CIMA

FINANCIAL MANAGEMENT

OCTOBER 2006 £4.50

TECHNICAL
Supply-chain accounting
Securitisation
Book reviews

STUDY NOTES

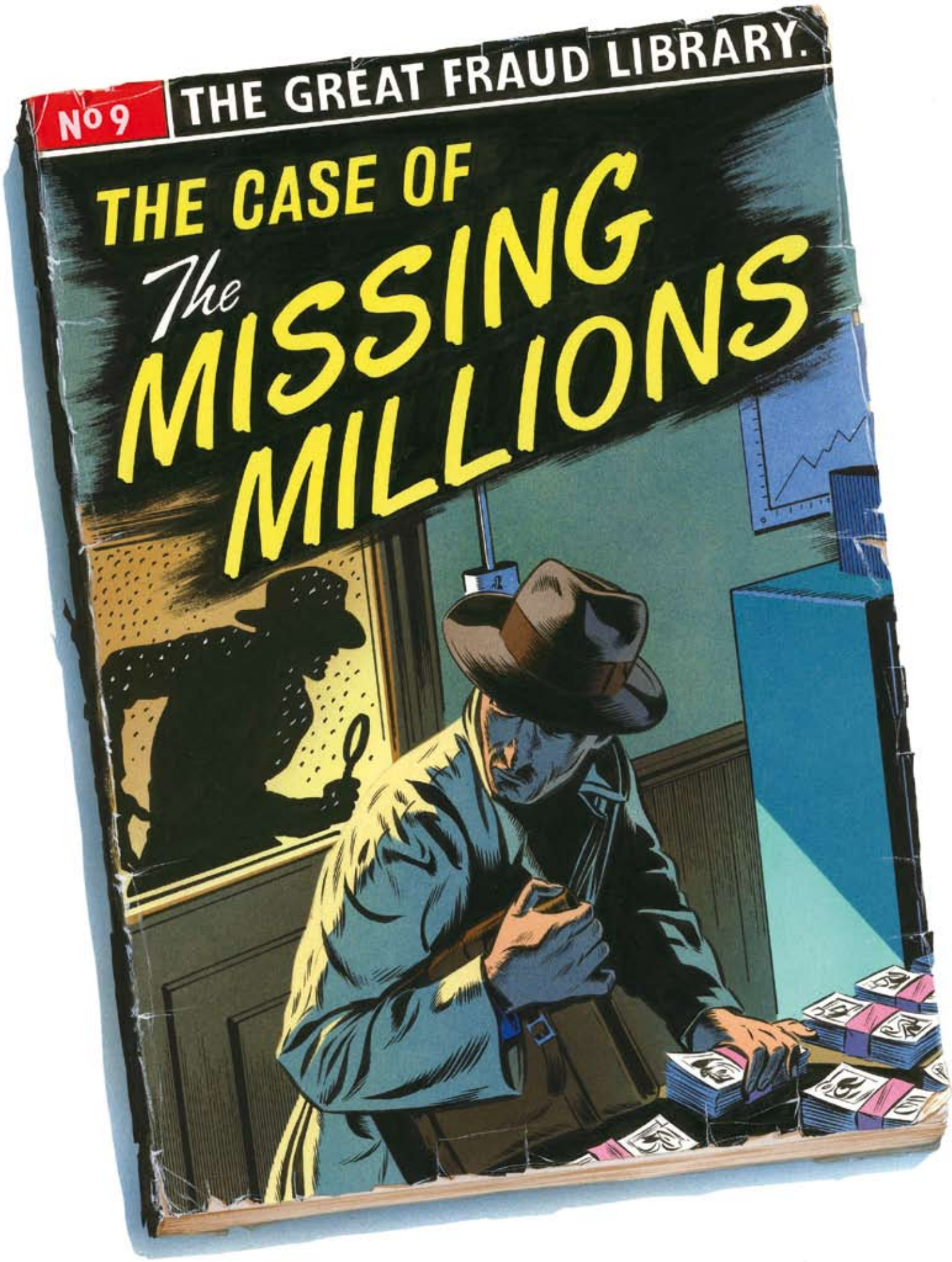
Paper P10
Test of Professional Competence in Management Accounting
Paper P3
Management Accounting – Risk and Control Strategy
Paper P6
Management Accounting – Business Strategy

OUT OF THE BOX

Charles Allen, chief executive of ITV, on why he's quitting television

CAUGHT IN THE ACT

Will the UK's new anti-fraud measures put criminals out of business?


No 9
THE GREAT FRAUD LIBRARY.
THE CASE OF
The MISSING MILLIONS

DRAG.NET

Fraudsters – especially the new breed of criminal that's exploiting web technology – have largely kept one step ahead of the UK's antiquated legislation, but it's about to be upgraded. **Neil Hodge** asks the lawyers whether the fraud bill will close all the loopholes.

At the end of 2005 Norwich Union estimated that fraud had cost the UK economy £16bn over the year – the equivalent of each adult in the country being £340 out of pocket. Compare that figure with the amount of money under consideration in the 222 fraud cases that reached court over the same period: £942m, or just under six per cent of the total. According to KPMG's annual *Fraud Barometer* publication, this was an improvement on the 172 fraud cases, worth only £329m, prosecuted in 2004. The research also found that, although the government was the biggest victim, financial companies had lost ten times more to fraud in 2005 than they had done over the previous year.

The conclusion from these figures is clear: fraud cases are tremendously difficult to prosecute, never mind prosecute successfully. The collapse of several recent high-profile cases, such as the failed Jubilee line litigation in May 2005, which tried six men for an alleged conspiracy to gain inside information on the £2bn extension to the London Underground network, has brought into question the adequacy of existing legislation – and what actually constitutes fraud. The problem, according to legal experts, is that the specificity of the current regulations governing this area and their allowance of technical defences has made bringing cases enormously expensive and securing convictions virtually impossible. The Jubilee line trial cost £60m alone, for example.

As a result, the government has announced that it's taking a co-ordinated approach to tackling the problem. It has introduced the fraud bill, which is currently before Parliament, and it will bring forward another bill to allow for non-jury trials in a limited range of serious and complex fraud cases.

In addition, the government has just published for consultation the final report of the Fraud Review, which began a year ago. This advocates the establishment of a financial court jurisdiction so that the different proceedings arising from serious fraud cases can be combined in one court and be heard by specialist judges. It suggests allowing plea-bargaining as an alternative to a full criminal trial.

The report's other proposals include setting up a national strategic authority as a public-private partnership to devise and implement a UK-wide anti-fraud strategy. It also recommends that the government should establish a national lead police force and fraud reporting centre. The consultation period closes on October 27.

Rosalind Wright, chairwoman of the Fraud Advisory Panel, an independent group of volunteers that aims to raise awareness about the economic damage caused by fraud, says that the success of the proposals is "completely dependent on how much money the government is prepared to put into them". And funding is an issue. The attorney-general, Lord Goldsmith, estimates the costs of establishing a strategic authority, reporting centre, lead police force and, if appropriate, regional support centres at between £13m and £27m a year.

But Wright believes that the plea-bargaining proposal is "deeply flawed". This is because the fraud bill provides for only

Illustrations: Mark Thomas

THE VERY LONG ARM OF US LAW

In Texas, it seems, the sheriff always gets his man, even if those under suspicion aren't US citizens or residents and the treaty on which prosecutors are basing their extradition case hasn't even been ratified.

Former NatWest employees David Bermingham, Gary Mulgrew and Giles Darby – better known as the NatWest three – were put on a flight from the UK to Houston in July to face fraud charges, despite widespread claims that the process used to do so was unfair and that they should stand trial in the UK.

US prosecutors had issued arrest warrants for the three men in 2002, accusing them of conspiring to defraud their employer and investors in collapsed US energy company Enron. It's claimed that they were involved in a fraud in which Greenwich NatWest was advised to sell its stake in an Enron unit at well below its market value. The trio then quit the bank and bought a $250,000 stake in the same unit – which they later sold, allegedly at a much higher price.

The men have denied any wrongdoing, but US prosecutors believe that they conspired with Enron's former CFO, Andrew Fastow – who's now serving a ten-year sentence – in the sale. As a result, they face seven counts of wire fraud in the US and, if convicted, could face prison sentences of up to 35 years.

They were arrested in the UK on April 23, 2004 and extradition proceedings started two months later. In September 2004 a judge ruled that the deportations could proceed. Such cases are covered by the Extradition Act 2003, which is the result of a treaty that has been ratified by the UK but not the US. On June 21, 2006 the House of Lords threw out the NatWest three's appeal against extradition. Less than a week later the European Court of Human Rights also ruled against them.

Critics claim that the legislation is unbalanced as it stands, giving British nationals far less legal protection. Under the act, the US authorities need to outline the alleged offence and provide "evidence or information that would justify the issue of a warrant for arrest in the UK". For its part, the UK must provide the US with evidence of "probable cause" if it wishes to extradite someone from the US – a much stronger legal test. Some lawyers believe there's a real danger that a grave injustice will occur where a country such as the US can request an extradition without providing *prima facie* evidence – ie, all facts essential to its case.

Critics of the legislation claim that the decision to designate the US as one of more than 20 non-EU countries where *prima facie* evidence is not required for extradition was not voted on in Parliament, although the government maintains that the issue was fully debated.

There is also concern that, more than two years after the extradition treaty was signed, it has yet to be ratified by US Congress. Two-thirds of senators need to support the treaty for it to be passed.

So far, only a handful of US nationals have been extradited to the UK while about 50 UK citizens face an enforced journey the other way, although it's likely that many more have already gone to the US voluntarily to increase their chances of obtaining bail. Notable cases include Ian Norris, former CEO of Morgan Crucible, who's likely to be the first British national to be extradited on price-fixing charges – something that Sir Anthony Tennant, chairman of Christie's when it formed its infamous cartel with Sotheby's in the nineties, managed to avoid. And Gary McKinnon, who admitted hacking into US government computer networks, albeit for "research purposes", could face life in a federal prison now that the home secretary, John Reid, has approved deportation proceedings against him.

"Plea-bargaining can save time and money, but it works only if there's a real threat of a long prison sentence"

a ten-year maximum prison sentence, whereas convicted fraudsters in the US can expect to face much stiffer sentences. For example, Enron's former chief executive, Jeffrey Skilling faces a sentence of up to 185 years after being found guilty of 19 counts of fraud and conspiracy relating to the company's collapse. The US is also more proactive in seeking extradition to try those suspected of committing a major fraud, as illustrated by its determination to bring the NatWest three to book (*see panel*).

"Plea-bargaining can save a lot of court time and money, but it works only if there is a real threat of a long prison sentence, which we don't have in the UK," Wright says.

The government hopes that the fraud bill will make prosecutions a lot easier. Introduced into the House of Lords in May 2005, it should receive royal assent by the end of this year if all goes to plan. The bill creates the statutory offence of fraud, which can be committed in three ways: "where a person dishonestly makes a false representation, or wrongfully fails to disclose

HOW NOT TO BE THE PHISHERMAN'S FRIEND

Not what it seems: phishing e-mails often display logos and other key branding elements from the companies they purport to come from

The objective of phishing is to trick you into giving up your personal banking information, *writes Martin Nimmo*. In most cases, you will receive an e-mail purporting to be from a financial services provider or from eBay or PayPal. This may inform you that there has been a breach of your security, that you need to update your details or that you have purchased an item. You are then directed to a web site, which appears to be legitimate, where you will be asked to disclose your details.

If you receive any such message, do not even reply to it, let alone e-mail any personal information. If you are worried, contact the real organisation by post or telephone at an address or number you know to be genuine. You should also install appropriate software to protect you from this type of attack. Anti-spyware and personal firewalls are ideal, while anti-virus software will give you some measure of protection against Trojan horse programs.

Last November the *Times* reported the case of a fraudster who'd been jailed for duping almost £200,000 from eBay customers using a phishing scam. David Levi of Lytham, Lancashire, was the leader of a gang that had amassed the money by stealing account details from users and assuming their identities. It is believed to be the first successful prosecution for phishing.

Cash-back fraudsters may try their luck when you offer something for sale on the internet, in *Exchange & Mart* or even in the small ads in your local paper. You may be contacted by a "buyer" who wants to purchase the advertised item without wanting to see it. They will send you a cheque for considerably more than the asking price. You will be asked to send some or all of the difference to the buyer/shipping agent by money transfer. The cheque will either be forged or stolen and, even if it's cleared by your bank, it can be recalled later and you won't be reimbursed for your loss.

Research by the Association for Payment Clearing Services shows that the amount misappropriated using credit cards via internet, mail-order and telephone sales – ie, where the card is not seen by the vendor – increased by 29 per cent in the UK to £90.6m by the end of 2005.

Many people put themselves at risk of fraud by not taking basic precautions. According to research, one in eight people fails to log out after shopping online, leaving their financial details available for others to see, while one in four does not check that a web site is secure (the padlock symbol to the bottom right of your browser's screen will usually indicate this).

Consumers are also urged to sign up to security schemes such as Verified by Visa and MasterCard SecureCode, under which you must type in a password or security code when buying online. This should make it impossible for fraudsters to use stolen card details.

Martin Nimmo is head of policy and plans in CIMA's professional standards department.

information, or secretly abuses a position of trust with intent to make a gain or to cause loss or to expose another to the risk of loss". Although there is no definition of what an abuse constitutes, "the bill does make it clear that it is to be widely construed", according to Adam Vause, senior associate at law firm Norton Rose.

Peter Kiernan, partner in the fraud and financial crime team at Eversheds solicitors, points out that one of the notable features of the proposed legislation is that "it will be sufficiently flexible to allow prosecutions where a defendant has been proved to have acted dishonestly, irrespective of the method used to commit the offence. This allows for the law to keep pace with technological advances."

The newly defined offence will carry a maximum sentence of ten years – three years more than the current tariff for crimes of theft and false accounting. It will replace at least eight offences under the theft acts covering "obtaining by deception" and related crimes, although it is likely that the offence of conspiracy to defraud will be retained. Prosecutions will rely on proof of dishonesty on the part of the defendant, rather than the effect of any representations made on the mind of the victim, as with traditional offences of deception.

The longest possible sentence for fraudulent trading remains unchanged at seven years. There is no limit to the fine that can be imposed on organisations involved in fraud.

The bill will also create two new offences that are mainly aimed at tackling fraud committed using technology, which is hard to prosecute under the existing legislation. Both will carry a maximum sentence of five years. The first, obtaining services dishonestly, will cover situations where credit cards that have been improperly obtained are used to obtain services from the web, or any other instance where false information is provided to a machine. The second, possessing articles for use in frauds, will cover computer programs designed to generate credit card details that are then used to commit or enable fraud.

It should become much easier to prosecute individuals and gangs for high-volume, low-value scams

In essence, the bill makes it clear that it is irrelevant what sum of money has been embezzled, which means that it should become much easier – and probably more worthwhile – to prosecute individuals and gangs for high-volume, low-value scams.

Rosalind Wright is optimistic that the new legislation will increase the number of successful prosecutions. "At the moment the limitation of the eight or so statutory offences, principally under the theft acts, means that cases can be brought only in situations where the facts can be fitted into the wording of these sometimes arcane offences, such as procuring the execution of a valuable security by deception or obtaining property by deception," she says. "The limitation here is that you need to prove that someone was actually deceived by a fraudulent representation. This is often impossible in an investment fraud, where investors often part with money for no better reasons than that their colleagues had invested with the same enterprise or that the fraudster 'sounded genuine'. Where a machine such as a computer has been the instrument through which money was fraudulently obtained, a charge for deception can't currently be brought at all, because no human being was actually deceived."

The new legislation will specifically cover "phishing". This generally involves the sending of an e-mail to an individual falsely representing that the message has been sent by an institution where the recipient maintains an account. The recipient is asked to click on a link to a web site masquerading as the genuine one, thereby allowing the phisher to obtain their password details (*see panel, previous page*).

The need to address the use of technology in fraud was highlighted by *R v Preddy* in 1996. In that case, funds were obtained by electronic bank transfer, which was unknown in 1968 when the first theft act was passed. This movement of money was held by the House of Lords not to be "obtaining property" under the strict wording of the law, and many convictions for offences in similar circumstances were quashed.

Despite eliciting a largely positive response, the bill is not without potential problems. One of the more keenly debated issues concerns the nature of the English courts' jurisdiction. It had been suggested that they should be granted "nationality jurisdiction", giving them authority over English nationals and companies involved in any fraud committed overseas. The government rejected this idea, claiming that the provisions of the existing Criminal Justice Act 1993, which apply to all statutory fraud offences, are sufficiently broad, since they give the English courts jurisdiction (in relation to a person of any nationality) where a "relevant event" takes place in England or Wales. But some legal experts argue that neither of these approaches seems particularly appropriate to a crime that, by its very nature, can easily be committed from anywhere in the world.

> ***"It's perhaps regrettable that the new legislation will not explicitly facilitate private prosecutions"***

"One of the reasons for the inclusion of phishing in the fraud bill was that the provisions of the Computer Misuse Act 1990 were not deemed clear enough to capture phishing in all its forms, and yet that act gives the courts a far broader, more comprehensive jurisdiction than the fraud bill," says Clive Greengrass, a partner in IT and e-commerce at Olswang.

Under the Computer Misuse Act 1990, the courts have jurisdiction over any case where either the crime was committed in England or Wales, or the victim was in the country at the time the offence occurred. "It's surprising that the government didn't mirror this provision in the fraud bill but instead opted for jurisdictional rules that are less appropriate to online crime. As it stands, the bill still gives the perpetrator the chance to argue that the relevant event didn't occur in the country," he says.

Greengrass points out that, while the new approach is to be welcomed, tracking down and bringing online fraudsters to book – particularly those that operate abroad – is another matter. "It's perhaps regrettable that the new legislation will not explicitly facilitate private prosecutions," he says. "That would have allowed private companies and other victims of online fraud to take action themselves in cases that the police and Crown Prosecution Service don't intend to pursue because they lack sufficient resources or have other priorities." **FM**

Neil Hodge is a writer specialising in business and regulation.