

Financial crime

There were many promising developments in the anti-financial crime arena in 2006. However, the rapid evolution of financial crime means that new risks have arisen that will need to be addressed in the future. There is also a need for strengthened leadership and resources from all parties to improve the existing frameworks and embed new anti-financial crime 'architecture' in 2007 and beyond.

Financial crime risks continue to evolve more quickly than we and the industry can respond. In the previous edition of the *Financial Risk Outlook* we highlighted the use of corrupt low- and mid-level employees by organised crime as a method to evade anti-fraud and anti-money laundering (AML) systems and controls. This is still the case, but 'insiders' now appear to be facilitating high-tech crime by also allowing criminals access to systems, stealing data and revealing weaknesses. While new technologies, such as Chip and PIN, have reduced fraud in some areas, criminals have found ways to circumvent some of these fraud prevention measures. We expect this evolution to continue and perhaps increase, as criminals exploit the advances of the 'information economy'.

Information security

Over the last 12 months organised crime has become more innovative

The technological competition between firms and law enforcement agencies on the one hand and fraudsters on the other continues. Firms and law enforcement have been at a disadvantage in this competition, in part due to the historically disjointed approach to combating financial crime (especially financial fraud) by industry, government and law enforcement.

Information-security risks (both high-tech and low-tech) continue to increase in importance, due to technology's rapid evolution and criminal exploitation of our reliance on personal data for verification and remote access to financial products and services. Information security and data protection are becoming more significant issues for our financial crime and consumer protection statutory objectives. Although a firm may suffer direct losses when personal and financial data is lost or stolen, it also creates identity-fraud risks for consumers, which can have both direct financial and additional

The main changes to the AML environment in 2007 will be systemic, with a significant amount of 'regime change'

Changes to the AML regime create opportunities and risks

non-monetary costs, such as time or distress. There have been a number of high-profile incidents where firms have lost data due to an unacceptable disregard for the identity-fraud risk to consumers. These incidents also demonstrate that the reputational risk to firms of significant data loss is very high.

Third-party information security is a growing problem. As financial firms tighten their information security, criminals are targeting sectors that hold the same or similar data, but have weaker data-protection systems and controls. For example, some telecoms, utility or non-financial retail firms may have inadequate systems and controls which are more vulnerable. However, the public and the media often blame the banking industry, even though they have little control over the actions of these other businesses. This public reaction could reduce confidence in innovative and efficient delivery channels, such as internet banking and off-shoring.

Money laundering and terrorist finance

The industry is adapting to the new AML regime that came into effect in September 2006, when our new Handbook provisions and the revised edition of the Joint Money Laundering Steering Group (JMLSG) Guidance came into force. Firms have been reviewing their procedures as a result of these policy changes. However, there is a risk that firms' implementation of a more risk-based approach to financial crime will be undermined if the processes put in place are not dynamic and flexible enough to adapt to the constantly evolving operating environment. In the previous edition of the *Financial Risk Outlook* we highlighted that some firms or sectors were incorrectly interpreting the move to a risk-based approach as our de-prioritising AML. We believe that this misconception is less prevalent, but it is still something that we are concerned about and will vigorously seek to correct.

In the previous edition of the *Financial Risk Outlook* we discussed the tensions created by some aspects of the Suspicious Activity Report (SAR) regime, particularly those regarding feedback to industry and the 'Consent regime'.¹ These tensions still exist, but there appears to be fresh impetus on all sides to resolve them. The Lander Review of the SAR regime is being implemented by the Serious Organised Crime Agency (SOCA), and expectations that the regime will fully deliver on its vast intelligence potential are high. However, as with other aspects of the anti-financial crime architecture, the risk remains that the expectations of some stakeholders may be higher than the results delivered by others. This could lead to stakeholders complying with the letter, rather than the spirit, of the legislation and a less-than-effective SAR regime.

The UK continues to lead the way in a risk-based approach to AML and financial crime. The implementation of the Third EU Money Laundering Directive and the Financial Action Task Force's (FATF) evaluation of the UK's AML regime both offer opportunities and risks for the AML regime. Raising international standards is beneficial for us and the industry, especially with the risk-based approach being institutionalised internationally. However, the risk remains that the UK may come under pressure to implement a more prescriptive approach.

¹ The 'Consent regime' allows persons and businesses generally, not just those in regulated sectors, to avail themselves of a defence against money-laundering charges by seeking the consent of the authorities to conduct a transaction or undertake other activity about which they have concerns. The legislation gives the authorities seven days to respond. Where consent is refused, the transaction or activity must be frozen for a further 31 days.

Increasing globalisation has reduced barriers to trade, and UK markets have benefited from this trend. However, increasing globalisation has also increased UK markets' and firms' exposure to jurisdictions where counterparties are not subject to equivalent rules for reducing financial crime. There is a risk that this could lead to more incidents of financial crime in UK markets, including large money-laundering scandals.

The July 2005 terrorist attacks in London demonstrated the strengths and weaknesses of the Counter Terrorist Financing regime. The difficulties in recognising terrorist-related account activity, coupled with the low amounts needed to carry out the attacks highlight the challenges for firms and law enforcement in identifying terrorist attack planning. However, the cooperation and information yielded from firms after the attack was vital for the investigations. Financial intelligence and evidence provided by the sector continues to play a crucial part in developing both proactive and reactive counter terrorist investigations. The current level of terrorist threat may increase the high level of demand on firms to support proactive and post-incident investigations. We expect terrorist funding to continue to be a major source of reputational risk for the financial services industry in the future. Those individuals intent on funding terrorism here and abroad show the same ingenuity as organised criminals but often a different pattern. For example, funding for terrorism can come from legitimate sources as well as the proceeds of crime.

Fraud

We welcome the recommendations of the recent Fraud Review

The public-sector response to fraud has been hampered by the fragmented structure of the UK's anti-fraud framework and the lack of a coordinated strategy for dealing with fraud. For example, figures produced by CIFAS – the UK's Fraud Prevention Service – show that during the first nine months of 2006, the volume of reported fraud grew by over 9%, with identity fraud rising by 17%, compared to 15% for the same period 12 months previously. However, a number of recent proposals have the potential to improve this situation. The government's Fraud Review has recommended a National Fraud Strategic Authority and a National Fraud Reporting Centre to gather a consistent measure of fraud. The Fraud Review also recommends the creation of a national lead police force for fraud and that fraud should be made a policing priority. We, like industry, have welcomed the findings and conclusions of the Fraud Review. However, there is a risk that the recommendations are not fully implemented due to disagreements over funding and control of the new powers.

The Fraud Review also highlighted the need for more data sharing within and between the public and private sectors. There appears to be political appetite for this, with the responses to the Home Office consultation on New Powers Against Organised and Financial Crime recommending CIFAS as the most appropriate vehicle to share public and private information to prevent and detect fraud. This data sharing is a priority to tackle fraud, but there is a risk that some firms may not be willing to share this information for reputational or competitive reasons.

Fraud risk is ultimately the responsibility of senior management

As part of a risk-based approach to regulation we do not require firms to comply with detailed rules and guidance on fraud management. However, firms are still required to take reasonable care to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime. If anti-fraud messages are not sponsored at the highest level within a firm and embedded within the firm's culture, it is unlikely that an effective fraud strategy will develop. Employees take their lead from the actions of the most senior managers. Senior management need to continue to invest in systems and controls and manage their responses to fraud to avoid being targeted as the weakest link.

The industry continues to battle organised and opportunistic insurance fraud

There have been a number of positive developments for insurance claimant fraud over the last 12 months. For example, the Insurance Fraud Bureau is in operation, and it is hoped that this will help reduce the scope for organised crime to abuse the general insurance market. It is estimated that a quarter of claimant fraud is organised rather than opportunistic. The Association of British Insurers (ABI) is also promoting best practice in claims handling and is encouraging firms not to see fraud prevention as a competitive issue. However, opportunistic claimant fraud continues to be high, with firms having to tolerate a higher level of fraud than other sectors to keep honest customers satisfied. This is a persistent problem which requires concerted action to alter the public opinion of insurance fraud.

The introduction of Chip and PIN has led to an overall drop in card fraud, but there has been a shift in emphasis by fraudsters to card not present fraud and spending overseas, where Chip and PIN is less widely used.

Table E1: UK plastic card and online banking fraud losses

Type of fraud	January to June 2005	January to June 2006	+/-% (05/06)
Online, phone and mail order fraud	£90.6m	£95.3m	+5%
Counterfeit	£45.6m	£53.0m	+16%
Lost/stolen	£44.3m	£36.1m	-19%
Mail non-receipt	£22.8m	£9.8m	-57%
Card ID theft	£16.1m	£15.0m	-7%
Total	£219.5m	£209.3m	-5%
Contained within this total:			
Fraud abroad	£41.8m	£48.5m	+16%
Retailer (face-to-face)	£73.2m	£42.1m	-43%
Cash machine fraud	£28.8m	£39.6m	+37%
Online banking fraud			
	January to June 2005	January to June 2006	+/-% (05/06)
Online banking fraud	£14.5m	£22.5m	+55%
Phishing incidents	312	5,059	+1,471%

Source: APACS

Consumers can play an important part in preventing fraud

We have also seen organised criminals adapting old techniques to new technologies with traditional ‘skimming’² attacks on the PIN entry devices. This involves tampering with the device and capturing details from the card’s magnetic strip and PIN details. While the Chip remains secure, the ingenuity and resilience of the fraudsters is concerning. Online banking fraud is at a relatively low level, but the increase is worrying and can be partly explained by the explosion in ‘phishing’³ attempts.

According to research by APACS – the UK Payments association – many consumers are not acting in the most secure manner:

- * 25% have disclosed their PIN to someone else;
- * 27% use the same PIN for all their cards;
- * 44% still let their cards out of their sight (in restaurants and bars for example); and
- * 51% never check that a website address changes from ‘http’ to ‘https’ before making a purchase, indicating that awareness of secure shopping advice is low.

There is a risk that anti-fraud is seen as an issue for firms only. However, tackling this problem requires the development of an anti-fraud culture throughout society and is the responsibility of all who hold valuable financial and personal data.

While no comprehensive measure of the size of fraud exists, work by the Home Office on the harm fraud committed by organised crime causes to society suggests that it may be second only to Class A drug trafficking, and roughly equal to the harm from people smuggling and people trafficking combined.⁴ The research we undertook on ‘boiler rooms’ demonstrates how the social harm of financial crime is often felt by the most vulnerable in society.⁵

Organised criminals know the weaknesses of internal anti-fraud controls

As noted throughout this section, the ways in which firms are defrauded have changed in recent years, with criminals showing themselves to be highly dynamic in reacting to changes to firms’ anti-fraud systems and always looking for the ‘weak link’. A reported and noticeable trend in recent years has been organised criminals (and terrorists) having knowledge of firms’ anti-fraud measures, allowing them to defraud the financial services sector at levels that fall below firms’ ‘fraud appetite’ and are outside of their control. For example, criminals have now begun to target asset management companies using Companies House – the official UK government register of UK companies – and other publicly available data. This risk is exacerbated because this sector has not traditionally been targeted by third-party fraud and so does not have the same level of prevention as other sectors, such as retail banking or general insurance.

2 ‘Skimming’ is the act of electronically copying a card’s magnetic strip details and putting them onto another (counterfeit) card.

3 ‘Phishing’ refers to a scam in which an email is sent falsely claiming to be from a legitimate enterprise in order to persuade the user to surrender private information that will be used for identity theft.

4 *Fraud Review: Final Report*, Attorney General, 2006.

5 *Typical boiler room victim loses £20,000 warns FSA*, FSA Press release, 6 June 2006.



We expect firms to take into account the social harm of crime as well as the direct losses to themselves

However, we expect firms to take into account the social harm of crime as well as the direct losses to themselves when assessing their ‘appetite’ for fraud and other financial crime risks. We also expect firms to consider the full implications of the risks they face, which may have wider effects on their reputation, their customers and the markets in which they operate. Although firms have an obvious incentive to protect themselves from fraud, they do not always suffer all the direct and indirect costs. The negative externalities of fraud, due to rapidly evolving financial crime and the rise of organised criminality, are tackled best in partnership. The risk that firms do not fully engage with all relevant stakeholders appears to be falling in most sectors, but there is still work to do in embedding recent cooperation across all sectors and stakeholders.