is the case, it is a fairly cynical manipulation of events and not in the spirit of the law.

Despite this, cross-border co-operation is obviously critical in combating money laundering across the globe. In her article, Baroness Scotland describes how these crimes can often have an international dimension, "they may be conceived in one jurisdiction, perpetrated on victims in others and the proceeds salted away in yet others." This can make following the trail of criminality difficult for local law enforcement to follow up. "Even with recent improvements in mutual legal assistance, the obtaining and deployment of foreign evidence causes problems for our police and courts," she says.

The Role of Banks

While the compulsion for corporates to involve themselves in AML efforts is increasing, banks have been positioned at the forefront of the fight against financial crime for some time. In his article, Can Banks Prevent Financial Crime?, Brendan Hewson, from Global Risk Advisory Services (gra-services), looks at areas that banks may find are weak points in their anti-fraud armour, and how these can be strengthened. It may be easy to remember the acronyms for Know Your Customer (KYC) and Know Your Employee (KYE), but the fact that US\$6.6bn was wiped off annual revenues by employee fraud last year suggests that these instructions are not being applied correctly. Hewson offers a three-step plan that banks should consider to minimise internal fraud:

Education-prevention is the product of experience, education and teaching.

Regular training for all staff-deliver interesting and interactive training sessions. The use of instructors with practical experience, credibility, integrity and ingenuity is paramount.

Knowledge-know your employees and know your customers while making sure there are practices and procedures in place with a mandatory compliance requirement attached to them.

To combat the threat of employee fraud, Hewson makes recommendations that every bank should implement if they haven't already. For example, establishing anonymous reporting mechanisms while strengthening internal controls has the effect of narrowing the fraudster's window of opportunity. Implementing a documentation policy means that it is clear who should be writing and signing correspondence and for whom-in this situation, any suspicious activity will be easier to identify and investigate.

The Facebook Conundrum

Social networking sites, such as Facebook, have seen a large rise in popularity in 2007. But in registering for a site like this, you or your employees could be posting valuable information for identity thieves. In his article, Banks on Facebook? Operational Risks, Operational Rewards, Paul Johns, from Complinet, explains that, "people regularly publish their name, address, email address, date of birth, phone number and relationship status." This information can be enough to set up a fraudster with a false identity. But, on the other hand, the same information could also be used by those people who are the epitome of the fraudster's moral counterpoint-bank compliance agents! Networking and information sharing websites can be useful to bank employees including marketers, recruiters, compliance professionals and staff who observe AML and KYC regulations.

Complinet's Johns refers to the example of TD Canada Trust-a bank that has developed a Facebook group to help students manage their money and, of course, promote its products. "At the time of writing, TD MoneyLounge had attracted 11,769 members, representing a captive audience for the bank's products and promotions," notes Johns. This cautionary tale may well have most of you clicking through to tighten your security settings after reading this commentary-if the fraudster doesn't get you then the banks will. Of course, this is just an example of how banks can add some extra functionality to their AML profiles, obviously the very nature of Facebook may lead some users to be less than truthful when they think that only their 'friends' are reading. Official watch lists are a more reliable source of AML protocols by far.

Online Banking Security

It is curious that Internet users seem to have a certain amount of blind faith in social networking sites, while at the same time confidence in online banking is falling. In their article, Online Banking: How to Avoid the Threat of Fraud, published earlier this year on gtnews, Gail Kerr and Sunil Ippagunta, from KeyID, describe the effect of this uncertainty. Phishing emails and the amount lost per online fraud have increased hugely-even though the amount of online fraud recorded has fallen. "Gartner estimates that in 2006 alone, over US\$2bn was lost in US e-commerce by customers abandoning or avoiding online banking, Internet shopping and e-payments," report Kerr and Ippagunta.

Clearly one of the key benefits of online banking is the savings made by the bank through automation, so if customers return to traditional banking methods, the so do the associated costs. In order to address this, banks need to ensure that they have a variety of security enhancements in their online bank offering-and especially make sure that they market this and let their corporate and personal banking customers aware of the measures they are taking. Trust can be a fragile element in a banking relationship-it takes a lot of work to build up and maintain and it can be destroyed with just one

mistake from the bank. To help counter this, Kerr and Ippagunta suggest a checklist that banks should incorporate in their online banking offering:

Mutual verification where the customer verifies the bank and the bank verifies the customer.
Out of band authentication because relying on the primary channel to detect a 'man-in-the-middle' will not work.
Two site validation where each location knows only part of the code.
Two factor authentication, which uses a physical device like a smartcard to add the 'something you have' factor to the 'something you know' much like a password.
End point and channel dependent authentication.
Session dependent authentication.
Transactional encryption prior to critical transactions.
Proactive monitoring to detect online threats such as trojans and malware.
This may look like a formidable list, but it is nothing compared to the task of re-asserting customer confidence following an online security breach.

Conclusion

Dealing with the threat of financial crime today is a costly and time-consuming business for corporates, banks and regulators-all three would agree with this statement. They should also agree that it is absolutely vital to make sure that programmes are in place to prevent and mitigate the risk of all areas of financial crime, from AML to online fraud. But when it comes to how much money is spent, how many protocols are initiated and how many regulations are enforced, there seems to be far less common ground. Motivation for this could range from self-interest, protectionism, penny-pinching and misplaced assumptions that fraud is something that happens to someone else. In the grey area that these excuses produce, the financial criminal can benefit.

Stung into action by global events such as 9/11, Enron, the dot-com crash and even the current credit crunch, regulators around the world have created a vast amount of legislation that banks and corporates must abide by or face the consequences. While these events were, and are, hugely traumatic for the financial markets, the regulator has been criticised for going beyond its remit. There seems to be a climate of uncertainty and fear in some quarters whenever the 'C' word is mentioned, and this shouldn't be the case with compliance.

Corporates, banks and regulators share responsibility in the fight against financial crime. Mutual dialogue and a willingness to listen to each other and work together is essential if all three parties are going to achieve their shared goal of eliminating, or at least minimising, financial crime. The tools exist to help make this happen-technology is constantly advancing in this area-and so are the experts with experience on the subject.

Ben Poole is Section Editor at gtnews