

# **The Prevention of Fraud**

Michael Levi

**CRIME PREVENTION UNIT: PAPER 17**  
**LONDON: HOME OFFICE**

---

Editor: Kevin Heal  
Home Office Crime Prevention Unit  
50 Queen Anne's Gate  
London SW1H 9AT

© Crown Copyright 1988  
First published 1988

### **Crime Prevention Unit Papers**

The Home Office Crime Prevention Unit was formed in 1983 to promote preventive action against crime. It has a particular responsibility to disseminate information on crime prevention topics. The object of the present series of occasional papers is to present analysis and research material in a way which should help and inform practitioners whose work can help reduce crime.

ISBN 0 86252 359 1

## Foreword

With the recent increase in public interest in the world of finance and the widening of share ownership, this report on the prevention of fraud has come at an appropriate moment. Prepared by Dr. Michael Levi, Senior Lecturer in Criminology at the University of Wales, College of Cardiff, the report is based on research supported by the Home Office and the ESRC and is a digest of a fuller text in preparation.

The report aims to alert the unsuspecting individual or company to the need for elementary precautions against fraud, and to give an idea of the form those precautions might take. It succeeds in presenting clear, practical guidelines on a complex, technical subject, and may save the unwary from costly error.

J A CHILCOT

*Deputy Under Secretary of State  
Home Office, Police Department  
September 1988*

## **Acknowledgements**

I am grateful to the Home Office and the ESRC for funding the research on which this paper is based, and to the Metropolitan & City Company Fraud Department and members of the South Wales Constabulary for helpful discussions. I would also like to thank Claire Austin, Gloria Laycock and Kevin Heal of the Home Office Crime Prevention Unit for support and advice.

Michael Levi

## Contents

|                                  | <i>Page</i> |
|----------------------------------|-------------|
| Foreword                         | (iii)       |
| Acknowledgements                 | (iv)        |
| Introduction                     | 1           |
| Methods of Fraud                 | 6           |
| Preventing Fraud                 | 8           |
| Preventing frauds on individuals | 10          |
| Preventing fraud on business     | 11          |
| The prevention of computer fraud | 15          |
| Reporting Fraud                  | 17          |
| Conclusion                       | 17          |
| References                       | 18          |
| Crime Prevention Unit Papers     | 19          |

## Introduction

Commercial fraud is a very broad subject. Its victims range from the very wealthy to the very poor. It includes swindles by 'professional criminals' against suppliers of goods on credit, banks and credit card companies, mail-order purchasers, and people willing to pay money upfront for a promised job or loan; by 'criminal professionals' against their clients' accounts held in trust or against building societies and banks supplying mortgages for their imaginary clients; and by businesspeople against consumers and employees. It is not always readily apparent whether or not a loss or attempted loss is a fraud: some people may believe that they have been defrauded though what was done was not contrary to the *criminal* law but rather was a civil deceit or even was perfectly lawful. Consequently, quite legitimately, when the police receive reports of suspected frauds, they refer some back for further investigation and/do not record them as crimes. Other complaints may, on investigation, turn out to be very different frauds from those the complainant alleged. What victims often find hard to understand is that irrespective of whether or not a fraud 'actually' occurred, it can only be defined as criminal fraud if there is evidence credible to outsiders that what happened fits into the category of 'certain crime': there is a larger grey area here than in other areas of serious crime (a full discussion of the fraud control process is contained in my recent book, "Regulating Fraud", Levi 1987).

Fraud traditionally has been an area in which the police crime *prevention* profile has been rather low. The aim of this paper is – without going into the more complex kinds of international fraud — to give police officers, businesspeople, professionals, and the concerned public some guidance as to how they might approach some areas of fraud prevention. But why should anyone think that fraud is an important area for crime prevention activity? After all, in 1986, recorded frauds constituted only 3.7 per cent of all offences, and those found guilty of, or cautioned for fraud and financial forgery, comprise 'only' 6.6 per cent of property offenders. Consequently, in terms of routine police work, fraud is comparatively unimportant. Yet when we look at the costs of crime, a different light is thrown on the issue. Recorded crime statistics for 1986 show the following:

**Table 1.1: The costs of crimes, England and Wales, 1986**

| Type of crime                | Cost of crime |
|------------------------------|---------------|
| Burglary in dwelling         | £257,000,000  |
| Burglary other than dwelling | £180,000,000  |
| Robbery                      | £30,000,000   |
| Theft                        | £882,000,000  |

Source: *Criminal statistics*, England and Wales, 1986.

By contrast, the amounts involved in fraud dealt with by Fraud Squads in England and Wales totalled £2,163 million in 1985, and the amount dealt with by the Metropolitan Police part of the Metropolitan and City of London Police Fraud Squad was £1,545 million in 1986. In short, Fraud Squad-recorded fraud — which itself excludes the

**Table 1.2: The costs of crime, Metropolitan Police District, 1986**

| Type of crime      | Cost of crime |
|--------------------|---------------|
| Burglary           | £157,000,000  |
| Robbery            | £16,000,000   |
| Theft and Handling | £407,000,000  |

Source: *Report of the Commissioner of the Police for the Metropolis, 1986.*

many smaller frauds dealt with by divisional CID and the vast frauds handled by the Department of Trade and Industry and the revenue departments — costs victims twice as much (or, in London, three times as much) as the combined total for theft, burglary, and robbery. It also excludes frauds handled by trading standards department of local authorities, and it is not my aim here to discuss' frauds in which goods are sub-standard. Rather, I will focus upon cases where people's goods, services, or money are 'ripped off' altogether.

It is important to realise that particularly where *individuals* suffer loss, the economic impact of £x fraud may be greater than £x burglary, because insurance against fraud is much less common than insurance against other domestic or commercial crimes. (Though collective insurance schemes may give compensation if people are defrauded by a firm advertising in a newspaper covered by the Mail Order Protection Scheme, a solicitor, an ABTA-bonded travel agent, or someone authorised to deal in investments under the Financial Services Act 1986, *provided that the person actually is a member of the insured body.* In the unlikely event of a bank going bust, depositors would be entitled to 75 per cent of their deposits up to a maximum of £20,000. Building Society savers are guaranteed 90 per cent of their funds up to £20,000.)

Another way of looking at the significance of fraud is to examine the costs of crime against business and public sector organisations (excluding legitimate business costs arising from the payment of claims by insurance companies).

**Table 1.3: Costs of crimes against business and organisations, 1986**

| Type of crime                    | Costs of crime |
|----------------------------------|----------------|
| Burglary other than dwelling (1) | £180,000,000   |
| Robbery (2)                      | £30,000,000    |
| Theft by employee                | £15,000,000    |
| Theft from mail                  | £300,000       |
| Theft from shops                 | £12,000,000    |
| Total                            | £237,300,000   |

**Note:** 1. A small percentage of this figure in cash terms, comes from losses from private outhouses and sheds.

2. It is estimated that no more than ½ of the £30m. robbery figure concerns businesses.

3. Source: *Criminal Statistics, England and Wales, 1986.*

This £237.3 million is a rather small proportion of the losses arising out of frauds, particularly when we bear in mind that

- (1) unlike these other crimes for economic gain, there are many serious frauds that are never detected as such by the victims; and
- (2) many serious frauds that are detected go unreported to the police or to other, governmental, agencies.

This indicates that despite (or partly because of) the concentration of private policing resources upon physical security, a potentially greater economic saving may be made by preventing fraud than by preventing other forms of crime against business.

#### Research on Fraud for the Home Office Crime Prevention Unit

A questionnaire survey of experiences of and attitudes to fraud among senior executives in 56 large corporations sampled from the Financial Times Index of quoted companies was funded by the Home Office and the international accountancy firm, Arthur Young, in 1986. A further 16 executives were interviewed. No attempt was made to collect systematic data on unreported fraud, and executives who were not interviewed were only asked for details about those frauds that they *had* reported. Even this revealed a high level of victimisation, as Tables 2.1 and 2.2 show.

**Table 2.1: Reported Fraud (other than Cheque and Credit Card)**

| Size of Fraud     | No. of times reported (% companies) |               |            |           |
|-------------------|-------------------------------------|---------------|------------|-----------|
|                   | never                               | once or twice | 3-10 times | >10 times |
| Less than £1,000  | 47.5                                | 15.0          | 10.0       | 27.5      |
| £1,000 to £4,999  | 47.5                                | 22.5          | 12.5       | 17.5      |
| £5,000 to £50,000 | 36.6                                | 36.6          | 19.5       | 7.3       |
| >£50,000          | 61.5                                | 25.6          | 7.7        | 5.1       |

**Table 2.2: Reported Cheque and Credit Card Fraud**

| Size of Fraud     | No. of times reported (% companies) |               |            |           |
|-------------------|-------------------------------------|---------------|------------|-----------|
|                   | never                               | once or twice | 3-10 times | >10 times |
| Less than £1,000  | 70.2                                | 10.6          | 6.4        | 12.8      |
| £1,000 to £4,999  | 75.6                                | 9.8           | 2.4        | 7.3       |
| £5,000 to £50,000 | 82.1                                | 10.3          | 2.6        | 5.1       |
| >£50,000          | 94.3                                | 5.7           | 0.0        | 0.0       |

The results of the survey show reporting in the expected direction. Fewer companies had reported cheque and credit card fraud than other frauds, and the average value of the cheque and credit card frauds was lower. The larger the sum involved, the smaller the proportion of companies who have reported frauds. (Despite the 'dark figure', it is unlikely that this *ratio* of large to small frauds would alter dramatically). On the other hand, it is interesting that almost 40 per cent of the companies had

*reported* at least one fraud costing over £50,000: one in 20 of them had reported more than 10 such frauds within the past decade. It should be borne in mind, however, that these were all large companies, and that this level of reported fraud is unlikely to be true of the smaller business sectors.

When asked the nature of the fraud that they had reported most recently, the largest single category was cheque/credit card fraud (23.8%), followed by embezzlement/expenses frauds (19%). Internal frauds of various kinds were popular. These were concentrated around customer accounts and goods received, with false invoicing being the most common method, sometimes in collusion with suppliers. Both money and goods were taken, often by “teeming and lading” – shuffling various accounts around — or simply not putting transactions through the books. After that, forgery of a bank paying in stamp, insurance (obtaining premiums for non-existent cover), hire purchase, commodities, investment (by a trustee of a fraudulent unit trust), liquidation, and computer fraud (against payments to pensioners) were mentioned by one of two people each. The sums ranged from less than £100 to over £100,000. The most common was the £10-50,000 range (35% of those reporting). Next came the £5-10,000 range (20% reporting); and a surprising 17.5% in the £100,000 plus range. The average sum involved was £89,537, and the median sum was £15,000. One fraud involved £2 million, which boosted the average figure. However, the median sum is quite high, particularly when compared with other crime figures: see, more generally, Levi (1987) ch.2.

What was the relationship between victim and offender? In almost three quarters of the cases (73.8%) reported, the offender was an employee. This is interesting because given the tendency towards informal disposal of employees who commit offences, the ‘true’ proportion of ‘insiders’ may be expected to be higher. (On the other hand, this is slightly counterbalanced by the fact that insiders may be easier to detect, so there is more point in reporting the fraud, and by the value of prosecuting the employee in providing a corporate defence against a charge of unfair dismissal).

What position did the ‘insiders’ occupy within the organisation? The most common was manager (29%). This was followed by accounts official (19.4%): salesperson/shopfloor operative (12.9%); director/partner (9.7%): distributor/driver (6.5%): and computer operative (3.2%): and 7 others, including cashiers, pensions administrators, and catering officers.

How were the frauds discovered? None of the frauds were detected by external auditors, though many were discovered by routine internal audits, the devising of which may have been at the external auditors’ behest. There was no consistent pattern in how the frauds came to light. The few frauds detected which involved directors or partners were detected because of (a) routine internal checks; (b) information from an ex-employee; and (c) when investors claimed interest and principal and the money was not there. The less senior management and accounting frauds were often discovered as a result of (a) routine checks of stock imbalances, or (b) chance queries from customers or from DHSS or Inland Revenue which prompted internal

investigations. In some cases, discovery of the fraud was delayed by the failure of employees to report on variances in accordance with laid down procedures.

#### Towards a strategy of coping with fraud

Looking more generally at fraud, what sort of frauds occur, and how might they be prevented? In thinking about these questions, it is important (a) to focus upon who the victims of different frauds are likely to be, and (b) to distinguish between the number of frauds and the cost of frauds. Individuals — not necessarily wealthy ones — are more likely than businesses to be the victims of investment frauds in securities and of mail-order frauds; businesses are the prime victims of credit and computer fraud. In terms of *numbers* of offences, there is no doubt that the most common are frauds involving the misuse of plastic money. Precisely because we are moving towards a 'cashless society', cheque and credit cards are the valued produce from many muggings and break-ins, both for their own exploitability and for their value as identification in obtaining credit from stores. (Consequently, fraud prevention may have a 'knock-on' effect in making these other crimes less desirable: see Burrows, (1988). However, 'plastic fraud' totals some £50 million annually, which is a small proportion of the overall cost of fraud.

Financial services victims — banks, building societies, and insurance companies — account for over 60 per cent of the costs of frauds recorded by Fraud Squads, so they are clearly one important area to start in fraud prevention work. But *anyone* who has money or is able to borrow it is capable of being victimised by fraud: since the spread of share ownership, more than one in five adults own shares, and if we add to these, people who have an interest in investments via life assurance, personal pension schemes, and mortgages, the majority of the population are susceptible to being defrauded directly or indirectly. Only *some* of these victims are in a position to take evasive action. Savers and investors can put pressure on the people they entrust with their money to take greater care of it: but they cannot *dictate* the fraud prevention strategies of their management. Although the potential targets for fraud prevention are very numerous, the numbers at risk from any particular *form* of fraud may be much smaller.

Fraudsters operate by manipulating our trust to their own ends, so the primary prevention task is to

create among all potential victims an awareness of the risk and the undesirability of being defrauded.

In the case of investment and mail order frauds, the target population is people as a whole. In the case of company frauds, prevention ideas must reach individuals at *all* levels of organisations. The reference to *all* levels here is deliberate: it must be

appreciated that although the credit manager or the head of security in a large company may be concerned about fraud, the managing director may be more concerned about corporate image and sales, so if organisational policy is to be changed, it is the *senior* managerial personnel who have to be convinced about the desirability of or necessity for this.

## Methods of Fraud

I will distinguish broadly frauds against individuals — some of whom may be businesspeople — from frauds against business. However, this line is not always clear-cut: if someone steals a credit card and misuses it before it is reported stolen, then the individual to whom the credit card was issued may be required to pay for the losses, whereas once reported stolen, the victim will be the credit card company. Public-sector organisations are included here under the category of ‘business’, but the prevention of tax and social security fraud is outside the remit of this paper. The following is a brief account of some of the ways in which fraud victims can be parted from their goods or money.

### (a) *Frauds against individuals*

Apart from ‘consumer frauds’ involving false weights and measures, from the greengroceries to second-hand cars, the major frauds relevant here are investment frauds. These come in an almost infinite variety of forms, but the underlying principle of most such schemes is that they are too good to be true. Some promise a high ‘guaranteed’ rate of return on your investment that is disproportionate to other available safe investments: for instance, one ought to be suspicious of advertisements that offer a 20 per cent return on investments in the purchase of containers, when building society interest on a similar amount is only 7 per cent. Others — particularly before the 1987 stock market crash sensitised investors to the downside risks of investment in shares — give ‘selected individuals’ (from a previous ‘sucker list’?) the chance-of-a-lifetime to get in on the ground floor or a wonderful share whose rise has already been phenomenal but whose product/new mineral discovery is going to put the price through the roof. The offers — from timeshares through shares to containers — are often supported by impressive statistics on price growth, some of which may even be true, but these may be the products of manipulation by those doing the selling. Some such schemes for selling investments e.g. cold calling — telephoning you or calling in person without an express invitation from you — are prohibited under the Financial Services Act 1986 even if they are not part of an overall fraudulent scheme. But they are very popular, particularly when operated from overseas and surrounded by gobbledygook about ‘tax efficient havens’ free from Revenue surveillance. The perpetrators — particularly those who operate from abroad — may expect to net a considerable amount before they are closed down. Timesharing has become a popular venue for fraudulent operators, who pocket deposits without building homes, or do not provide adequate legal title to the land on which the homes are built.

At the 'lower end' of the market, there are fraudulent schemes which exploit the desperation of the unemployed and the poor, by pyramid selling or by promising to find them jobs abroad or accommodation in exchange for an initial investment or administration fee. As a proportion of the wealth of those defrauded, these crimes are very serious in their impact, and the victims may be easier to dupe.

Other frauds of which individuals may become victims include 'charity frauds', where the charities either are wholly fictitious or are genuine but pay almost all their intake to the organisers as 'administrative expenses'. There are a multitude of smaller frauds in which individuals falsely pose as collectors for genuine charities, or 'roofing frauds' where 'builders' use the inaccessibility of the part of the home to get householders to pay large sums for work that is not done, some or all of which may have been unnecessary to begin with.

(b) *Frauds against businesses*

I will discuss here the principal sorts of frauds against business, excluding those (such as Automated Teller Machine frauds) that are well known to their small number of victims. It is common for modern discussions of fraud to be dominated by 'computer fraud'. Certainly, since money transfers and both the invoicing of and payment for goods and services occur mainly via computers, it is foolish to neglect them, not least because computers may contain vital records of transactions and thus provide an 'audit trail' of when the computer was used and for what purpose. They may be used also as a 'front' to give the appearance of commercial sophistication. Most so-called 'computer frauds' involve not breaking into computer systems from the outside but manipulation of input data by employees, whether Electronic Data Processing (EDP) staff or not. How do unauthorised persons obtain access to computer files? Many companies do not change the access password issued by the supplier — which tend to be standard and well known to computer enthusiasts — or their operatives write the password 'somewhere convenient' in case they forget it! In either case, it is not difficult for unauthorised persons to access payments files and change instructions. However, hi-tech frauds that involve hacking or electronic wizardry play a small role in the general picture of fraud, so it is more meaningful to treat the computer as an aid to fraud than as essential to it.

(b1) *External Frauds*. Frauds originating from outside the business involve primarily the abuse of credit facilities. The long-firm fraud, in which a company is set up or taken over with the intention of obtaining large quantities of goods on credit and reselling them without paying suppliers, is a familiar part of the criminal scene. The business is built up, paying for initial orders fairly promptly, until the credit rating is well enough established to justify a substantial expansion of credit. Then, having disposed of the goods, the principals disappear or arrange a fire or burglary — real or fictitious — to cover their tracks. This is sometimes organised in connection with insurance fraud. Other credit frauds include the forgery or misrepresentation of documentation such as shipping bills of lading, invoices for goods sent but not yet paid, mortgage application forms, etc. The banks or building societies or credit factors

(who loan money on the basis of expected income) then pay out against the false documents. The use of forged documentation — including share certificates — as collateral for loans has been increasing substantially. So too has been the use of false surveys and lawyers' reports to overvalue property for loans and/or to strengthen the apparent assets of companies: sometimes, this is never detected, because the money is put to profitable use; sometimes, the investment is unprofitable and its false collateral is discovered; and sometimes the money is simply stolen. The latter happens particularly when a solicitor takes out or assists others in taking out several mortgages on the same property at the same time. Such frauds have in the past been facilitated by the unwillingness of the potential lenders to co-ordinate.

(b2) *Internal Fraud*. This can vary from the fraudulent conversion of cheques stolen from the company mail to the electronic transfer, by a person authorised to make legitimate transfers, of millions of pounds to a personal nominee account in an overseas bank. Fictitious suppliers may be created by accounts staff to justify payments to what are in fact their own nominee accounts; staff may pocket cash payments and destroy both the delivery notes and records of the order held on the computer. Expenses frauds may be perpetrated by employees claiming for fictitious visits or overclaiming expenses; accounts personnel may also generate bogus expenses which they pay to nominees. They may also steal from the business by telling customers who come into pay for goods to leave the payee section blank because they have got the business stamp!

(b3) *Collusive Fraud*. Many frauds involve collusion between employees or officers of an organisation and persons outside. Financial services firms such as banks may lend money to businesses owned directly or indirectly by a director or person with authority to make loans, which intend not to repay or obtain loans under unduly favourable conditions. Firms may buy overpriced property from, or sell underpriced assets to, companies connected with their directors. Purchasing officers may agree to overpriced contracts in exchange for kickbacks in cash or other services. Employees of suppliers can grant discounts to customers in exchange for kickbacks and falsify documentation in support of this. Agents or employees can arrange for real or fictitious intermediaries to be overpaid or to be paid commissions for non-existent services.

## **Preventing Fraud**

The successful fraudster must accomplish three objectives: to obtain the tools of fraud, to use them to get goods or monetary instruments, and to convert them into disposable income. (This is not the place to discuss his or her fourth objective — to avoid conviction). The sorts of tools a fraudster needs may depend on whether he (which includes, for present purposes, 'she') is an insider or an outsider. For some *external* frauds, the only 'tool' the fraudster needs is his tongue: Billy Bunter 'borrowing' food or money by telling fellow pupils that his postal order was due the following day; itinerant 'roofing contractors' telling elderly persons that their roofs were in bad repair

and then falsifying the amount of work they have done on them. The modern-day equivalent of a tongue or signature — a computer password — may have to be obtained in order to effect some fraudulent transactions, particularly the electronic transfer of funds. In other cases the would-be fraudster may need a smart office, hi-technology office equipment, and expensive notepaper, perhaps with a false (or genuine) claim on it that he is a member of a professional body and is authorised to sell investments. For others still, he may need to forge documents such as bills of lading or share certificates or deeds to a home. Except for the poor who require an expensive 'front' for their particular scheme, the obtaining of the means of fraud is seldom difficult in itself: much office equipment can be obtained on credit. The main barrier may be knowledge of how to conduct the fraud and the motivation to do so and risk the consequences. For *internal* frauds, the fraudster normally possesses both the tools and the opportunity to commit fraud, except where he requires computer authorisation beyond his status, in which case he may either recruit others or seek illicit access.

*So how can fraud be prevented?* This paper starts from the premise that we are very unlikely to be able to eliminate any type of fraud altogether, but what we can do is to reduce the risk of being defrauded by increasing our 'fraud consciousness' and taking certain practical steps. These measures can be taken both by people/companies who have never been defrauded and by those who *have* been victimised but wish to avoid this happening to them again. It is not uncommon for victims to find themselves on a 'sucker list' or firms that are 'easy credit touches' to be circulated free or for a price among groups of long firm or securities fraudsters. So although there are no hard data on the risks for individual victims and very little systematic information on the risks for corporate victims either, it is plausible that if no lessons are learned from past experiences, the risk of becoming a multiple victim is a genuine one.

The following may act as a useful framework for interpreting and evaluating fraud prevention aims, for measures that may be effective in preventing some sorts of fraud may not be at all effective with others. Fraudsters may be divided into three groups:

(1) *Pre-planned fraudsters*, who start out with the initial intention of defrauding and devise some scheme — whether it be setting up a phony financial or trading business, or obtaining a particular position with a company — with that fraudulent aim;

(2) *Intermediate planned fraudsters*, who start out with honest aims but who, for whatever motive — bad company, resentment, or a penchant for expenditure in excess of income — later devise a fraud; and (3) *Slippery-slope fraudsters*, who never consciously intend fraud but trade recklessly, continuing to incur debts long after they have become insolvent. I will look first of all at some steps that individuals can take to reduce the chances of being defrauded, and then examine what businesses can do about fraud.

### *Preventing frauds on individuals*

Many investment frauds succeed to convincing members of the public that they have an opportunity to get in on the ground floor of a sure-fire winner and that if they do *not* invest, they will bitterly regret their over-cautiousness. They exert considerable psychological pressure to achieve this goal. Rationally, and after the event, participation in such schemes often seems absurd, and victims feel humiliated by their gullibility. For example mathematically, any chain letter or pyramid selling scheme will have exhausted the entire UK population within six months, so the simple rule is *don't subscribe*. The first step towards protecting against investment fraud is:

*If an investment seems too good to be true, it probably is. Always ask yourself why, if it is such a certain winner, the borrower needs your capital at rates higher than he could get from a bank. Never subscribe to a 'make your fortune' or timeshare scheme on the spot. Always take it to someone independent and if they are sceptical, heed their advice. Many people are defrauded because they turn a deaf ear to reasoned arguments that would put an end to their dream.*

The fraudster plays (i) on your dreams about what you will do with the 'investment profits' he is offering, and (ii) on the annoyance that we all feel when we have not taken an opportunity that turns out well for others. The reality is that the only person who will profit from his investment is himself but you do not know that. Ask yourself why you have been selected for a 'special deal' and, even if the deal is not a complete rip-off, watch out for commission charges, particularly in the commodities market.

Another method that fraudsters use — particularly since the Financial Services Act 1986 has tightened up the conditions under which investment business can be conducted lawfully — is to build up an aura of respectability by claiming impressive qualifications or membership of a professional body that is approved by the government and/or that has a compensation scheme. Such false claims are often a criminal offence in themselves, irrespective of proof of fraud, but this will not worry the fraudster very much, since he hopes not to be around if victims ever get around to complaining to the police or self-regulatory organisation. So the second major preventative measure is

*Check that the qualification or membership of approved body is genuine. For example, if your broker claims that he is a member of FIMBRA, a body that authorises people to sell investments, ring them or write to verify the claim. If he is not a member, you will not get a penny compensation from them.*

Be particularly wary of offers that come from overseas, because if you are defrauded — totally or partially — you are unlikely to be able to use any United Kingdom courts for civil restitution or criminal conviction, and it is very expensive and troublesome to do so abroad. The third preventative measure is

Avoid any deal that has to be completed on the spot. Fraudsters work by suspending your disbelief. If you are offered an opportunity to invest overseas particularly in property, consult an appropriately experienced lawyer.

### *Preventing fraud on business*

The aim of crime prevention is to keep the criminal out. Normally, this is conceived of in terms of steering columns, locks, and bolts: better physical protection. However, in the case of fraud, a different set of preventative methods must be employed. There are *some* physical measures that are relevant — access controls to reduce the risk of illicit entry to computers or computer areas — but the major threat comes from people with whom the defrauded party has a contractual relationship of some kind. In this sense, fraud prevention is closer to family violence prevention than to burglary prevention: the danger is already within but what we need to do is to take avoiding action and change the nature of the relationship.

#### i. Entry control

The first line of defence against fraud is entry control, which may be applied both to people we employ and to people with whom we do business. For *internal* frauds, entry controls may take the form of vetting employees or members of professional associations to ensure that they are “fit and proper persons”. Except for a limited number of special jobs, criminal convictions cannot lawfully be divulged to employers in the private sector. However, the absence of criminal convictions is by no means a guarantee of probity. In the past, the low rate of reporting and prosecution of fraud meant that fraudsters were unlikely to be convicted: many people suspected of dishonesty are allowed simply to resign rather than being prosecuted. The first prevention step is to identify the areas of your business which might be vulnerable to fraud and ask yourself how much you know about the backgrounds of the people who work for or with you. Did you ask for a reference, and did you verify whether what was written actually came from a disinterested party or even from the candidate himself? The first fraud prevention measure is to

*carry out a risk audit on posts in your organisation which might give people access to fraudulent opportunities and/or to confidential data that might be used for industrial espionage, and take up references on all employees in those posts, including more than just one previous job. This would apply not only to the financial director but also to temporary secretaries.*

Many companies might regard this as unrealistic: it is inconvenient and it is unlikely that any given person will commit fraud. This trust (or laziness) may appear to be justified by experience: there are few areas of crime prevention where, if defensive measures are not taken, victimisation is *certain*. However, if one’s judgement turns out to be incorrect and the person is practising his profession as a confidence trickster, the financial damage can be very severe.

One way in which the government has tried to protect businesspeople from internal and external fraud is by banning from taking part in management of a business certain people who have shown themselves to be unfit to do so. In addition to the traditional ban on bankrupts engaging in trade, under the Company Directors Disqualification Act 1986, the court may forbid a person from acting as a director on conviction for an indictable offence 'in connection with the promotion, formation, management, or liquidation of a company'; where someone is persistently in default in filing returns with the registrar of companies; where it appears that a person is guilty of fraudulent trading or breach of duty to the company; and where his conduct as a director makes him 'unfit'. This is an attempt to deal with 'phoenix companies' and 'long-firm frauds', where rogues manage a series of companies that are run fraudulently. It is also an attempt to stop people who are honest but incompetent from trading at the expense of their creditors. However, although copies of disqualified persons may be obtained from the Department of Trade and Industry, there is nothing to stop such persons trading under a false name, even though they commit an offence by doing so and can be prosecuted for this even if there is no evidence of fraud. So disqualification provisions give only limited protection, and given the rate of conviction and sentences in fraud cases, you cannot rely on imprisonment to keep many fraudsters out of circulation for long. In short, it is hard to prevent people with a record of prior dishonesty from doing business with you.

So overall, how effective would entry controls be in preventing fraud? The survey of major companies carried out in 1986 in collaboration with accountants Arthur Young and the Police Foundation found that three-quarters of frauds reported by companies to the authorities were committed by employees. The quarter who were outsiders are not immune from prevention by entry control: for example, references can be obtained from trade protection societies. The 'background checking' measures discussed above may assist in weeding out *some* fraudsters, and psychological tests can give guidance as to who is a devious and 'unsound' character. However, firms may actually *want* to employ devious, unorthodox 'go-getters' as creative entrepreneurs, particularly in a competitive market. Moreover, there is one major problem with the principle of 'entry control', which is that to place one's trust in 'good character' assumes that the major threat comes from those who are known to have "done it before" and neglects the influence of more immediate situational factors, whether they be of a fast lifestyle or merely a sense that one is not prospering as much as one deserves. Many of the most scandalous affairs in the 1980s have been generated by persons of impeccable social background and no previous record of dishonesty: this was why they were able to do such large frauds. So although it is personally uncomfortable,

*always distrust and test your own judgement that "x is a solid chap". He or she may have been once, but people change.*

## ii. Post-entry controls

If we cannot rely on entry controls to prevent fraud, we must focus upon the second-line of defence: internal management systems and compliance monitoring (for internal

frauds), and creditworthiness checking (for external ones). Here, organisational tone is important. It is impossible to state whether there is any 'displacement effect' whereby intending fraudsters choose to work for organisations that have a lax reputation, but 'sucker lists' are passed around by *external* fraudsters, and this may be true of internal ones too. Some companies interviewed in 1986 took a general deterrent line on both fraud prevention and firm post-discovery action. Indeed, the latter may be as important as the former, because if frauds are not readily preventable without causing significant commercial dislocation, deterrence may be achieved by increasing potential fraudsters' perceptions of risk.

Perceptions of risk do depend not only on whether people think they will be caught (and punished in some form) but also on whether they are aware that they are breaking the law. Some newly appointed directors may not realise that they have special legal obligations such as avoiding wrongful trading.

*One fraud prevention measure, therefore, might be a programme of better education of company directors as to their responsibilities under the Companies Acts.*

More generally, fraud prevention measures might involve educating colleagues and internal security to watch out for and enquire into the circumstances of employees who are living in a style far in excess of their salaries. Several defrauded firms had allowed employees on modest salaries to go on driving new Porsches and taking expensive holidays without conducting any enquiry or a more than superficial one into how they could afford this. Where the 'high liver' is a member of senior management, however, (as many Department of Trade Inspectors' Reports have noted), there are serious difficulties in knowing to whom one should report. Here, non-executive directors can play a vital role as impartial insiders.

Clear rules on own-account dealing by employees of financial institutions are vital. The mere existence of clear rules tells us nothing about whether they are followed. The use of nominee shareholdings — preferably in companies controlled from Panama, Luxembourg, or the Netherlands Antilles — and suspense accounts, from which one can load profitable deals into one's own account and unprofitable ones into the trust's accounts, are examples of activities which are difficult to monitor successfully unless the individual is very greedy or unless there is some reason why the Stock Exchange mounts a special investigation, e.g. insider dealing suspicions.

*But consistent sacking and reporting for prosecution where individual — at whatever level — are caught dealing in breach of rules are essential if discipline is to be maintained.*

One American-based transnational interviewed had a code of ethics which is expressed strongly and is applied vigorously. This company sends letters annually to suppliers drawing their attention to the code of business ethics and in particular to the requirements not to make gifts or take other actions towards employees which would

contravene this. All senior employees have to sign an annual representation to say that they are not aware of and have not during the year contravened the code of business ethics.

*To prevent the simple theft of cheques in the company post and their conversion into cash ensure that cheques are drawn in favour of names that are difficult to represent as being personal names.*

Ideally, this should be combined with fraud prevention methods aimed at getting building societies to make it more difficult to open accounts. Some are willing to open accounts where the only means of identification is the cheque itself and/or a letter addressed to the prospective account-holder (that could have been self-addressed!) This makes stolen cheques easy to launder. Building societies themselves are sometimes victims, if someone pays a large cheque to open up a new account, and they allow the customer to use an automated teller machine account before the cheque is cleared.

Much more difficult to prevent are frauds that involve collusion, and they can occur in any area of business. The people in the cashier's department (perhaps in league with computer assistants) who pay phony invoices against goods that have not been received. The people in the purchasing department (or, perhaps, more senior than that) who get a rake-off from the supplier. The manager who extends loans or credit terms to doubtful enterprises in which he has a covert interest. The main prevention method is to require standard devices like double signing of cheques, counter-signing of records of cheques, and careful controls over purchasing and contracting in public and private sectors, with *prompt* checks to verify claims about how the money was spent. However, where there is collusion, (and where, equally importantly, friendships and/or pressure of work make it troublesome to report violations, particularly where management does not see this as a high priority), the checks do not operate, and this increases the length of time that the fraud can continue undetected.

*To reduce risk of collusion in accounts departments, change the counter-signatories fairly regularly.*

Relations in the workplace are very important. Not only fraud but also damage to vital installations can occur as a result of employee dissatisfaction. People of quite low status and pay are often entrusted with crucial posts and if they develop a resentment against what they consider to be their correct status, the results can be dangerous, even if they only take the form of employee walk-out. In this sense, ego massage and managers who listen to the problems lower down the scale are important to crime prevention as well as to general industrial relations. As the computing film, *Time Bomb* — made in collaboration with Arthur Young — reveals, it is also important to ensure that staff who are dismissed are unable to indulge in acts of sabotage, industrial espionage, or fraud before they leave.

*Dismissed employees should not be admitted to places which contain sensitive data.*

Finally, better information-sharing strategies *between* organisations, e.g. building societies and banks, may be necessary to prevent credit frauds such as multiple mortgages on one property.

#### *The prevention of computer fraud*

Much — perhaps too much — has been made about the dramatic crime transformations made possible by the advent of computers. Certainly, they make possible the accessing of confidential information by young whizz-kids and by groups of enthusiast hackers as well as industrial spies. However, the known costs of computer fraud are low relative to other forms of fraud, and despite the obsession — fuelled by films like *War Games* — with access to computer systems by unauthorised personnel, most known computer frauds are committed by insiders, just as all traditional accounting frauds have been committed by insiders. There are, however, some new aspects to computer usage that are relevant to computer crime, particularly because unlike the classic portrait of the fraudster failing to set fire to his records because it is raining and his firewood is too damp, without good back up, computer records can be easily, quickly, and permanently destroyed *by pre-coded devices that do not require the physical presence of an offender (who may be under arrest)*, and because copies of documents are indistinguishable from originals. Moreover, auditors who are not computer literate may not be aware of the change in the nature of the validity of the records upon which they are relying. In general, whenever a former task with separate responsibilities has disappeared, computerisation will lead to greater fraud risks. One of the problems, for example, is the creation of fictitious customer accounts which are paid out although no goods are received (or even ordered). By checking new accounts against credit references received, the risk can be reduced. High frequency small transactions are more preventable than large, one-off frauds.

There are three types of control that reduce the risk of fraud:

- (1) physical controls (such as locks and guards);
- (2) administrative controls (procedures laid down by management); and
- (3) technical controls (such as passwords).

Often, as the Audit Commission Report (1985) demonstrates, password protections are useless not so much because of hi-tech wizards but because people carelessly leave them written up by the side of their machines to make life easier! As studies of the unofficial organisation of work suggest, subversive routines are commonplace in most jobs, and the more that security measures intrude upon 'operational' performance, the more likely rule-violation is.

The great majority of *reported* computer frauds (about three quarters) involve the fraudulent manipulation of input, and these support the view that the absence of basic controls — Good Housekeeping — is the key issue. In Britain and America, few perpetrators use sophisticated techniques; the inadequate segregation of duties provides the most opportunities for frauds (at least by volume if not by average sum defrauded); most frauds are committed by computer ‘users’ and occur in the input area; and (in the past) about a third are detected by chance rather than by any significant audit techniques.

As regard computer frauds, there are some fairly simple rules that could cut down the usually rather simple frauds:

1. Cryptographic transmission of data.
2. Adequate password controls for different levels. Here the spread of micros can be a danger point, and it is vital to restrict authorisation to some files, particularly the programme itself. (This may also be important to control industrial espionage). It is recommended that passwords be changed regularly and be done cryptographically. (Levi should not be my password!)
3. Error lockout, so that the terminal is closed down after successive failures to login (i.e. like bankcards).
4. Automatic shutoff after a while if operator fails to log out.
5. A user-call back mechanism, so that a phone call is made to the terminal site to verify the user’s identity before permitting login.
6. Perhaps even a personal information questionnaire for users, which would require them to supply data that only they would know.
7. Access control over any specialist printers, such as those used for producing cheques or magnetic stripes. Otherwise, fraudsters can literally write their own cheques.
8. Separation of duties so that, for example, no one individual can authorise payments without receipts.
9. For the transfer of large sums, more than one computer signature should be required.

The difficulty is often to ensure that these rules are followed, particularly at a time of scarce supply of computer operatives. Again, this focusses upon the role of good management in reducing the risk of fraud by creating an environment in which Standard Operating Procedures are willingly observed.

## Reporting fraud

In the case of business victims, all surveys show that the primary responsibility for preventing fraud lies with management, not with auditors or the police: fewer than 1 in 10 executives in the Home Office survey disagreed with this. But let us assume now that you have not prevented a fraud and that you have decided to report it as a crime. To whom should you report? There is some overlap in the roles of different agencies, but if it involved an *authorised* investment business, report it to the relevant Self-Regulatory Organisation; if it is a consumer fraud, report it to the local council trading standards department; other cases should be reported to the police. Remember that the police do receive many complaints that turn out not to be crimes, and that their job is primarily to prepare a case that is capable of leading to a criminal prosecution. Your case to any official agency is more likely to be dealt with quickly and effectively if you have first sat down and prepared a timetable of events and amounts; a statement of what you were told initially — verbally or in writing — to induce you to lend money or supply goods; and what happened subsequently. Preferably, this should be supported by documentary evidence such as contract notes or letters. The police may find your complaint easier to deal with if you attend in person at the Fraud Squad offices, though you may find that the matter is referred to the divisional CID if it is not a particularly complex case. But you must not assume that because you have been ‘ripped off’, a crime has been committed. The criminal law is an imperfect mechanism for controlling business malpractice. If ‘your’ offender is convicted, recent legislation on the confiscation of assets of offenders may increase your chances of getting your money back, but your best bet is to avoid being ‘caught’ in the first place.

## Conclusion

What emerges globally from fraud research are three sorts of fraud control measures:

- i. employing reliable staff (with adequate references and fidelity insurance);
- ii. good systems, regularly monitored by internal auditors and supervisors;  
and
- iii. company policy of dismissal and prosecution for fraud, backed up by a much more substantial police presence and expertise.

We will not be able to eliminate fraud entirely. As with all crime problems, it is a question of making them manageable. Changes to make it harder for senior officials to dominate a company and override controls — such as firm auditors who are free to report fraud to regulators, and the presence on the Board of strong non-executive directors — will reduce the risk of fraud. So too will measures to prevent people with bad reputations from selling investments and from setting up new businesses. Fraud prevention, like other forms of crime prevention, is an attitude of mind. Our social learning about crime tends to generate and sustain the view that crime is committed by ‘other people’, by strangers rather than intimates. We would do well to bear in mind the words of a fraudster I interviewed who, when asked what the code of the fraud sector of the Underworld was, answered: “Do your friends first; they’re easier”.

## References

**Audit Commission** (1985). *Computer Fraud Survey*. London: HMSO.

**Burrows, J.** (1988). *Retail Crime: prevention through crime analysis*. London: Home Office.

**Levi, M.** (1987). *Regulating Fraud: White-Collar Crime and the Criminal Process*. London: Tavistock/Routledge.

## Crime Prevention Unit Papers

1. **Reducing Burglary: a study of chemists' shops.**  
Gloria Laycock. 1985. v + 7 pp. (0 86353 154 8).
2. **Reducing Crime: developing the role of crime prevention panels.**  
Lorna J. F. Smith and Gloria Laycock. 1985. v + 14 pp. (0 86252 189 0).
3. **Property Marking: a deterrent to domestic burglary?**  
Gloria Laycock. 1985. v + 25 pp. (0 86252 193 9).
4. **Designing for Car Security: towards a crime free car.**  
Dean Southall and Paul Ekblom. 1985. v + 25 pp. (0 86252 222 6).
5. **The Prevention of Shop Theft: an approach through crime analysis.**  
Paul Ekblom. 1986. v + 19 pp. (0 86252 237 4).
6. **Prepayment Coin Meters: a target for burglary.**  
Nigel Hill. 1986. v + 15 pp. (0 86252 245 5).
7. **Crime in Hospitals: diagnosis and prevention.**  
Lorna J. F. Smith. 1987. v + 25 pp. (0 86252 267 6).
8. **Preventing Juvenile Crime: the Staffordshire Experience.**  
Kevin Heal and Gloria Laycock. 1987. v + 29 pp. (0 86252 297 8).
9. **Preventing Robberies at Sub-Post Offices: an evaluation of a security initiative.** Paul Ekblom. 1987. v + 34 pp. (0 86252 300 1).
10. **Getting the Best Out of Crime Analysis.**  
Paul Ekblom. 1988. v + 38 pp. (0 86252 307 8).
11. **Retail Crime: Prevention through Crime Analysis.**  
John Burrows. 1988. v + 30pp (0 86252 313 3).
12. **Neighbourhood Watch in England and Wales: a locational analysis.**  
Sohail Husain. 1988. v + 63pp (0 86252 314 1).
13. **The Kirkholt Burglary Prevention Project, Rochdale.** David Forrester, Mike Chatterton and Ken Pease with the assistance of Robin Brown. 1988. v + 34pp (0 86252 333 8).
14. **The Prevention of Robbery at Building Society Branches.** Claire Austin. 1988. v + 18pp (0 86252 337 0).
15. **Crime and Racial Harassment in Asian-run Small Shops: the scope for prevention.** Paul Ekblom and Frances Simon with the assistance of Sneh Birdi. 1988. v + 54pp (0 86252 348 6).
16. **Crime and Nuisance in the Shopping Centre: a case study in crime prevention.** Susan Phillips and Raymond Cochrane. 1988. v+ 32pp (0 86252 358 3).