THE PREVENTION OF CHEQUE AND CREDIT CARD FRAUD

Michael Levi, Paul Bissell and Tony Richardson

CRIME PREVENTION UNIT PAPER NO. 26
LONDON: HOME OFFICE

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

First Published 1991

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 633 7

Foreword

The problem of cheque and credit card fraud has increased in magnitude. Since 1988, British losses from these types of fraud have almost doubled. As a consequence, in 1990, total fraud losses were running at £150 million.

This report explains how these losses are incurred, and evaluates the effectiveness of existing security measures. What is of most significance is the collaborative work of banks, building societies and credit card issuers to reduce their escalating losses. To add to this welcome development, this report offers a range of additional suggestions by which both the institutions and the police could maintain their effort in the long-term control of fraud.

I M BURNS
Deputy Under Secretary of State
Home Office, Police Department
June 1991

Acknowledgements

Many people and organisations have helped us in this project. In the business sphere we are grateful to senior fraud specialists from all the major card issuers and merchant acquirers; to Club 24; Ian Robson and Darrell Barnes of De La Rue; Dixons Stores Group; Cyril Garton of Bemrose Security Cards; GE Capital RFS; Alan Hilton and other officers of the Credit Industry Fraud Avoidance System; Mike Hoare of the Post Office Investigations Department; John Hulbert of Cogitaire; Jonathan Killin and Frank Hickman of Touche Ross; Marks & Spencers plc; John McCullough of Sears Financial Services; Colin Stanbridge of Cardcast; and Sue Thornhill of the Committee of London and Scottish Bankers. Particular thanks are due to Barclaycard (especially Chris Kay, John Nickson, and Wayne Henry); to Robert Littas of Visa International; and to Jim Parsons of APACS. In the world of commerce, time is money and we appreciate the considerable time that the above (and many other financial services, staff, inventors, and consultants not named here) have spent on explaining things to us and on answering our requests for information.

In the policing sphere, we are particularly grateful to the City of London Police Cheque Squad (especially D.I. Roy Stevens); to the Gloucestershire Constabulary (especially D.Supt. Malcolm Hart); to the Metropolitan Police International and Organised Crime Branch (especially former D.Supt. David Sowter); and to the West Midlands Cheque Squad (especially D.I. Guy Johnson, D.C. Ian Nicholls, and Jacky Horner). We also appreciate the assistance of D.C.I. Mike Culverhouse of the Merseyside Cheque Squad.

On the Home Office side, we thank Mary Barker and Gloria Laycock for their continual support and encouragement in what has proved to be a much more complex task than it appeared when we were originally commissioned to carry out this study. We also received assistance from a number of commercial organisations and fraudsters who prefer not to be thanked publicly. We hope that our efforts in this report will repay – at least in part – the time all those parties gave to us.

Michael Levi
Paul Bissell
Tony Richardson
June 1991

Contents

List of Tables

Introduction

The Objectives of This Study

In this modest exploratory study of an area of crime previously unresearched in the UK (and - to our surprise - almost totally unresearched elsewhere in the world), our objectives have been

— **to develop a better understanding of the extent and *modus operandi* of cheque fraud, cheque card fraud, and credit card fraud;**

— **to examine how business and public policing have developed in relation to them,**

— **to analyse which methods seem to hold out most - and, equally importantly, the *least* - promise of dealing successfully with such frauds in the future.**

It is relatively easy to justify prevention initiatives if one regards prevention as an unalloyed good. However, **business** initiatives such as those discussed here have a tangible cost if they involve spending money on hardware, and on computer systems and staff, which has to be balanced against **expected** loss reductions which may not materialise, or may materialise only in the medium or long term, while the business has to borrow the money from the short term. Even initiatives which involve the time of existing staff but no marginal cost of employing others have a high opportunity cost in the economic climate of British industry and commerce today. For business, unless pressure is brought to bear by government and/or by policing agencies who withdraw their co-operation from the arrest and prosecution process – whose **economic** benefits to business are not self-evident - a 'business case' has to be made out which offers direct economic benefits as well as general social betterment. We are acutely aware that if – as in pollution control – the 'externalities' of costs to the public were taken into account, the costing of crime prevention in **every** sphere would take a different form. However, we live in the real world and in this study, we have taken seriously these financial imperatives and have sought to develop 'best practice' guidance within the framework of what is economically viable as well as what is socially desirable.

The development of payment cards: a brief history

'Plastic' cards have come a long way since 1965, when the National Provincial Bank introduced the first cheque guarantee card (for £20 cash from their branches). In 1966, the Barclaycard was introduced, followed by Access in 1972. The most recent addition – in 1988 – has been the debit card. It functions in a very similar way to a credit card in that it can be offered for payment at any store displaying a sign accepting the card. The customer signs a till printed voucher detailing the card number and the amount of the transaction, and signs the voucher. The customer retains the top copy of the voucher, the cashier examines the signature and the

transaction is completed. The customer's current account is then debited for that amount usually within three working days - the same as for a cheque. Visa debit cards such as Barclays Connect and the Lloyds and TSB payment cards are accepted at **all** Visa outlets worldwide. The Switch debit cards were slow to take off because of the limited number of retail outlets taking them, but are now accepted at over 20,000 outlets. The advantages of debit cards are that they are quicker and more convenient than a cheque payment; customers can in some outlets withdraw cash over the transaction amount, and they serve as a limited banking service, enabling customers (including fraudsters!) to avoid going to the bank. The result of these developments is that per capita, the United Kingdom is now the world's largest user of plastic cards. Under the auspices of giant rival networks, their use and application has spread across all continents.

Both credit and debit card stores have floor limits set - after negotiation – by the 'merchant acquirers' (mainly the large banks). Below those limits, no authorisation for transactions is required; above it, authorisation by means discussed in this paper takes place. Basically, what the authorisation process does is to inform the retailer – by phone or by other electronic means - whether the customer can use the card for that transaction, It therefore deals with customer overspending as well as with fraud. Some of these authorisations take place by checking against 'negative files' of cards 'blocked' by the issuer; others - more expensively - take place 'on-line' so that the information involved in the authorisation process is completely up-to-date. New Electronic Point-of-Sale (EPOS) terminals can check - with or without the knowledge of people working in the store - every **nth** transaction **below** the normal floor limits, to guard against fraud by customers and/or staff. Such terminals can also check all banded transactions, so that some or all transactions, say, between £40 and £50, are automatically checked 'on-line', whether in all stores or in particular locations viewed as vulnerable to fraud. Many shoppers would be surprised at the amount of electronics involved in their activities.

The cost of 'plastic' and cheque fraud

How costly is cheque and credit card fraud, and how has this been changing? Let us put this in context. In 1990, there were 32.5 million **credit** cards issued by banks and building societies; 36 million **cheque** cards issued by banks and building societies; approximately 11 million scorecards (of which approximately 6 million are Marks & Spencers); and 1.5 million charge cards. By volume of transactions, there were 700 million credit and charge card transactions and 75 million retailer card transactions, i.e. over 2 million transactions per day. Worldwide, UK-issued credit cards can be offered for payment at 8.4 million merchant outlets.

Since 1988, the total cost of fraud against the major retail banks has increased 97 per cent, while that of plastic fraud has increased 126 per cent, the principal rises being in Visa/Mastercard fraud and in Cheque Card fraud. Barclaycard alone has experienced a growth in fraud losses from £2.6 million in 1980 to £25 million in 1990.

The losses are set out below.

Table 1

Fraud Losses (£m),Major Retail Banks, 1988-1990

	1988	1989	1990
Cheque card fraud	19.9	18.8	34.3
Eurocheque card fraud	1.9	2.5	2.6
Cashpoint	1.5	2.3	2.3
Visa/MasterCard	24.2	32.9	68.1
Non-plastic fraud	21.7	23.2	29.5
Debit cards	N.A.	N.A.	13.5
Total	**69.3**	**79.7**	**150.3 million**

In addition to these costs, there are losses to building societies, to finance houses who manage Scorecards (such as Dixons, Debenhams, House of Fraser, and Marks & Spencer); to merchant acquirers in relation to fraudulent telemarketing - the purchase (or apparent purchase) of goods by phone using credit card numbers that do not belong to the actual purchasers; and to merchants in respect of unguaranteed cheques or sums in excess of the guarantee limits. There are also unquantified but plausibly very substantial losses accruing to private individuals and businesses whose outgoing and incoming cheques are stolen and converted into cash without the banking negligence that would enable them in law to reclaim the loss from the bank. The figures for **credit** card fraud are conservative: they exclude the category of 'credit write-offs', where issuers terminate an account which has been misconducted and where debt recovery is deemed impossible; and **potential** credit write-offs which are not yet treated as irredeemable, thereby enabling them to be treated as assets in the accounts rather than as bad debts. Such 'bad debts' would not be reported up the line to the fraud department and therefore would not enter the fraud figures, though they are relevant in assessment of the economic benefits to the company of fraud prevention measures. It is almost pure guesstimation what percentage of such write-offs and future write-offs actually represent fraud - for instance the (in fact intentional) slow building up of a legitimate credit rating for a later boosting of rating which is exploited by the fraudster who does not, in the end, pay his bill - but it seems plausible to us that the total would be many millions of pounds.

It is instructive to compare these costs - few of which have entered the recorded crime statistics either as stolen cards or criminal deceptions/attempted deceptions - with the costs of other crimes. During 1989 – the most recent year for which data are available – thefts from the person cost £22.2 million and robbery, £31.4 million; thefts from vehicles, £138.4 million; **recorded** theft from shops, £16.2 million;

burglary other than in a dwelling, £218.6 million; and burglary in a dwelling, £271.8 million. (Cost of fraud figures are not collected by the Home Office or most individual forces, but earlier analysis – Levi, 1988 – enables us to deduce that 'plastic' is only a small proportion of the cost of fraud dealt with by the London or provincial police forces.)

If unrecorded crimes are taken into account to provide a comparable database the total figure for non-bank crimes will be greater, though the British Crime Surveys note that most high value crimes **are** recorded. However, the Home Office figures above are **gross** losses, and take into account ('stolen' cards excepted) neither the modest recoveries, which **are** published, nor the insurance paid to victims. (See Hough and Mayhew, 1985; Home Office 1988.) In financial terms, therefore, it is plausible that the **net** costs to **victims** of reported and unreported non-bank crimes would be no higher than the above figures. By contrast, the bank (and other financial institutions) losses are uninsured, and our informants stated that little is recovered from offenders. Much of the general anti-fraud insurance takes the form of fidelity bonding against employee fraud, though insurance is available - and is taken up by some large store chains - against bad cheques, and some organisations, such as Transax, guarantee to pay all bad cheques in exchange for fees on authorisation calls. (During 1990, Transax guaranteed over 5 million cheques involving over £500 million in this way, for an average cost to retailers of 1 per cent of the value of each transaction.) Although they do not cost separately the reported and unreported fraud, credit card issuers informed us that to maximise the cost-effectiveness of police time - and not alienate the police by flooding them with uninvestigateable cases - they report only cases that they judge to be most likely to yield a conviction, and these amount to between ten and twenty per cent of the frauds that they experience.

These are the **aggregate** statistics. How do these costs vary when we break down the patterns further? It may be helpful here to set out the costs of lost or stolen Barclaycards from a random sample of 200 taken in January 1991, discussed in more detail later. For the 200 lost and stolen cards, an average loss per card of £294 was sustained, totalling £58,800. 43 per cent of the cards were **not** subsequently used fraudulently: the actual loss per fraudulently used card was £513.

Average loss by **method** of theft shows some interesting variations. The average loss sustained where the card was obtained during a household burglary was £615. Where the card was reported stolen from the person, the average loss was calculated to be £474. Where the card was stolen from an unattended motor vehicle the average loss was £378. Where the card had been **lost** rather than stolen, the average loss sustained was £421. Again, these are probably underestimates, since not all of these cards will have been recovered and – though unlikely - fraud may take place subsequent to our survey. Patterns of fraudulent use reveal that after initial use within the first day of theft, **some** fraudsters wait months until they expect the card has been removed from the 'hot file', and then re-use it. But as well as requiring more discipline than is generally found among **street** offenders, this involves risk

in retaining stolen property for a long period. Attempting to **explain** the wide variations in average fraud losses is probably unwise due to the small number in our sample of losers. It is at least conceivable that the variation in the loss figures (when looked at by offence type) have as much to do with the relative audacity of the fraudster who subsequently used the cards as with the offence type itself.

The increased total fraud losses are not entirely the result of the boom in credit cards issued or turnover. True, there has been a general increase in credit cards in the UK, from 16.9 million in 1984 to 24.9 million in 1988 to 32.5 million (including building society cards) in 1990. However, we may see that while credit cards **issued** rose only **30 per cent** between 1988 and 1990, **fraud losses** rose by **99 per cent.** Police and banking sources suggest that there has been a definite growth in organised criminal interest in 'plastic' and cheque fraud, and – though there is little evidence that narcotics **traffickers** finance their drugs purchases by credit card fraud - there are local networks in which stolen cards and cheque books are exchanged for drugs.

The Costs of Crime Working Group (1988) observed (p.19) that **"action against fraud is dictated more by the proportion of turnover than by the absolute sums involved, particularly where turnover (and thus profit) might be reduced by taking necessary crime prevention measures".** In the **credit card** business, the ratio of fraud to turnover had declined from an average of roughly 0.27 per cent in 1980 to 0.13 per cent in 1987, and appeared to have stabilised at that rate. The credit card companies broadly thought that they had cracked the problem of fraud as it materially affected their business, and were willing to put up with that level of losses in order to maintain the sales and marketing dynamic. During 1990, however, many major credit card (including storecard) issuers found that the ratio had doubled again, to approaching 0.25 percent and rising. (One storecard had by far the lowest ratio, the result of a combination of the non-acceptance of out-house credit cards and technological measures of in-store validation before first card use which are not cheaply or readily available to many organisations.) Moreover, since credit card profitability declined, the effect of these fraud losses on operating profits - 'the bottom line' - was correspondingly greater, particularly where the banks themselves were suffering much reduced profits or even losses on their general business. Currently, by contrast with the situation that prevailed at the time of the Monopolies and Mergers Commission Report (MMC) in 1988, no major issuers are making significant profits from credit card business and this has an effect on their **perceptions** of the seriousness of the fraud problem and on what they are prepared to do about it.

Britain's problems are far from unique: there is a global trend towards increased fraud losses and rising fraud as a percentage of sales. MasterCard's worldwide fraud losses rose from $128.7 million in 1988 to $240.8 million in 1990, to which Britain contributed 18 per cent; Visa's losses in the same period rose from $189 million to

$355 million. Credit card sales almost doubled over the same period, but fraud (not counting credit write-offs) as a percentage of sales rose from 0.095 per cent to 0.1 per cent for MasterCard and from 0.09 per cent to 0.11 per cent for Visa. There are considerable geographical variations within this figure. Germany, which in 1989 had a comparatively small credit card user population of 3.4 million due to (subsequently declining) cultural resistance has fraud losses of 0.8 per cent of turnover: over three times the UK figure. Although MasterCard data show that in 1990, compared with 1989, the percentage **increase** of fraud was seventeen times greater in Italy than in Britain, MasterCard data show that **total** fraud losses in the UK were more than eight times greater than those in Italy. These national differences are partly a function of differential credit card ownership rates: in Italy, there were approximately 4.4 million cards in circulation in 1989, compared with 18.7 million (of which 4 million incorporate smart card technology) in France; 3.4 million in Germany; and 32.3 million in the UK.

But abstract opportunity is plainly not a **sufficient** explanation for crime. Criminal organisation and levels of (subjective) criminal 'need' are part of the equation, as are aspects of the legal system: in Italy, until pending legislation is passed, it is virtually impossible to prosecute for credit card fraud. The organisation of fraud is briefly examined elsewhere in this study, but it is relevant here because of its effect on legitimate commerce. Largely as a result of 'offers they cannot refuse' to Southern Italian merchants by Mafiosi who 'induced' them to process the vouchers from stolen and counterfeit cards – 1 to 2 per cent of Italian cards in circulation are stolen each year - *Banca d'America e d'Italia* alone cancelled Visa merchant contracts with 4,000 merchants in the Campania region and 3,000 in Sicily during 1990. Indeed, some 40,000 Italian merchants have been 'terminated' (as credit card acceptors!) during 1990-91. Unless one takes the view that the availability of credit facilities is socially harmful, this undoubtedly has a very negative effect in reducing the credit shopping facilities of Southern Italians, as well as reducing tourist expenditure in those areas where tourists are brave enough to venture!

Another aspect of the cost of 'plastic' and cheque fraud is its effect on the level of 'primary' crime such as thefts from the person and burglary. It would take a far more elaborate study than this to determine how many crimes would not have occurred without the lure of substantial income for the thief and robber as well as for the fraudster (who normally is a different person). However, the black market prices in London suggest that **to the thief,** cheques with a guarantee card are worth £3-10 per cheque; credit cards are worth up to £150; and charge cards up to £200. Debit cards are worth more to the thief than the cheque guarantee cards that they are replacing, because they are not limited in usage by the number of cheques in the book, and because they circumvent the ideal crime prevention practice of keeping cheque book and card separately (which many see as impractical anyway). This benefit to the primary thief is the equivalent of a much larger crime where goods are taken and have to be resold; the benefits to the fraudster are correspondingly greater, for s/he will obtain an average of £600 for a card for which

s/he has paid £50-150. One alleged fraudster has obtained some £128,100 through using stolen cheques and £100 guarantee cards in 24 police areas, obtaining roughly £1,000 per cheque book stolen. One bank informed us – on the assumption that 10 cheques per book were used – that its average loss was £370 on £50 limit cards; £594 on £100 limit cards; and £777 on £250 limit cards. Although the **proportion** of the theoretical maximum obtained falls for larger card limits (from 82 per cent to 37 per cent), there is a clear positive relationship between guarantee limits and fraud losses. The availability of rewards such as these means that for those with the requisite contacts, cheque and credit card fraud are highly profitable compared with rewards for many other types of crime. This is so particularly when the modest downside risks – conviction and imprisonment – are taken into account.

The risk of fraud

In short, in terms both of absolute losses and of ratios of loss to turnover and profit, 'plastic' fraud is a growth industry in crime. One bank informed us that of all **cheque** cards issued, 1 in 416 of the £50 limit cards were used fraudulently **(excluding** mere account misuse by holders); 1 in 273 of the £100 cards were used fraudulently and 1 in 1,028 of the £250 cards were used fraudulently.

By what means does this rise come about? The methods by which cards come to be fraudulently used are from false applications, theft in transit, misuse by genuine cardholders, and the recycling of lost or stolen cards through criminal markets (or by primary offenders). There are also developing important methods of 'plastic' fraud whose impact falls not so much upon the card issuers, from whom the cost data have been calculated, but upon the merchant acquirers, who are not necessarily the card issuers: Midland may handle Barclaycard payments, for example. Such developing frauds include telemarketing and frauds in which merchants evade electronic controls by using manual over-rides on their tills. Burglaries and thefts from vehicles, work, and places of entertainment have undoubtedly increased the level of stolen cards in circulation and these – along with theft of cards in transit and fraudulent applications – constitute the subject matter of this project.

'Active citizenship' has rightly been a major **motif** of the culture of crime prevention, but with some noteworthy exceptions (CBI, 1990), the campaign against crime in business has lacked any organised research base. We have attempted the difficult task of gathering data from a huge variety of organisations, some of which had not previously gathered the kind of information we wanted, and have tried to assemble it into a mosaic of crime analysis and crime prevention strategies. We hope that this has repaid the efforts of all those - particularly those listed in the preface - who have given of their scarce time.

Preventing Counterfeiting

The prevention of counterfeiting depends essentially on making it difficult for fraudsters to deceive **those who exchange goods or money for the payment medium.** This is **not** the same as making it difficult for people to deceive **experts** as to the genuineness of the card or cheque, though if the latter can be fooled as well, this extends the lead time and profitability for the fraudsters. Since the introduction of the cheque encasement card in 1965, a number of measures have been taken to improve the standard of security and the design features built into the card. The main emphasis of these has been on refinements to the signature panel in an attempt to make it tamper proof; the introduction of a standardised hologram bearing the features of William Shakespeare (for cheque guarantee cards only); and increasingly complicated printing types embossed onto the face of the card. An examination of any recently produced cheque guarantee or credit card will reveal the type of fine line, rainbow, and split-dot printing used on the face of the card. These changes have made the cards considerably more difficult to counterfeit or copy. To counterfeit guarantee cards **effectively** - in the sense of being likely to deceive those who looked closely - would necessitate a substantial outlay in printing technology. Patterns of dies fluorescing in ultra violet light have also been built into certain sections of the card, which technically means the cards can be validated under ultra violet lamps, **where these exist at point of sale or exchange.**

In 1984, the hologram of William Shakespeare was phased in as the industry standard for all cheque guarantee cards issued by banks and building societies that were members of the Association of Payment and Clearing Services (APACS). Its principal uses are (i) to provide a standard symbol for till staff to establish whether the card does or does **not** guarantee cheques; and (ii) to prevent fraudsters simply colour photocopying the face and rear of a genuine card and pasting these onto a blank card. Outside the Far East, few holograms have been counterfeited. As an additional security feature, the more recently introduced £100 and £250 cheque guarantee cards have the cheque guarantee limit built into the hologram.

The signature panel

Much attention has focused on the need to improve the durability and security of the signature panel on the reverse of the card. Since this represents the main feature on the card through which point of sale staff can validate a customer's instruction - certainly with cheque guarantee cards and with credit cards accepted under a retail outlet's floor limit – emphasis has been placed on striving to ensure that the signature panel is tamper proof. In the past, fraudsters obtaining credit and cheque guarantee cards had been able simply to 'wash' the signature panel of the card with detergent or other chemical means, thereby removing the original signature, and replacing it with their own. Changes to the design of the signature panel have now made this practice rather more difficult. If any attempt is made to erase or alter the signature using whatever means, the card will be unusable since the words VOID

or INVALID should appear from below. By ensuring that the signature panel is flush with the surface of the card, and adding fine-line printing to either side of the strip, fraudsters have been thwarted from pasting on additional signature strips with altered signatures without incurring the risk of detection. Although these developments mean that **once signed** (which currently excludes those cards stolen prior to customer receipt), the body of the card is reasonably tamper proof in terms of signature alteration, we are aware that fraudsters have adapted to this by merely making greater efforts to copy to an 'adequate' standard of retailer acceptability the existing signature on the panel. Furthermore the substitution of a fresh signature panel is ineffective only if salespeople physically feel the panel to ensure that it is flush with the card: consequently, **cards should not he checked simply by inspection through clear plastic inside a wallet.** Credit cards are not so vulnerable in this respect, since with the exception of telephone sales (which are generating increased fraud problems), they always have to be touched by a salesperson.

The magnetic stripe

In **unattended** situations, the visual aspects of the card do not need to be counterfeited: what needs to be counterfeited is the information encoded on the card. The card manufacturers we spoke to commented that probably one of the most insecure features of present day card design was the magnetic stripe on the reverse of the card holding the encrypted data that allows access to automatic teller machines (ATMs) and enables the card to be read by 'swipe' terminals at the point-of-sale (POS). It has recently become possible to purchase relatively inexpensively a device that is capable of reading the data on the magnetic stripe. Once decoded and read, these data can then be encoded onto a blank card and, as far as can be ascertained, **subject to the additional knowledge of that individual's Personal Identification Number (PIN),** can be used to access the genuine card-holder's account via ATMs. The susceptibility of the magnetic stripe to abuse and its use in unattended ATMs is understandably an area the banks are concerned about. Both Jack (1989) and the consumers magazine Which? (1991), as well as some comments on the draft Code of Banking Practice (1990), have drawn attention to the risk of ATM fraud without customer complicity. Notwithstanding this fact, ATM types of fraud are not increasing at the same rate as other types of fraud, probably because, we are told, the fraudster risks losing the card in the ATM transaction if anything goes wrong and because ATMs normally require knowledge of the PIN, which is sent to customers separately. (Though unless customers are allowed to choose their own PIN - as they are by some issuers – the problem of remembering it, particularly for multiple cards, often leads them to write down the number(s) in places such as wallets and diaries where they can be examined if stolen.) Other fraud *modus operandi* are probably easier to carry out, involve less technical expertise and carry considerably higher financial rewards. (This includes the conversion of stolen cheques, particularly blank institutional ones stolen from building societies, whose validity is seldom questioned.)

What can be done to improve card security? High coercivity – and, *a fortiori,* dual coercivity - magnetic tape is very much more difficult to decode using simple technology, and if magnetic stripe counterfeiting becomes much more prevalent, may have to be introduced. Swedish card manufacturers currently utilise an even more sophisticated type of tape – known as watermark - to encrypt data onto the magnetic stripe. These tamper proof cards have a code imprinted onto them that is sealed during the manufacturing process. However, it is estimated that this would add an extra 12 pence to card production costs - over half the present cost - and would require adaptation of existing ATM and 'swipe' terminals, if this were adopted as standard technology. At present, it would cost £500 to upgrade each ATM, and since there are currently 17,000 of these in use, an approximate outlay of £8.5 million would be needed. The change to watermark tape would also necessitate the adaptation of existing point-of-sale terminals accepting debit cards. At present the terminals cost £1000 each and the additional cost required to upgrade to watermark standard is estimated to be £200. There are currently 20,000 EPOS terminals, so a wholesale upgrade would amount to about £4 million, plus the extra cost of each future EPOS terminal.

Furthermore, there are fears that machine manufacturers might increase the costs of service contracts or refuse to service them. For the change to watermark cards to have any viability, there would have to be not only substantial inter-issuer agreement – otherwise there would be no compatibility with other cards as exists at present – but also service agreements with machine manufacturers.

Smart cards

In essence, the smart card is a payment card in which the magnetic stripe is replaced by a chip containing a memory, itself controlled by a chip processor. The card not only can be validated for authenticity by the terminal: it can itself validate the genuineness of the **terminal,** for the terminal can be a counterfeit, built to record PIN and account number details for later misuse. The card can store data in such away that all payments can be handled for a customer, with set expenditure limits (so that even transactions below floor limits will be rejected once the limit has been reached). In addition, the smart card provides added security in that it cannot be counterfeited, it simplifies administration for banks, and its multiple functions mean fewer cards per customer. Currently, smart cards cost £2-5 each to produce. In France, where the development and promotion of the smart card has outstripped that of other European countries, there are estimated to be well over 4 million smart cards currently in use. Point-of-sale terminals have been redesigned to accept both magnetic stripe and chip and based payment cards. The decision to go ahead with the smart card for future cash, debit and credit card transactions was taken in early 1990 by the national organisation *Groupement des Cartes Bancaires.* This decision means the magnetic stripe card will be progressively phased out, and the dual technology smart card will be introduced as standard. Whether this is strictly cost-effective from a fraud prevention viewpoint is questionable, but centralised

dirigisme (and stimulation of the French electronics industry) has made it happen. One difficulty with smart cards is that there generally has to be some manual fall-back facility in case they should malfunction. This has enabled French criminals simply to stamp on them, opening up relatively uncontrolled manual keying mechanisms.

Biometric techniques

Of the card manufacturers and issuers spoken to, there was a general feeling that **some** biometric solutions to card security (retina and fingerprint recognition) were socially unacceptable in most applications, and were additionally disadvantaged through cost and imperfect performance. On data storage and cost implications alone, it is considered unlikely that any of these verification techniques have a viable future in the mass produced credit card market. Voice recognition, however, is still under review and, though slow, is less intrusive than the above. Dynamic signature verification, based on the unique styles by which we press when writing, is a serious prospect in future years.

Another preventative initiative under consideration by card manufacturers and issuers alike is that of laser-engraved, raised signatures digitally embossed onto the card's signature panel. More economically, this should eliminate attempted alterations to the signature on a common payment authorisation card. This idea is discussed later in the paper.

Cheque production and design

With the increasing availability and use of colour photocopying machines in this country, a primary problem faced by cheque manufacturers has been to build security features into the design of cheques, to prevent people simply presenting photocopied cheques. The steps that have been taken to defeat counterfeiting include the use of ultra violet light on cheques - which does not photocopy - and again more complex designs and fine line printing. Certain colours, notably pastels, are known to be more difficult for photocopying machines to reproduce accurately and these have tended to be adopted by manufacturers. Additionally, all cheques have to be printed on special security paper which allows them to be more easily distinguishable from photocopied cheques. The type of ink used to produce cheques is water soluble and should prevent fraudsters from attempting to erase any of the handwritten information on the cheque. Indeed, one of the professional fraudsters interviewed stated that the tippex-type liquid imported from the US was difficult to apply without discoloration: hence he preferred simply to add a few thousand pounds to the beginning of the sum and the figures on the cheque! It is possible to print a hologram onto the surface of the cheque, which prevents photocopying.

One other initiative designed to prevent the fraudulent use of photocopied cheques was examined. It is known as Copyvoid, and is basically a simple printing process that entirely prevents the subsequent use of photocopied cheques. All cheques produced using the Copyvoid system have the word 'VOID' printed onto them during the production process. This is hidden to the naked eye. However, if the cheque is then photocopied on popular colour copiers, the word 'VOID' appears to render the cheque useless. Although the problem of cheque photocopying is not known to be particularly extensive, this process obviously has applications for cheque manufacturers (and fraud victims) seeking to eliminate it. The cost of this printing technique is known to be equivalent to adding one additional colour to a cheque. As we write, only Midland's First Direct of the banks or building societies utilises this system, but some individual companies do – and, in our view, more **should** - have their cheques printed with these features.

Preventing Fraudulent Card Applications

Apart from general theft and loss of credit cards, one principal method of obtaining credit cards for criminal use is through fraudulent applications. Indeed, the extent of fraudulent credit card applications is so severe that one card issuer reported that up to 30 per cent of new applications in one recent month had been fraudulent. Since losses from fraudulent application cards cost on average substantially more than those on stolen ones, this clearly is a priority area for prevention.

There are a number of different *modus operandi* when completing fraudulent applications, but the principle is usually the same. A fraudster completes an application for a credit card, or store card and either uses a false name, the particulars of another person, a false address, or falsifies his or her own personal details in some way, possibly by creating fictitious employment (or even using a fraudulent company to supply false employment details). One of our criminal informants told us that good counterfeit or stolen full driving licences could be obtained in any name for £50, so at least in **some** areas, the provision of false identification is not a problem. (This may be inhibited when photographs are included on driving licenses.) It has been known for the personal details of deceased persons to be used for fraudulent card applications. Alternatively, fraudsters will find out from cardholders - either by conspiracy or by temporarily redirecting their mail - which cards they **do** have, and will then apply for those cards they **do not** have, arranging for those cards to be sent to a redirected address.

Multiple fraudulent applications are a frequent occurrence which entails the same fraudster applying for a number of credit cards from the same or different issuers using a number of different names and personal details. Sometimes the details vary only in minor respect, but they are sufficient to cause problems for credit reference

agencies in terms of data protection restrictions – currently subject to litigation - which prohibit the refusal of credit on the basis of information which is not specific to that **individual.**

When a completed application is received, it is run through a credit reference agency which will check the validity of that information and scrutinise the electoral roll to ensure that the applicant lives at the address stated. Further checks, such as telephoning the applicant's place of work or home have not, in the past, generally been made. In addition, there has been only a modest degree of data sharing regarding attempted frauds and actual frauds by the competing financial institutions. This problem may have intensified since the breakdown of the Joint Credit Card Company (JCCC) agreement in 1989 which led to an increase of card issuers and merchant acquirers. There is, however, no obstacle to companies co-operating **solely** for security reasons.

In an attempt to amend this situation, a number of initiatives have been embarked upon. The most important of these is CIFAS: the Credit Industry Fraud Avoidance System, conceived by the Consumer Credit Trade Association and soon to include all the major banks and building societies. Membership of CIFAS is open to any credit grantor, leasing or hire company, credit reference agency or other organisation expressing a concern to reduce fraud. CIFAS is a method of preventing fraud by allowing credit grantors to exchange details of fraudsters **if and when they are discovered.** This information is kept by the credit reference agencies, and it is to these companies that credit grantors supply and from them that they obtain information regarding possible frauds. CIFAS thus facilitates the dissemination of information on actual and suspected fraud to all its member credit reference agencies and credit grantors, showing that in this respect, there is no commercial competition in fraud.

The procedures for the exchange of information are simple. Where fraudulent activity has been confirmed by one of the participating credit grantors - in accordance with strictly defined criteria approved by the Data Protection Registrar, for which there is no space here – the case details of that fraud are entered onto a standardised input form. CIFAS members are then required to forward a copy of this to each of the participating credit reference agencies by the fastest possible means. When a search is made against an address and a positive fraud warning is given, to safeguard against an innocent party, the application is not immediately declined. First, a check has to be made to ensure that the details passed to the agency for the purpose of the search correspond accurately with the details on the application form. Then further checks - which for security reasons we will not reveal – are made.

If, following receipt of that information, the member is satisfied that there was no fraud or attempted fraud, normal credit underwriting conditions apply, with the customer's application being accepted or rejected. However if, on receipt of that information from CIFAS, a member is able to identify a known or suspected

fraud, that member should file a further report. Each day the list of new frauds coming into CIFAS are notified to the participating credit reference agencies and all matches are investigated. In this way, multiple applications from suspected fraudsters can quickly be identified and action brought against them.

This exercise in data sharing does appear to be bearing dividends. During 1990, CIFAS identified 6,991 fraudulent applications, of which over 1,000 involved innocent parties whose identities were being 'borrowed' for the purpose, to add credibility y to the application. The **average** value of all fraudulent applications was £1,505. At a cost of some 80,000 to members, CIFAS saved £10.5 million in fraud. During the first quarter of 1991, the net saving to members was over £4.5 million, reflecting the escalating level of application frauds as well as a new category of rejected attempted fraudulent applications with which CIFAS now deals.

Data from one major credit card issuer demonstrate the success of the CIFAS initiative in preventing application fraud. Since this issuer joined CIFAS, 88,000 new applications were checked against the data CIFAS held on potential and actual fraudulent applications. Out of those 88,000 checked, a total of 1,275 applicants who otherwise would have been accepted were refused credit, That issuer's average loss on application fraud is estimated to be approximately £2,600 per case.

Multiplying the average loss by the number of applicants refused credit, a cash saving of £3,315,000 has been realised in just over six months of membership, costing the issuer £350. Though the benefits are uneven and some companies put in much more information than they receive, **data sharing can achieve positive results.**

The process depends, however, on the identification of the application as a fraud, and this sometimes only occurs *ex post facto,* when investigations into major loss have arisen. The issue of card non-receipt is dealt within the next chapter, but it should be noted that systems of identifying suspect **delivery** addresses are salient to the identification of fraudulent **applications.** Both the Post Office Investigation Department - through their 'Canberra' system - and the Plastic Fraud Prevention Forum - through their 'Pinkerton' system - have developed sophisticated databases for addresses which are viewed as liable to theft and fraud. Card issuers (including storecard issuers) will feed their loss data into 'Pinkerton', which in turn will feed this into the 'Canberra' system for the Post Office Investigation Department to analyse loss patterns and investigate theft in the postal system. There is thus a prospect of a co-ordinated approach. The general point here is that the prevention of **continued** offending is as significant as the prevention of the initial offences.

For all the information technology developments, only some of which have been described here, the yield in terms of detection will depend substantially on how many organisations subscribe to the system. It is our opinion that as for other 'criminal intelligence' systems, **there is a risk that a multiplicity of only partially overlapping databases creates confusion and does not maximise the economies of scale that are necessary to combat fraud.**

Preventing Card Theft and Loss

To place credit card fraud in the perspective of general crime for gain, the 1988 British Crime Survey showed that in 1987, one in thirty households were the victim of burglary or theft in a dwelling in which something was stolen; over 1 in 10 households had something stolen from a motor vehicle; and over 1 in 100 **persons** suffered a robbery or theft from t heir person (such as having a handbag snatched). Additionally, though BCS data are not analysed for this purpose, a substantial proportion of people are victims of theft at work. **Recorded** crime figures suggest that the risk of being a victim of these crimes has increased since 1987. Cards and cheques are 'at risk' in all of these incidents and **may** be the specific target of some of them.

Methods of Card Loss in the UK

Data from the 1988 British Crime Survey (Mayhew, personal communication) reveal that of crime incidents in which cheque books and/or credit cards were stolen, the methods of loss were as follows:

Table 2

Methods of Card and Cheque Loss, BCS 1988

theft of personal property (inc. property from handbags, wallets, theft from work)	57%
theft **from** motor vehicles	20%
theft of household property (inc. burglary)	15%
robbery	5%
theft of motor vehicles	3%
Total	**100%**

Detailed data are not available, but even if **all** the handbags, wallets, and briefcases etc. stolen from cars had cheque books and credit cards in them – whether or not these were reported to the interviewers as such - the maximum proportion of 'plastic' and cheques **taken** from vehicles (though not necessarily **used)** would be 40 per cent of those lost.

Unfortunately for us, **police** statistics are not yet kept in any form that would enable us (or them) to deduce how many times plastic cards or cheques were taken during

these crimes, let alone used after them, but we did organise one study in Gloucester during October 1990 which yields some clues, however atypical of the country at large, to the relationship between thefts, burglaries, and robberies and plastic and unguaranteed cheque fraud.

The Gloucester Study

In Gloucester, during October 1990, there were recorded 108 house burglaries; three robberies and thefts from the person; and 327 thefts from motor vehicles. The total 'crime for gain' (excluding taking cars without authority) recorded was 929. Assuming victim reports of what they lost to be complete - a fairly bold assumption - cards or cheques were taken in 1 in 65 thefts from vehicles; 1 in 22 burglaries; and (though there were very few cases) 1 in 2 thefts from the person.

During October, 53 separate incidents of either theft or loss in which cheques, credit cards, cash cards, store cards, or debit cards were taken were reported to the police. In 21 cases, more than one **card** was taken; in 14 of these, cards from more than one financial institution were taken; and in 5 cases, identification documents – mainly driving licence - were also taken. Two fifths of the victims were women. Altogether, following Home Office counting rules and taking cheque books as one item, 100 separate items were stolen or lost. Of these, just under half (47 per cent) were recorded as lost, rather than being the product of crime. However, issues such as pickpocketing or theft from home by intimates make these categories looser than they may appear, and it is plausible that some 'losses' may be thefts. Our interviews with the police and victims suggest that some victims may find it less humiliating - and less time-consuming in terms of filling in police reports - to see their loss as a loss rather than as a theft, particularly where it has been pickpocketed or taken from a bag or where there has been some such offence implying negligence on their part. All they wish to do is to notify the loss to fulfil their obligations to the bank or insurer. In some cases, they may have 'lost' the card in circumstances which might cast some discredit on them in the eyes of a partner and/or the police. In 2 per cent of cases, the method of loss was not known by the reporter.

The majority of cards that were stolen were taken in public places. Thefts of cards or cheques during a household burglary accounted for 9.2 per cent of incidents of theft or loss; theft from the workplace accounted for the same percentage, as did thefts from motor vehicles; theft or loss while the 'victim' was in a supermarket generated 14 per cent of thefts or losses. The majority of **lost** cards were lost in and around a town centre, or in public houses, nightclubs, telephone kiosks or other public places.

However, **as far as the police or victims were aware,** the rate of **usage** of the cards was low. In one case involving theft from a handbag in a nightclub, the Visa card was recovered in a failed attempt, and a Dixon's storecard which was stolen at the same time (but not listed to the police, indicating victims' problems of recalling

to the police what they have lost) was not used. That was the **only** case in which a card was known **by the victim** to have been used. Appreciating that neither victims nor police will be aware of all misuse, we conducted a follow-up study in which the banks co-operated in finding details of whether or not the card actually was used. Without having branch details, some could not be traced, but four major issuers had no misusers; another had only one; and it can reasonably be concluded that whatever its impact elsewhere, the possibility of misusing credit cards was **not** fuelling thefts, burglaries, or robberies in Gloucester.

The Barclaycard study

In order to throw some light onto patterns of credit card theft and loss, a telephone survey of 200 credit card losers was carried out for us by Barclaycard's market research arm. Our objective was to investigate what were the most commonplaces and methods of loss/theft of credit cards; the patterns of reporting of the loss; the attitudes of cardholders towards the credit card companies, to the police and to the offence of 'plastic' fraud itself, and more generally, their reaction towards some of the proposed initiatives designed to reduce credit card fraud. In this section, only the methods of loss will be discussed. It should be remembered that the sample of 200 relates to just over one quarter of Barclaycard's average **daily** card losses, and although they remain the largest credit card issuer, that figure itself indicates the scale of loss and of potential fraud. The survey was carried out in January 1991 and involved customers who had experienced loss or theft of a credit card throughout the months of September, October and November 1990.

The characteristics of postally intercepted credit cards were excluded first, because it is virtually impossible to know in these cases whether the fraud that occurred resulted from the genuine cardholder defrauding the issuing bank (first party fraud), or from someone intercepting the card pre-delivery, and second, because those who **were** genuine victims of postal intercept would not be able to answer a large proportion of the questions concerning the loss and the subsequent reporting of that loss.

Of the 200 strong sample, 16 per cent stated that they had **lost** their card, whilst the remaining **84 per cent** had had their card **stolen.** 15 per cent had experienced loss or theft of their card on more than one occasion. Of those cards that were **stolen,** the most common category was from the person, corresponding to 50 per cent (83) of all cases of card theft. Cards stolen during a household burglary accounted for 17 per cent (28) of all cases. Cards stolen from unattended motor vehicles made up 22 per cent (36) of all cases of theft. These data correspond closely to the unpublished British Crime Survey 1988 data cited earlier this chapter. The car itself was **not** stolen in 89 per cent (31) of the cases in which a **card** was stolen, suggesting that the theft of the card was a purposeful, rather than an incidental, crime for gain. Additional items stolen from the car included a cheque book in 60 per cent (18) of car related thefts, and a car radio (20 per cent (6)). This seems to indicate

that cars are popular places for the theft of credit cards as an item for theft in their own right, supporting the general conclusions of Home Office research and the 1988 British Crime Survey regarding the importance of autocrime prevention.

Where the credit card had been **stolen,** respondents were then asked what they were doing when the card had been stolen. 49 percent (35) had been at work, 11 percent (8) for each of the following had been out for a meal, on public transport, or abroad at the time of theft. In 10 per cent (7) of cases, the respondent had been in a shop when the theft occurred.

Where the credit card had been **lost,** the only categories of any significance were cards lost in a shop - 38 per cent (11) – and cards lost on a trip or excursion, accounting for 38 per cent (11) of cases of loss.

Losers were then asked whether anybody had used or tried to use their stolen or lost card. 75 per cent (150) indicated that someone had tried, whilst 17 per cent (34) said that no attempt had been made to use it. 8 per cent (15) did not know or could not remember. This suggests a fairly high level of awareness of misuse. The ratio of cards fraudulently used to cards lost or stolen was believed by some major issuers to be between 1 in 10 to 1 in 15, but despite our findings in Gloucester and the low rates of usage of lost and stolen **scorecards** (from 1 in 46 to 1 in 10), this ratio seems too low to be true overall: our Barclaycard survey (which excluded non-received cards) showed that half those lost or stolen were used.

In fact, over 80 per cent of all cards stolen during a burglary or from the person had subsequently been used fraudulently. A slightly lower proportion (67 percent) of cards stolen from unattended motor vehicles were subsequently used fraudulently, (These rates are much higher than in Gloucester, suggesting that the rate of usage varies considerably, being higher in large cities with more established underworlds.) Of those cards that were used fraudulently, 66 per cent (99) were utilised to purchase something. Only 23 per cent (35) were used as a facility for obtaining cash in some way.

Our survey revealed that where a credit card was lost or stolen, there was a fairly high likelihood that other payment media would be lost or stolen as well. In over 40 per cent of all cases of lost and stolen credit cards, either a cheque book, cheque guarantee card, other credit card, or personal documentation (such as a driver's licence) went missing. Of these additional payment media stolen or lost, nearly half of these were used fraudulently. It would appear that the initial loss of credit cards has a knock on effect on the fraudulent use of other payment types, not least because they can be used as evidence of identity to open accounts or to get other cards. Only 24 per cent of losers suffered **only** the loss or theft of the credit card.

The general prevention implications to be drawn from these data are that apart from limiting the **number** of cards carried on any one occasion (i.e. thinking about whether one is likely to use **that day** any particular card one has), general risk awareness is the best avenue for card theft protection. To this extent, cheque and

credit card fraud prevention is linked to the general issues of crime prevention such as securing motor vehicles and homes, ensuring that handbags and wallets are not left unattended in the workplace or pubs and clubs, and guarding against bag-snatching and pickpocketing while shopping or in the open. An additional problem relates to card awareness on vacation: over a quarter of some credit card issuers' losses arise from theft abroad, since people are often more casual about watching their belongings on the beach, and in some areas of Spain, for example, general rates of thefts from cars and hotels are very high. We recognise that holiday-makers have a difficult choice between leaving cards on the beach, in the car, or in the hotel: all are vulnerable. However, they can at least spread the risk by not keeping all documentation together.

Research in Rochdale suggests the value of targetting crime prevention efforts on those who have been victims, since the likelihood is that they will be repeat (Forrester et al., 1988). Whilst only 15 percent of our Barclaycard sample had suffered card loss previously, we were interested what effect the experience of having a credit card stolen had on victims' behaviour in terms of the general safety keeping of their credit card. It should be borne in mind that all the sample had at least a two month gap since their card loss and so it is not a **very** short-term reaction, though not a long-term one either. Approximately one third stated they were now more vigilant about the safe keeping of their card. 21 per cent (42) stated it had had no effect on their behaviour. 18 percent (35) stated that they only carried their cards with them when they were sure they were going to use them. 7 percent (14) attempted to keep their cards separate from one another in their wallet or handbag.

The vast majority reported no particular post-loss changes in their general use of the card, nor any change in their attitude towards the police or the credit card companies. This suggests the potential for greater awareness of risk on the part of victims, though ironically, **storecard issuers** told us that shoppers, seeing a bargain they wanted in their stores, sometimes reported their card as lost when in reality, they had left their card at home, thereby inflating their 'lost' figures but allowing the shoppers to obtain the instant credit they wanted!

The Problem of Postal Interception

Card production and distribution to issuers are very secure. However, once the cards are prepared for sending through the postal service, potential fraud risks begin to multiply. The financial loss arising from customer non-receipt varies as a proportion of total fraud losses from 8 per cent to 67 per cent for different issuers: major issuers average at 30 per cent, though this is a dynamic figure reflecting (i) success in other fields of prevention, and (ii) changing methods of customer delivery. The fundamental problem with using the postal service for high value deliveries is that all items are simply treated as first class cargo.

To give some idea of the problem of postal theft and/or interception from multi-accommodation/empty addresses, for the year of 1990, one issuer lost

approximately 12,400 credit cards in the post; another lost 4,380 cards; and a third lost 1,009 cards. It should go without saying that cards lost or stolen in the post are unsigned, and therefore are probably the easiest cards for the fraudster to use and - with the exception of fraudulent applications - carry the heaviest losses sustained on all cards: approximately £1,000 per **general** credit card and ranging from £271 to £800 per **storecard.**

Although it is difficult to express accurately the number of credit cards that go missing every year, the Post Office Canberra database of customer non-receipt of cards estimates that during 1990, some 160,000 cards went missing, not all due to theft: a Post Office survey revealed that 30 per cent did not reach the customer because the address was wrong or inadequate, so there is plainly room for card issuers to keep more accurate records. One of us recently received an Access card in the post for a previous occupant: this could easily have been used fraudulently. Likewise, there are serious problems of insecurity of personal and company mail at the point of receipt, which are exploited by persons who steal cheques as well as 'plastic'.

The methods by which internal fraud can be prevented are in principle known to the Post Office Investigation Department: a specialised police force of over 300 with immense experience. However, there are 165,000 staff nationwide in the letters department alone, a large percentage of whom are seasonally employed on short-term contracts. With the pay and conditions of work offered to staff, they are unable to attract and retain personnel of the integrity they require in all areas of the country, and since some employees deliberately gain employment at post offices with the intention of defrauding, while others become fraudulent *in situ* for reasons discussed elsewhere (Levi, 1981; Mars, 1983), the structural problem of policing a large and complex organisation is considerable. Some 60 per cent of first frauds on unreceived and allegedly unreceived cards take place in the near vicinity of the point of delivery, suggesting that prevention should focus on distribution and on insecure addresses. The main scope seems to be for better tracking-down of mail to those individuals who deal with it: a service that is provided for up to £2 per letter by the special secure Post Office Courier delivery service (and, less reliably and no cheaper at present, by private security firms). The loss data can also help to deal with the problem of thefts after delivery but prior to customer receipt at multi-occupancy dwellings and business addresses. Such tracking makes it far riskier for postal staff to "flog cards at £50 a time for their beer money", in the graphic description of one informant.

The problem for credit card issuers is that unless they can target the areas and even specific addresses most 'at risk' - which is difficult because the fraudsters shift around - the total price of secure delivery of large numbers of cards is much greater than the losses from postal intercepts of relatively small numbers. Although use of the Post Office Courier Service cuts the level of intercepts by thousands of percent, those cards that **are** intercepted are now used much more frequently in the short period after theft, reducing the benefit to the card issuers. The fine-tuning of secure

deliveries has led to a reduction from 45 per cent to 25 per cent in the proportion of Barclaycard's losses that arise from postal intercepts (Burrows, forthcoming). Nevertheless, the more rapid updating of the Post Office database and its linkage with the 'Pinkerton' one currently operated by the Bank of Scotland for the Plastic Fraud Prevention Forum would assist greatly in mail fraud prevention.

The other method of reducing postal intercepts is not to deliver cards by mail but to have the customer collect them, as happens on the Continent, where the banks tend to be open at more user-friendly hours such as some evenings. The traditional card issuer objection to this is that people seldom go to their banks, often work far from where they bank, and that this would be administratively inconvenient to the customer and / or to the bank. (This is particularly so for charge card organisations like American Express and Diner's Club which have very few branches and therefore have to deliver to homes.) Given banking hours, the time when most people would wish to collect their cards is probably lunch time, and this would generate either queues or extra bank (and therefore, ultimately, customer) costs. This objection has some force, and it is costly to write to customers to ask them to nominate a convenient branch for customer collection. Moreover, secure mailing to bank and building society **branches is** very expensive, and raises cost implications for the storing of cards - particularly in building societies whose safes are less secure – and for potential staff fraud, requiring elaborate logging procedures. However, in areas where the mail is insecure, customer collection has increased, and the market to this extent is self-regulating. (In France and Belgium, the customer is required to produce evidence of identification before the card is handed over.)

With this issue in mind, we included questions in our Barclaycard survey. It is of interest that 90 per cent of our sample of Barclaycard losers thought that a bank collect system would reduce fraud. 50 per cent of them would strongly welcome it, whilst a further 34 per cent favoured it; 5 per cent said they would **not** welcome it; and only 2 per cent said that they strongly disliked the idea. The remainder stated that they would not be bothered either way. When asked what problems a bank collect system might incur, 45 per cent thought there would be no problems; 24 per cent said it would be inconvenient; 16 per cent commented on the inaccessibility of a local branch (which could be remedied by allowing them to choose); and 5 per cent mentioned queues. So **at least amongst those who have suffered loss,** who are more likely to be sensitised to the fraud issue, the support for the notion (at least in principle) was not founded on ignorance of practical considerations.

Another possibility for reducing potential losses incurred from non-receipt of credit cards, is to ring or write to customers informing them that their card will arrive within the next few days, and to ask them to contact the issuing bank if the card did not arrive. A number of attempts at using this procedure have already been made by some of the issuers to whom we spoke. Unfortunately, they had

experienced considerable problems due to the fact that, in their opinion, it was not possible to trust the postal service to deliver the cards within the stated period. With a small minority of first class mail taking over two days to reach its destination – particularly, in defence of the Post Office, if it is incorrectly addressed as noted earlier - and the customer reporting the card as not received, the issuing bank then has to block the card to prevent possible fraudulent use only to discover the card turning up several days later. In other cases, it had not been possible to contact the cardholder, prior to the card being released. There then arose the problem of what the next course of action should be - to release the card or not. In cases where the card had been released and the holder was not contactable, should the issuers block the card just in case it might be fraudulently used? On the whole, the attempts to contact cardholders pre-delivery had been deemed a failure.

Other possibilities exist for post-delivery notification. ATM fraud could be reduced or its future growth prevented not only by allowing customers to select their own PINs – making them easier to remember – but also by the universal use of 'return mailers' to the issuing bank to confirm receipt of the cards before they are activated. A field experiment conducted by us involved the senior author receiving a renewed unlimited value travel card and deliberately not sending back the confirmation of receipt slip requested. Two months later, a full fare ticket to New York was purchased by him, without authorisation being queried (e.g. for identification), let alone refused: there exists a flourishing market for airline tickets. It may be that there is a balancing of the need to prevent fraud against the undesirability of upsetting customers for 'upmarket' cards. However, the more general point is that there must be follow-up systems for pre- and post-notification of receipt. Indeed, bearing in mind the delivery problems mentioned above, it might be good customer relations as well as good fraud prevention for card issuers to telephone their customers and ask them to call day or night if they have not received their cards within, say, two days.

The final aspect of fraud prevention in relation to card delivery is that cards can be sent to the customer's home but have to be validated prior to first use by the customer going into the store or bank and having the card run through a machine. This is done in both Marks & Spencer and Abbey National building society. However, apart from the cost of the machines, this is feasible only in relation to 'on-line' terminals where the issuer has control. Traditional 'non-swipe' machines cannot be programmed to reject cards on this basis, though theoretically, the cards could be designed so as to change their features only **after** they had been validated by the issuer, thereby providing some visual cue to ordinary users. **The point of this is that cards will be stolen from the post only if they are of some subsequent use.**

Preventing Merchant Collusive Fraud

On the reasonable assumption that fraudulent applications and the theft and counterfeiting of cards cannot be totally prevented, we now turn to consider how best to stop them being misused once obtained. This involves both technological and human factors of crime prevention, most of which have a cost. We begin with the merchants who accept cards. A large proportion of losses from both cheque and credit card fraud occur within the retail sector. In the normal course of lawful trading, merchants sign up with one of the credit card acquiring networks and agree to pay a proportion of the value of the vouchers accepted to the acquirer, in exchange for the acquirer processing all the information and arranging with the credit card issuer for them to be repaid in advance of the credit card **holder** paying, or even receiving, his or her monthly bill.

A significant - though variable over time - amount of this fraud is known to be the result of dishonest merchants accepting cheques or credit cards known to be stolen. Another method of defrauding credit card companies arises from dishonest merchants embossing blank plastic cards with the account details of genuine cards and imprinting this information onto credit card vouchers, or simply counterfeiting the vouchers. The merchant later claims that someone attempted to defraud him. The card issuer will bear the losses for this activity. One case of merchant collusion reported in The Times (January 11th 1990) revealed that eight businessmen had received over £l.5 million in payments for embossing blank plastic with genuine account information. Such information commonly comes from employees in other merchants - such as staff in expensive overseas hotels or retail outlets - who pass on the information for a ‘cut’.

A particular problem arises where merchant A agrees to allow merchant B to pass credit card vouchers through A’s account. A may agree to this knowing it is for criminal purposes or, innocently, because B has told him that the issuer will not allow him to pass a certain credit limit. A’s account is credited immediately, but when the vouchers reach the account for payment, the credit card has been stolen, or ‘whitecarded’. By then B (and perhaps A, if he is a conspirator) have disappeared, or ceased trading. Not all acquirers have this settlement procedure.

Within the credit card industry, there are relatively simple procedures for tackling merchant collusion. Once the merchant has been identified as engaging in collusive activities, the bank signing up the merchant in the first instance simply has to remove that merchant’s decal from his window and cease processing any vouchers through the payment system. That merchant is effectively struck off the list of approved traders. This also applies to merchants suspected of operating collusively through the use of stolen debit cards.

A less drastic method of dealing with collusive merchants, and one that does not result in the loss of an outlet to the credit card company, is to reduce the floor limit on all transactions to zero. All credit card transactions thus necessitate an

authorisation call to be made to the issuer before any transaction can proceed. This helps to deal with the forms of collusive merchanting involving staff receiving money from fraudsters in exchange for (i) informing them about in-store credit card floor limits, below which no authorisation calls have to be made; and (ii) allowing them to use stolen credit cards without risk of apprehension. One merchant who had managed stores in Central London told us that he was regularly approached by credit card fraudsters for a licence to operate in exchange for split profits. The confidence with which they made these approaches indicates their expected tolerance of their fraudulent activities.

The usual manner of spotting collusive merchants is for all transactions that are later claimed to be fraudulent to be just below the issuer's floor limit for that store. Where a merchant's floor limit is zero, this effectively prohibits the fraudulent use of cards that are known to be lost or stolen. Unfortunately, this still does not afford protection on cards that are lost or stolen but that have not yet been reported to the issuing bank. In these cases, the transaction will proceed and the losses are sustained.

Following the Monopolies and Mergers Report (1988) on Credit Card Services, there has been greater competition between both credit card companies and merchant acquirers. Acquirers have also sought to reduce their costs by limiting the amount of authorisation traffic, which involves staff costs, at British Telecom rates. These changes combine to make collusive trading easier. In this environment, the control of collusive merchants through the lowering of floor limits has been made more difficult, since it is often possible for a merchant to sign up with another acquirer (or threaten to do so) and thereby instigate a rise in the floor limit offered.

The response by the cheque issuing authorities

The process is not so easy where merchants undertake fraud on stolen cheques, since there is no merchant agreement whereby a merchant can be prohibited from trading using that bank's cheque cards. The mechanics of cheque collusion are simple. The merchant agrees to accept stolen cheques, normally up to the limit of the cheque card scheme. The cheques are signed and the cheque card number is written on the reverse of the cheque. No goods are exchanged: the merchant simply takes a share of the value of the cheque which is passed through his till. When investigations are carried out, it is not uncommon to discover that a genuine business does not exist and that most of the transactions carried out by the business involved stolen cheques (and perhaps credit card numbers).

In order to investigate and analyse the extent of merchant collusion, a bank needs simply to input the details onto a standard computer database of the merchant's name; the customer's name; cheque number of stolen cheque; crossing stamp of collecting banker; amount of cheque; date cheque was issued; and handwriting style (where known). At present, only National Westminster Bank, Abbey National, and the Leeds Building Society have the capability of analysing handwriting styles.

Other banks that had the capability have now abandoned it, and the remainder did not invest in the expertise in the first place. To ensure that all banks have details of potential collusive merchants, the reports from all cheque issuing organisations should be merged. This would produce a listing of all retailers who had taken stolen cheques over a particular period, broken down by volume of stolen cheques accepted.

Suggestions have been made for the establishment of a central register of collusive 'cheque fraud' merchants fed by data from all the issuing banks. A specialist handwriting bureau would be required to link criminals with the handwriting styles obtained. There are currently two possible options. One is the establishment of such a unit under the auspices of APACS (or some other industry body); the other is that the unit should operate as a wing of the Post Office Investigation Department. APACS are currently considering the venture and are well placed to proceed with the project with their close links with 51 banks and building societies. However, the pitfalls operating against concerted action in this area are well demonstrated by the rejection by the banks of a proposal in 1987 by the POID to carry out full investigations into collusive merchants for a six month trial period, using NatWest's handwriting facilities and collusive merchants file, the cost being shared out between the participating banks.

Best practice against merchant collusion

The potential for collusive merchanting, as with credit card fraud of all kinds, has been enhanced by the unwillingness of merchant acquirers to act aggressively in controlling their merchants in the environment of greater competition, stimulated by the Monopolies and Mergers Commission. This has meant that if terminated by one acquirer, the merchant has often been able to find another willing to sign them up, in ignorance of the merchant's prior history. The economic stresses of the recession likewise have increased the **temptations** for merchants to collude with fraudsters, and have doubtless made it easier for them to rationalise their involvement as a 'necessary evil' to keep themselves in business or to maintain their standard of living.

With regard to credit card fraud, the appropriate preventative approach to collusive merchants is the development of a **collective** 'terminated merchant' file against which all merchants applying for registration to take credit cards are checked. This is about to come into being as we write. However, though this will be a major improvement, it is not itself sufficient, since the corporate names of merchants can be changed at will, and even the personal names of directors can be falsified to reduce the value of checks on them. (Postcode-based address files are valuable as a supplement here, but fraudsters move around!) There needs to be – and increasingly is - continuous monitoring by merchant acquirers of transaction levels to check that these are plausible for a business of this kind. Otherwise, merchants

who either started out with the intention of defrauding or who later moved down the 'slippery slope' will be able to process large numbers of fraudulent vouchers before they disappear.

Staff collusive fraud

Turning from collusive **firms** to collusive **individuals,** we note that similar economic stresses apply to increase the temptation to 'fiddle'. We have come across cases where a member of staff in a large retail outlet will offer a fraudster 'instant credit' on the basis of the fraudster paying in a cheque known to be fraudulent to both parties. That member of staff then merely has to tick a box on the application form stating that additional identification was offered by the fraudster. The fraudster then purchases the goods under the 'instant credit' scheme and splits a proportion of the proceeds with the staff member. If the retail outlet subsequently makes an investigation into this and discovers a case of staff collusion, some finance companies then charge back the amount to the retailer. Where this practice occurs, there is thus no incentive for retailers to carry out investigations into staff collusion. We are aware that a number of other credit and store card companies take a more enlightened view and do not charge back the amount lost. They compliment the retail outlet for taking the trouble to mount an investigation in the first place. In cases of employee infiltration of this nature, it might well be useful for fraud prone retail outlets to invest in basic systems of crime pattern analysis to assist in the easy identification and investigation of perpetrators.

Preventing Card Misuse

Where the retailer does not want to assist credit card fraudsters, the prevention problem arises in two ways: **'pre-block'** fraud, which occurs before the card is reported lost or stolen; and **'post-block'** fraud, which arises after the loss of the card is reported. Let us deal with post-block fraud first. The general problem of effectively blocking transactions is that most terminals are not 'on-line' in real time. There are some exceptions to this, for example Abbey National terminals discussed earlier. But even where terminals are supposedly 'on-line', they are often loaded up only daily-overnight- rather than continuously. This gives the fraudster some leeway, though as observed earlier, preventing **continued** fraud is more important than preventing solo use fraud. Support for this is given by the breakdown of Barclaycard losses given to us in relation to our sample: the data come from Barclaycard, not from the losers themselves.

Table 3 below shows the (unusually high for the industry) number of fraudulent transactions taking place on cards that were either lost or stolen.

Table 3

Number of Fraudulent Transactions on Barclaycards Lost or Stolen

No. of transactions	% of cases	No. of cases
0	43 %	85
1	11 %	22
2-3	15 %	29
4-5	9 %	17
6-10	6 %	13
11-20	7 %	15
21-50	6 %	12
51 +	3 %	6
Total	**100 %**	**199**

Across the two hundred losers questioned in the survey, **including** those cases where no fraud took place, an average of 6.8 transactions were made on a lost or stolen card. Looking at only those cards that had fraudulent transactions made on them, a higher average of 11.5 transactions per lost or stolen card is calculated. Unfortunately, we are not able to say whether these transactions were made on goods purchased or across the counter at financial institutions.

Patterns of reporting

One of the objectives in reducing the average losses per card is to speed up the process by which the card company discovers the loss and transmits this onwards. (The extent of the 'pre-block' time lapse is one reason why average losses on postal intercepts are so much higher.) We asked Barclaycard respondents a number of questions designed to capture information on at what point they realised that the card had been stolen or lost, and their subsequent patterns of reporting that loss. Over 50 per cent (107) of persons realised their card was missing when they had tried to find it. Only 2 per cent (3) were informed of that loss by the issuing bank. 27 per cent (54) realised the loss after a household burglary they had suffered.

Overall, the majority of respondents realised they had lost their cards within a fairly short period of time. Over 80 per cent realised they had lost their card within a day of its loss. Only 12 per cent subsequently discovered the loss 2 or 3 days later. The vast majority self reported the loss to the issuing bank (98 per cent).

Over 80 percent of respondents reported that loss to the issuing bank within one hour of realising that the card was missing. Only 2 per cent reported the loss the following day, rather than informing the issuers immediately. (However, these results may well be an underestimate, resulting from the fact that – for reasons

of customer confidentiality – Barclaycard was carrying out the survey for us, and customers are theoretically liable for losses from the time of the loss to the time of reporting it.)

Respondents differed slightly when asked what more credit card companies could do to investigate the problems of plastic fraud. Although a quarter did not know and a further one third were adamant that was nothing they could do, a number of respondents came up with a list of preventative measures the credit card companies could initiate. 6 percent stated that a photograph could be put on the card. 12 per cent felt they should be more aware of current forms of identification. 13 per cent felt they should simply offer a better service.

Respondents were questioned on their perceptions about how easy or difficult it was to use fraudulently someone else's credit card. Interestingly, 40 per cent (80) thought it quite easy and a further 40 per cent (80) thought it very easy to use someone else's card. Moreover, a full three quarters contended that it was too easy for people to obtain credit cards. This message was pressed home when respondents were asked whether the ease with which it was possible to obtain credit cards had contributed to the growth of credit card fraud. Again, well over two thirds were adamant that it had contributed to fraud.

Retailer action on cheque card fraud

One multiple retailer indicated that approximately 0.08 per cent of the cheques it accepts annually are subsequently found to be stolen. Some of these transactions lead to conflicts with the issuing banks: where fraudulent cheques are passed using £100 or £250 guarantee cards, some banks are not informing the store that the guarantee was over £50, in the hope that the store will claim only £50 back from them. Several banks have toughened their attitude to reimbursement in cases where the signature on the cheque does not accord very closely with that on the signature strip: their assumption is that the signature strip has not been 'washed' successfully.

In total, this store chain recovered just over one stolen cheque card per outlet in 1990 – a fairly low proportion. This store offers refunds on its goods which affects its popularity among the criminal (as well as the law-abiding) population, since fraudulently obtained goods can be refunded for cash. This company has recently introduced a refund audit due to the fraudulent use of its refund policy. It is now possible to tie customers back to the cheques they have presented. Where the sum is over the limit of the card, this store asks the customer to write their name and address on the back of the cheque - which provides additional forensic evidence for later handwriting examination – and the customer is required to produce supplementary ID. If a driver's licence is offered, staff are requested to check the age on the document since the customer may not correspond to the licence holder.

In terms of the fraudulent use of charge cards offered by the store – or debit cards - all cash tills in each store are logged to an in-store mainframe computer and if these cards are used more than a certain number of times, or above a specified value, a call has to be made to verify that card. So far, only two cards are known to have defeated that test.

Other preventative developments being worked on in that company include competitions to point-of-sale staff offering a £250 prize draw for card capturers. Also, there are plans to develop the capabilities of their 'hot' card files. The file is now updated daily in three stores and the daily update will be extended to another three stores soon.

Some retailers are fairly critical of the information and assistance given to them by banks. For instance, if the retailer questions whether or not an account is sufficiently creditworthy for the sum of the transaction being undertaken the banks refuse to divulge information on the grounds of banker-customer confidentiality. This is despite the fact that the information will benefit the **bankers,** not the store.

Point-of-sale training in cheque card acceptance

Altogether, in 1990, banks lost £25.3 million as the result of fraudulent cheque transactions at retailers, excluding losses to retailers themselves from **unguaranteed** cheques and cheques accepted over the guarantee limit. The whole effort for shop staff to prevent cheque fraud is underpinned by the payment of a reward of £50 for the retention of a card being fraudulently used, though we witnessed some tensions over the way in which stores themselves determined who should receive rewards: some paid till staff; some paid the supervisors; some kept the money for the store; and some did not claim at all. Annually, about 6,000 rewards totalling £300,000 are paid out to shop staff, and this figure is rising. However, with some 600,000 fraudulent cheques being passed each year, there is an immense potential for increasing this reward figure.

Both between different stores in the same chain and between different chains, the variance in card recovery per fraudulent cheque rates is enormous: from approximately 1 in 268 for one large chain to 1 in 24 for another in a similar line of business. The 'worst' chains recovered, respectively, (i) 8 cards, passing 363 cheques per card recovered, and costing the banks a total of £166,404; and (ii) 11 cards, passing 411 cheques per card recovered, and costing banks £261,017. The 'best' chain recovered 365 cards, passing only 2 cheques per card recovered, and cost the banks only £52,164. The average number of fraudulent cheques passed per card recovered was 50 for the retail sector as a whole. The inconsistency almost certainly results from differences in management attitudes which permeate through to their staff. However, there is a risk that the replacement of supermarket store booths which validate card transactions at the point of **entry** by more consumer-

friendly point-of-sale 'swipe' machines will lead to **lower** rates of recovery than at present. This is because staff fear violence from fraudsters and those who have reached their credit limits, both of whom are supposed to have their cards retained.

An initiative in Manchester's Arndale Centre, one of the largest undercover shopping precincts in Europe, was launched in late 1990 by the Association of Payment and Clearing Services (APACS). It aimed to raise the awareness of cashiers and store managers of the extent of cheque fraud, and to assist them in the identification and recognition of potential fraudsters. Over 100 shops took part in the exercise.

The exercise aimed to inform cashiers about the Standard Cheque Card Scheme, emphasising the high security printing employed, the hologram, and the embossed data common to all cards: customer's name; code number; card number; issue number (optional); expiry date; and primary account number (optional). Furthermore, attention was drawn to the information on the reverse of the card, particularly the magnetic stripe and the multi-coloured security printed signature strip. The difference between the £50 and £100 and £250 cheque guarantee cards was also noted. A set of procedures for handling cheque card transactions was outlined, as was a list of potentially suspicious circumstances that might indicate an attempted fraud. These suggestions for identifying and detecting **cheque card** – some of which could equally well be applied to **credit** card – fraud included:-

(i) signatures do not compare
(ii) pre-signed cheques in book
(iii) very slow deliberate signature
(iv) damaged or defaced signature strip
(v) thick felt tip pen signatures
(vi) indiscriminate and hurried purchases
(vii) unusual combination of goods
(viii) person does not match name on card (e.g. oriental name English presenter)
(ix) person does not match title/gender on card
(x) type of goods
(xi) value of goods

The last was mentioned since it is known that (with most guarantee limits being £50) about 90 per cent of frauds in shops are on cheques valued between £40 and £50. This was confirmed by our own survey of retailers. (A similar logic applies to floor authorisation limits on credit cards.)

The training information advised cashiers to communicate with a supervisor where suspicions were aroused regarding the possible fruadulent use of a cheque card and cheque, or to make a telephone call to the 24 hour free enquiry services for suspicious transactions discussed later in this section.

Whilst it is clearly difficult to evaluate the effectiveness of training given to point-of-sale staff, APACS commissioned a market research organisation to carry out some research into the effect their training programme had on staff attitudes and awareness of fraud before and after the initiative. The research into store managers showed very high levels of awareness of fraud and the types of suspicious activities associated with it. The percentage of cashiers aware of the £50 reward rose from 81 per cent pre-study to 97 per cent post-study. The proportion of cashiers stating there was "nothing in the shop on fraud" declined from 48 per cent pre-study to 15 per cent post-study. Over 90 per cent of cashiers stated that the Helpline card giving details of telephone numbers to ring in cases of suspected fraud was quite or very useful. (This has been confirmed to us by other retailers.)

The study of cashier attitudes showed a 20 per cent rise in the number of respondents stating that cheque fraud was a very serious problem: pre-study 49 per cent; post-study 69 per cent. Most cashiers felt fairly confident about being able to spot potential fraudsters, with 78 percent agreeing with the assertion that "if you follow procedures it should be easy to catch them out".

Although the aim to raise awareness on the part of point-of-sale staff of the serious extent of fraud and the methods of spotting potential fraudsters seems a useful starting point for any campaign attempting to promote fraud prevention, there seems to us to be a number of serious limitations to its utility. First, as APACS pointed out themselves, there is a notoriously high rate of turnover of point-of-sale staff. Staff employed at weekends are freqently employed only for weekend work on short term contracts. With such a changing body of staff it is likely that any improvements in fraud preventive knowledge would be dispersed over a relatively short period of time. Such training programme would have to be implemented frequently over the course of one year for them to have any sustainable effect on cashier practices. Furthermore, as our interviews with a variety of sales assistants and managers indicate cashiers are under considerable - though variable – pressures from management to reduce queuing times and increase through-put rates at cash tills. The work itself is repetitive, dull and low paid. The requirements of fraud prevention seem to clash head on with the corporate needs to sustain through-put times.

One of us made a number of purchases in some of the stores participating in the training programme subsequent to it, using a cheque guarantee card containing a signature that due to frequent use, was very hard to discern. Whilst signing the cheque, the researcher attempted to print rather than adopt his usual signature style and to take an unusually long period of time over the signature. On no occasion were card Helplines utilised to check the status of the card. Examination of the two signatures by the point of sale assistant was never more than cursory and no objections were made to the relative difference between the two signatures. On only two occasions, in the same store, were comments made about the limited visibility of the signature on the proferred cheque guarantee card. On these two occasions, the researcher - upon asking what he should do about this - was told it would be all right if he simply re-signed on top of the existing copy.

Although by no means an exhaustive study - only 6 stores were visited at what was considered to be the busiest times of the day and week – it does tend to highlight some of the problems and weaknesses of relying upon the signature as the sole means of authentication of a customer. Throughout the period of our research, we have attempted in our purchases and our discussions with traders to explore this area of relying upon point-of-sale staff to identify potential fraudsters through discriminating between the signature offered and that contained on the reverse of the payment card. In many transactions over a 6 month period where a payment card was used, we deliberately altered our signatures so that they differed from that on our own cards. Several colleagues also told us about occasions when they used their wives' cards, with completely different signatures and even - in one case - where the gender was printed on the card. In numerous transactions, particularly in restaurants, there was little or no attempt by cashiers to observe the signature as it was offered and only a very cursory glance towards the corresponding signature. (British retailers are far **more** conscientious than their counterparts in the United States, France and Spain in examining signatures.) In many retail outlets, it seems to be considered discourteous to take time examining the card and signature.

Some till staff who had **not** participated in the Arndale experiment also mentioned their confusion over which number on some cards should be recorded as the cheque guarantee number. There is no set UK standard to cover the **format** of the multiplicity of cards which guarantee cheques, for multi-function cards differ from the Standard Cheque Card. Some banks also issue cheque guarantee cards without standard magnetic stripes, which makes it difficult for some large retailers to put in proper 'swipe' procedures for cheque transactions. Furthermore, as regards cheque guarantee cards - though not those credit and debit cards which have to be touched in order to be 'swiped' - few staff ever ask for cards to be taken out of clear plastic wallets. Yet it is only by feeling the card that point-of-sale staff can determine whether or not an additional signature strip has been placed on top of the original.

Some store chains do seek to increase fraud awareness, by criticising managers whose stores have low rates of card recoveries per number of fraudulent cheques passed. (This is done particularly, though not exclusively, where those cheques are over the cheque guarantee limit and where part of the loss is charged back to the store by the bank.) Staff awareness can be increased by charging costs to the store manager's 'bottom line', thereby encouraging local responsibility and enhancing the likelihood that s/he will put pressure on till staff to pay more attention to fraud risks. But in a cost-control environment (coupled with low staff morale), staff seldom feel they have sufficient time to lookup at customers despite the prospect of financial rewards for capturing cards.

'Hot' line cheque card schemes

Another scheme aimed at preventing the use of cheque guarantee cards once cards have been reported as missing or stolen to the issuing institutions is currently being

operated by Midland Bank. In essence the 'Check Card' scheme is simple. The 20 card issuers who are now members of this scheme – Barclays, Lloyds, and NatWest have their own individual ones - report the cheque card numbers of all missing or stolen cards to a central data base. If a point-of-sale assistant has his or her suspicions aroused concerning the legitimacy of the individual presenting the cheque guarantee card, that card can be verified against the database of lost or stolen cards by a telephone call. Depending on the result, the transaction will be confirmed or rejected.

Begun initially in 1986, the new phase of this scheme has been operational since March 1990. In the 9 months up to the end of the year, 26,000 calls were received requesting confirmation. For such a scheme to operate at optimal efficiency, all institutions need to be members. However, 12,000 (i.e. almost half) calls related to the cards of non-participant card issuers, taking up expensive staff time at both ends, and blocking the telephone lines. Out of those 14,000 calls for scheme members, 9 per cent (1260) related to cards that were listed as stolen or missing. Estimates of a £500 saving per card have been expressed by the participating banks. In total, a saving of £630,000 has been realised over those 9 months alone. The cost of the system to run (over that period), was estimated to be less than £50,000.

Anecdotal evidence from a number of the larger retailers to whom we spoke indicated that the length of time spent attempting to contact the service was sometimes unacceptable. When the system initially became operational, the average time spent contacting the Hot Line was estimated to be about 17 seconds. Since operations moved out of London to Leicester, one retailer complained of having to wait for over one and a half hours for the service to return their call.

This problem of delayed response is not restricted to the Midland scheme. On visiting one retailer's headquarters, the senior researcher got the retailer to validate use of his own card (from a different issuer). The request for validation took 9 minutes and necessitated 2 phone calls since the first was cut off by the receptionist. In other field experiments with the same card, validation took an average of 5 minutes. Irrespective of the potential time wasted checking valid cards, the inconvenience to a legitimate customer and the probable lengthening of till queues, it is unlikely that fraudsters will be prepared to idle 9 minutes (or even 1 minute) away whilst awaiting a telephone call to confirm the status of their cheque guarantee card: retailers told us that fraudsters (unlike those who had simply exhausted their credit lines) normally "did a runner". First line prevention (and **'card** arrest') will probably succeed, but second line **personal** arrest will almost certainly fail. One chain reported almost no successful arrests, except where store detectives were already suspicious. Another chain reported many violent incidents accompanying such authorisation transactions.

So long as the retailer can convince the issuer that it has complied with the issuer's statutory procedures in processing the cheque and the guarantee card, the retailer will not sustain any loss if the cheque is eventually found to be 'delinquent'. Issuers

are required to reimburse the retailer for the cost of the transaction. Indeed, where investigations are carried out and fraudulently obtained goods recovered, it is common practice to return these items to the retailer from whom they were initially acquired. In these cases, it is in the retailer's economic interest to promote fraud, coupled with the successful investigation of the offence! Although retailers do not pursue such a 'rational' strategy, it helps to underline some of the difficulties associated with harmonising the real clash of economic interests that can occur when the externalities of a particular commercial process are addressed.

In the case of cheque guarantee card fraud, some stores operate a very limited information storage system for 'hot' cards: even 8,000 card files would not hold one week's losses, and some are as low as 1,000 incapacity. One chain loads details twice weekly onto Psion databases through which cheque guarantee cards are 'swiped'. The recovery rate is modest on most of these systems because of the delayed loading of data. The cards contained on the database tend to be 'lukewarm' rather than 'hot'.

We examined a variety of inventions for authenticating the customer at point-of-sale, from fingerprinting cheques and card transactions to the Validity Viewer, an intriguing calculator-sized device which activates a photograph of the card-holder when a PIN is keyed in. Unfortunately, none of these schemes seem to us to be **cost-effective** and several devices have the problem that it may be difficult to distinguish between genuine and false mechanisms, e.g. how does one tell that the keyed-in photograph machine is really the Validity Viewer and not a counterfeit machine? In principle, the most promising initiative is Dynamic Signature Verification, a system of encoding signatures onto 'smart cards' which will process the transaction only if the customer's signature is written in the **identical** way as the cardholder's: trials in progress suggest high reliability for some such schemes.

All in all, relying on point-of-sale staff to use visual signature examination to authenticate a customer's instruction seems to have limited potential for preventing and reducing cheque and credit card fraud. Although some sales staff we interviewed were quite good at spotting 'proactively' whether or not the customer was actually the card-owner - and this is particularly important in preventing **cheque** card fraud – hundreds of interviews by us with sales assistants indicate that much of the success in **credit** card apprehension results from authorisation calls **above** the card floor limit, which enable the staff to spot the fraudster or bad debtor **automatically,** eliminating the human discretion to challenge which is a serious psychological hurdle to fraud prevention. This suggests that **on-line authorisation,** supplemented by **frequent** staff training, is needed to improve substantially the rate of recovery of lost and stolen cards. The trouble is that authorisation in 'real time' is much more expensive, and many stores are moving towards 'bargain basement' portable EPOS terminals which have very modest 'hot' card file capacities: increasingly, fraudsters simply wait until they believe the card number has been removed from the 'hot' card database before seeking to use the card. Apart from doing away with the need for paper transactions, cheap EPOS is a security improvement on traditional machines, but falls short of the optimum.

Cardcast - combatting post block card fraud

Normally, since most transactions are not authorised 'on line' in real time, post-block fraudsters would not be apprehended unless they requested a transaction over and above the retail outlet's floor limit. The Cardcast system has been designed to eliminate all post-block card fraud (including fraudulent transactions involving cheque guarantee cards) by offering a swift and simple on-line card validation service at the point-of-sale. The system offered by Cardcast is basically a 'swipe' unit through which each card is passed when offered for payment, that is connected to a database of all known lost or stolen cards, be they cheque guarantee cards, credit cards, store cards, debit cards or charge cards. This 'swipe' tests the offered card against the file of stolen cards and then generates a response in terms of 1 of 3 coloured lights: a red light signifies that the card is stolen; an amber light requests the sales assistant to pass the card through again; and a green light notifies the sales assistant to proceed with the sale.

At present, most of the issuing banks, credit card and store card companies have only rudimentary mechanisms for forwarding the details of lost or stolen cards to point-of-sale staff, For example one store card company still utilises a hand typed list of stolen cards cellotaped to the side of the cash till that point-of-sale staff are supposed to refer to when presented with a card for payment. In many cases, these lists or 'negative' files are updated fairly irregularly and are cumbersome to use and irregularly referred to.

What Cardcast does is to stand in and act as a central collator of stolen cards as they are informed by the issuing banks that are Cardcast members and transmit this data via the BBC's Datacast system - basically spare capacity on a BBC satellite transmission - to slave units serving the point-of-sale terminals. As yet, Cardcast has installed the system in only 3 sites in the UK, 2 of which are large shopping precincts. It takes approximately 3 minutes to transfer details from the card issuer to the Cardcast database. This technology is useful also for ordinary business purposes, such as communicating price changes.

Current costs for an authorisation call are about £1 and at present 95 per cent of all calls are accepted. The ratio of cards captured (as lost, stolen, or bad debts) to transactions authorised as valid varies between 1 in 992 and 1 in 2,475. Since it is possible to store information on credit limits, floor limits, and bad debtors on the system, it is hoped that all calls could be handled from one source. Additionally, Cardcast is developing a backup system whereby management reports could be produced on a daily or weekly basis to identify what product ranges are being purchased with which cards, including which stolen cards. This would include the time and date of the attempted fraud and could act as a system of crime pattern analysis for each product range.

The Cardcast system could also act as an automatic 999 service for shopping centre security staff. Where it had been ascertained that a stolen card was being used, a

message would be sent automatically to security staff who could then attend the scene of the crime.

One of the major card issuers has refused to join because it is involved in the development of the system involving Digital Cellular Radio services, which requires no connections or installation. This system can make up to 60 simultaneous authorisation messages on one call, reducing the average cost of authorisations which is the source of retailer resistance. However, as a result, all stolen plastic cards originating from that issuing bank are not listed on the Cardcast system and a potential means of defeating post block fraud is being missed. The losses sustained on those cards in the shopping centres where Cardcast operates could be prevented.

Apart from the recoveries, no hard data yet exist on the impact of Cardcast, and this system has been limited also by the low sales volume experienced in trial areas in the current economic recession. There is a need for greater agreement by merchant acquirers on which system should be adopted, but reduced telecommunications costs are essential if this optimal approach to 'post-block' fraud prevention is to become commonplace.

Fraudwatch: a proactive system of fraud prevention

One of the initiatives examined in the course of the project emanated from the work carried out by Touche Ross Management Consultants for Barclaycard, and since implemented by other financial institutions. Using a knowledge based computer programme, containing models of likely fraudulent behaviour assembled from the working knowledge of individuals within the Barclaycard fraud investigation department, Touche Ross devised a system designed to identify, **prior to their being reported as stolen,** classic Barclaycard accounts whose behaviour was indicative of fraud. By the end of 1990, the system had undergone 2 sets of trials, which, it was claimed, would generate annual substantial savings net of the cost of implementation of approximately £350,000. (See also Burrows, forthcoming.)

Previous pro-active solutions utilising conventional computing techniques had been attempted, but had always resulted in vast output of accounts, with little analysis consequently taking place because of the volume of output. The object here was to distinguish by behavioral modelling the fraudulent and non-fraudulent patterns of spending, thereby fine-tuning the accounts investigated in depth. (Clearly, part of this objective could be achieved by triggering off inspection when the number of daily transactions per card reaches a pre-set limit, but for large issuers, this is not cost-effective in staff time.) Those accounts that have been identified as containing possible fraudulent transactions are then compiled, and each individual account holder is then contacted by telephone by a member of Barclaycard's staff, in order to ascertain whether or not the card has gone missing or has been stolen.

As fraudsters become aware of the workings of this pro-active system, fraud must change its pattern to remain undetected. This means that the current models contained in Fraudwatch would have to be adapted to meet new patterns of fraud. In tests carried out in March/April 1990, Fraudwatch identified pre-block third party credit card fraud with a hit rate of about 1 fraud for every 20 accounts it spotted as being potentially fraudulently used. The comparable figure for the conventional computing system was about 1 in 12,000 accounts output. Some 67 accounts were eventually classified as containing fraudulent transactions. During this period, 1120 accounts were output by Fraudwatch, containing 59 of the 67 frauds. The system is particularly useful in spotting postal intercept fraud, but its value is enhanced considerably when it can operate 'on-line'. Given the life-cycle of much fraud, the first few days of use are critical, so the solution must lie in speeding up the loss to notification ratio.

Fears that the system might prove unpopular with customers have apparently proved unfounded. The reaction from most customers when they have been contacted to advise whether the card has been lost or stolen has been generally favourable: they are apparently pleased that someone has been keeping an eye on their cards. The only operational problem is that some customers have been telephoned more than once, on separate occasions when unusual use has been identified. There have also been technical problems with the time available for off-line analysis and with communication facilities for on-line processing.

Photographs on credit cards

The possibility of placing a photograph on a card has generated extensive debate. Most police officers we interviewed strongly supported it as a crucial contribution to the reduction of cheque and credit fraud. Suggestions have been made for the introduction of a **generic** Payment Authorisation Card which would have a photo of the bearer and would be accepted by all banks and building societies and at the point-of-sale in retail outlets. The other alternative is for **all** cards to carry a photograph of the bearer, but though this would have a preventative advantage that the photograph could appear on the same card as the signature, rather than the retailer or banker having to look at two cards and perhaps ignore one identifier, its total cost would be much higher, since cardholders own on average 3 cards. (With the spread of multi-function cards, this cost disadvantage should reduce.)

The case **for** the introduction of photographs on credit cards **soon** runs along the following lines. Fraud losses throughout the 1980's have escalated and look likely to continue unless drastic action is taken. The signature system of verifying a customer's identity where fraud takes place – banks, building societies and retail outlets – has serious limitations in that it is all too easy to forge another's signature, and the security checks on this process are rudimentary. Laser-engraved, digitised photographs, unlike pasted photos or even thermally engraved ones, are extremely difficult to counterfeit, at least **to the level at which experts would be deceived.** This

is because the machines to make these are very rare and are uneconomic for fraudsters to purchase. The technique to imprint by laser passport sized photographs onto cards is readily available at present, and the cost of production has reduced significantly over the past few years. Current estimates put production costs at about £1.40 per card, excluding photography costs and distribution, the latter being considerable. The cards themselves would have to last between 3 and (as in Finland) 10 years to be cost-effective, for the longer the cards last, the less the average annual fraud reduction has to be to justify the initial cost of producing them. (The costs of production would fall if the machines could later be used to put photographs on UK driving licences or photocards overseas.)

Logistically, there are a number of very severe production (and mass photography) problems that would have to be addressed before the introduction of photos on cards could be taken up as a serious suggestion. Nevertheless, the proposal is viable.

Public opinion is **not** resistant to the idea of a photograph on a bank card. Previously unpublished research conducted for the 1988 British Crime Survey (Mayhew, personal communication) indicates that a large majority are in favour of their introduction. 5,400 respondents taking part in the British Crime Survey were asked whether they had "an Access card, a Barclaycard or another credit card". 45 per cent said they had. These respondents were then asked "thieves often make fraudulent purchases with stolen Access and Barclaycards. It has been suggested that, to reduce the chances of this happening, these cards should have the holder's photograph on them. Do you think this is a good idea, or a bad idea?". 89 per cent said they thought it a good idea, whilst only 8.3 per cent thought it a bad idea and 2.7 per cent did not know.

Research carried out by Barclaycard for this research study supports the proposition that **card losers** are not resistant to the idea of photographs on cards. When asked if they thought a photograph would deter fraudsters, 96 per cent thought photographs would deter, with only 2 percent saying they would not. The sample were than asked how they felt about having photographs on cards. 85 per cent said they would either welcome them or welcome them strongly. Only 3 per cent said they would not welcome them, with a further 12 per cent stating that they had no preference either way.

There is, therefore, some evidence to show that public opinion is in favour of a photo card, though issuers may reasonably counter that the public is doing so in ignorance of the **financial** costs and benefits. How could photocards be administered? The cards could be produced either by issuers individually – if photos were on individual cards - or under the auspices of the APACS Standard Cheque Card Scheme, of which 51 UK banks and building societies are members, displaying the hologram of William Shakespeare and the standard signature panel. This 'Mastercard' could be used as a back up to all 'plastic' tendered by customers. All that would be required from customers requesting a card would be 2 colour passport type photos, 1 of which might be retained by APACS to act as a central photographic bank. The only

additional task this would entail for the retailer would be a requirement to write down the number contained on the Payment Authorisation Card - to show they have seen it – in addition to that of the card offered for payment. This would increase till waiting times. With the security of cheque guarantee card assured, it might then be possible to increase cheque guarantee limits across the board, benefiting customers and retailers, who would have a larger proportion of their transaction guaranteed. The introduction of photographs on cards could be backed up with larger rewards paid to cashiers, in order to increase the incentive involved in apprehending cheque and credit card fraudsters.

Proponents of the scheme argue that it would be possible to market a system of photocards to customers on the grounds that it was added crime protection for a customer's card, and the introduction could be phased in over a length of time. Those cards in the 'premier' range i.e. those that attract the highest average losses, could be given photos initially, moving onto the rest of the card base afterwards.

Against this argument are ranged a number of objections. First, there is the cost of their production. Even a common Payment Authorisation Card would cost the issuers a total of over £42 million, not to mention the costs involved in altering the administration of such cards in terms of instructions to retailers, changes to credit card vouchers and processing procedures. A new control and audit process would have to be instigated to ensure the quality and security of the cards being produced.

Secondly, it has not been proved that the presentation of photographic identification would result in decreased cheque and credit card fraud. It would be extremely foolhardy, this argument runs, to introduce such an expensive initiative without any concrete evidence that it would achieve its stated aim. A number of senior fraud investigators have expressed concern to us that it would be placing far too much emphasis on point-of-sale staff, effectively expecting them to police the system of card payments. As one fraud investigator stated to the research team, "you cannot expect people earning £5,000 per year to act as unpaid police officers".

Detractors to the argument point to the situation in France where a photocard was introduced several years ago but had to be withdrawn because some people refused to accept a photograph on their card. Issuing banks in the United States have toyed with the idea for several years, but rejected it on costs efficiency grounds, albeit that the geography of the US makes it more difficult to administer and costs have reduced only recently. New Zealand has abandoned photocards for the present, for Trustcard N.Z. ran an experiment for 18 months and found it not cost-effective, though it **did** reduce fraud. (The effects may be different where only one institution has photocards from where they all do so.) Only 3 countries have successfully introduced photographs on credit cards: Denmark, Finland and Norway. In these countries, the card base was low to begin with, which facilitated the introduction of photographs, and there is a relatively unsophisticated criminal underworld there, which means the absence of a major market for card misuse.

In addition, it is possible to obtain Visa cards in the United States, which presumably would not bear a photograph: these could be presented for payment in the UK. Would some fraudsters not simply move into cards obtained overseas to assist their activities? How should **these** cards be processed and authorised? (This merely shows that prevention would be incomplete not that the system would not reduce fraud.) Suffice it to state here that as with other areas of counterfeiting, it is crucial to examine the way in practice that such cards are likely to be treated at point-of-sale. If photographs or signatures look vaguely like the people to whom they refer, then given the social psychological reluctance of 'ordinary people' - not police or customs officers, who have specific crime reduction roles for which they are trained and paid - to challenge people the value of photocards is not as great as is imagined. Women, in particular, commonly change their appearance by different hairstyles and clothes. Organised criminals, who represent an unknown proportion of credit card fraudsters, may have available a range of people who look enough like the photographs to resist normal challenge: the major areas of likely deterrence are in relation to opportunists and to professional fraudsters of an ethnic group or gender different from that of the cardholder. We have been informed of cases where young English blacks - who are statistically unlikely to have been ennobled - have used the gold cards of titled persons of the same or even the opposite sex without challenge: photographs might make even the most diffident or absent-minded salesperson think, and would increase the risks to collusive traders who might currently accept such cards for transactions which increase their sales! However, if the counterfeiters produce cards with photographs on them, waiting for the stolen card before imprinting - however imperfectly – an accompanying name and signature the obstacles to counterfeiting will be reduced, and in the opinions of the industry as well as psychological research, the presence of the photograph will make it less likely that other security features such as signatures will be attended to. (Though since very few credit or cheque card frauds currently are detected by poor signatures, this may make little practical difference.)

In the US, some 80 per cent of transactions are authorised compared with 17 per cent in the UK: this is felt to be a more effective measure to prevent post-block fraud. Indeed, in all unattended card transactions, the bank 'Mastercard' would have no impact on the problem of fraud where the cards were lost or stolen. (Via increased risk of subsequent detection, however, it might deter fraudulent **applications.)** Payments made by credit card over the telephone – a major growth area for fraud - would not be affected, since it would not be possible to validate the card visually, Similarly, the photocard would have no impact on ATM fraud, though the banks – who deny the existence of **genuine** 'phantom withdrawals' – claim that this is very low at present. There might be **some** displacement effect, whereby more UK cards were sent abroad and used there. If there were a phased introduction of the photocard, the fraud reduction benefits might not be seen for years, because sales staff would not know whether the cardholder ought to have a photocard or not.

The final important point in this context is the civil libertarian one. In our view, this is largely illusory. No individual would **have** to apply for a photocard, nor would

they have to carry it with them if they possessed one. If they currently carry a card – their own or a stolen card – that serves as a limited ID which the police, under the Police and Criminal Evidence Act 1984, have some right to check out. If the card they choose to carry has a photograph and that photograph is theirs, this is a benefit since the police would have no right to detain them for verification purposes. The only losers in these cases would be fraudsters.

(Unguaranteed) cheque fraud

Would-be cheque fraudsters face 2 problems: getting a cheque, and converting it for cash. The most desirable cheques to steal are company cheques, whether blank (from the workplace, and ideally one of a bank or building society itself) or already made out. This is because in general, there are sufficient sums in the account (and overdraft limit) to cover the funds and because companies take time to discover the absence of the cheque. Both police and fraudsters have described to us the principal methods by which cheques are taken, and loose security over incoming mail at business premises – particularly multi-occupancy ones – is the principal opportunity, along with theft by postal employees. Here, there is evidence from our interviews with business people that theft of cheques from the mail is simply not seen by most trading companies as a serious risk to them.

Having stolen the cheque, the fraudster has to convert it. Given the huge volume of cheques and – by contrast with cards - the lack of need for continuing use, expensive security features are not normally considered, and cheques are produced for roughly one penny each. In the realm of cheque security, features that do not require high levels of concentration or time on the part of bank and non-bank employees seem *prima facie* likely to be more effective than features which, however subtle, require the kind of staff attention that is unrealistic in the cost control consciousness that we observe in business, including the banking business, today. Thus, as discussed earlier, clear visual displays are desirable on the **front** of the cheque if it is tampered with - by typewriter/printer as well as by ink - or is photocopied. The principal methods of achieving this are by holograms on cheques and the bringing up of 'VOID' following interference. The banks, not customers, would then be liable for any photocopied cheques that were paid by them. Because of their awareness of risk, victims of cheque theft are prime targets for enhanced fraud prevention: however, many cases are not reported to the police, so the banks have a preventative advice role here also.

Anti-counterfeiting/photocopying measures do not solve the problem where no alteration of existing words and numbers is made. In the past, it has been extremely easy for fraudsters simply to open accounts in any name, with minimal identification, most popularly in building societies. Having endorsed the cheque in the payee's name, s/he pays the cheque into the false-name account as a third party cheque. A variant is where the payee is a well known organisation - e.g. Inland Revenue, Ernst & Young – and the name of that organisation is altered to appear

to be an individual. The cheque is then laundered through a personal account in the individual's name. Sometimes – if the payee were, for example, accountants Arthur Andersen - this alteration may be unnecessary, though most people would not find it easy to open an account in the name of Arthur Andersen. In our view, the opportunities to do this should be diminished considerably by the implementation of the Guidance Notes for Banks and Building Societies issued by the Joint Money Laundering Working Group in December 1990. Nevertheless, convincing full driver's licences and passports are readily available on the black market.

The only method of ensuring-without tampering by the fraudster - that cheques are non-transferable is to add the word "only" after the payee; deleting the words "or order" which usually appear above the box giving the amount in figures; initialing that deletion; and writing the words "non-transferable" between the 2 vertical crossing lines printed in the middle of a cheque. This, combined with the technology described above, and writing the figures in the box and the words in such away that it is difficult to insert extra sums, should provide adequate security. Apart from consumer ignorance, the principal problem with these recommendations is their cumbersome quality. But we cannot stress enough that even small value cheques may be converted into large value ones.

Conclusion

If we had carried out this study 18 or even 12 months earlier, our conclusion would have been that the credit industry was riven with organisational conflict; that there was almost no information sharing except at an interpersonal friendship level; and that the prospects for a concerted business crime prevention effort were minimal. There was – if not antipathy, at least a Mexican stand-off - between card issuers (particularly **credit** card issuers) and many police forces, Each time either party had sought to develop any plan to tackle the problem, the others (or at least an important section of the others) had failed to respond positively: the classic example being the collective decision of the banks to drop the idea of a central handwriting bureau despite the genuine attempts - all be they unsuccessful - of the Metropolitan Police to tackle collusive retailers in the early 1980s. Though there were many examples of small groups of police acting against cheque fraud, the broad picture was of each side hoping that the other would solve their problem for them; while making tentative efforts at intra-industry co-ordination. Happily, that negative portrait is substantially inaccurate now. Indeed, there are so many initiatives by the Plastic Fraud Prevention Forum that it is difficult to list them adequately, let alone evaluate those that we have been told are 'in the pipeline'. Nevertheless, and despite these significant changes, we remain convinced that there is room for substantial improvement in cross-industry co-operation.

In this concluding chapter, we list such 'best practice' initiatives as we have found - or can envisage – in the logical sequence from cheque and card production to the conversion of the proceeds of fraud into cash or goods. We do not expect any reduction in the **motivation** to commit cheque and credit fraud, whether by opportunists, by professional criminals, or by those cast out by financial institutions upon the employment market. Rather, as the statistics on the growth of fraud indicate, we expect the popularity of fraud to increase. This makes it all the more important to develop methods of preventing that motivation from being converted into criminal practice. Our recommendations are as follows.

Credit, debit and cheque card fraud: some key prevention recommendations

Applications for cards

— **merge data sets in the industry,** even at the risk of reducing competition among fraud and 'doubtful address' database suppliers;

— **initiate tighter controls over requests to redirect mail,** including re-checking requests with customers;

Card and cheque theft

— **continue crime pattern analysis to identify insecure addresses;**

— **customer collection by, or secure delivery, to persons living in the areas identified above;**

— **card awareness campaigns among the public,** particularly at work, while travelling, at leisure, and even at point-of-sale, to reduce accidental loss and theft. Changing habits is difficult, but a useful focus here would be on the inconvenience of card loss. To reduce multiple card theft, people should only carry cards that they expect to use that day;

— **cheque awareness campaigns among businesspeople,** to increase their awareness of the risks of cheques being stolen in incoming and outgoing mail;

— **cardholder awareness of the risks of telemarketing fraud,** by not giving credit card details on the telephone more often than is absolutely essential;

— Card misuse

— **allow customers to select their own Personal Identification Numbers,** to reduce the chance of their writing down their number in a document that is likely to be stolen or looked at (even perhaps by people in their own household) with their card;

— **reduce telecommunications and terminal costs, which are the key to increased 'on-line' authorisation;**

— **encourage 'on-line' card authorisation mechanisms and technology to vary floor limits from remote terminals,** making it more difficult for fraudsters (including store staff) to predict safe card expenditures. Given the importance of floor limits, this constitutes a matter that should be taken into consideration when deciding whether or not anti-competitive practices are justifiable;

— **introduce laser-engraved Payment Authorisation Cards with photographs,** which will **reduce** the number of people who can pass off cards as their own. We cannot be **certain,** however, that this will bring **net** benefits to financial institutions;

— **improve staff training and encourage the retaining of suspect cards.** Setting 'charge-backs' from the banks for improper signatures against the individual store manager's performance targets may encourage them to train staff properly. Staff also need greater awareness of what **aspects** of the card are validated by the authorisation process;

— **tighten controls over merchants by acquirers, checking them against collective 'terminated merchant' files and, if appropriate, obtaining merchants' photographs.** Also, continuous monitoring of merchants' accounts to prevent them passing counterfeit vouchers (including those of numbers obtained by telemarketing) through their stores;

Cheque misuse

— **improve security for business cheques,** with holograms and other measures to make cheques harder to photocopy and successfully present for payment;

— **tighten controls on the opening of accounts and the acceptance of countersigned third-party cheques.** Adherence to the Guidance Notes issued by banks and building societies to prevent money-laundering will help this;

Policing changes

— **improve regional or national handwriting examination facilities,** paid for by banks or police authorities;

— **regionalism cheque squads, and particularly cheque and credit card fraud intelligence.** At present, cheque squads only deal with cheques that are stolen from that force area, not with cheques that are passed within the force area but stolen elsewhere. If only criminal intelligence is regionalised or nationalised, mechanisms which ensure appropriate follow-up action are vital;

— **include offences of theft of cheque hooks, of cheque and credit cards, and the fraudulent use of lost and stolen cbeques and cards, as separate categories in incident-based crime recording systems;**

— **encourage bank-police liaison throughout the country at operational as well as senior level;**

— **change credit card voucher system, so that store or bank, rather than fraudster, retains the top copy with fingerprints and good signature.** This would make vouchers forensically useful in investigations and prosecutions, and would bring the UK in line with the rest of the world;

Partnership policing: the way forward

During 1989 and 1990, a series of discussions were held between staff of the Home Office Crime Prevention Unit and 90 Metropolitan police officers. One topic for discussion was which offences - of those they spent time investigating - they considered to be 'preventable' by victims, given sufficient goodwill. These debates led almost unanimously to the choice of cheque and credit card fraud as the most preventable area of crime. There was clear frustration within the police service at the amount of time taken up by these cases, which they felt could be reduced if the banks, building societies, and other credit issuers co-operated with each other more.

In the light of those discussions, the research reported here was commissioned, and it has shown that during 1990 and 1991, the industry has made substantial moves to protect itself. For the first time, there is concerted information sharing between most institutions, and – to improve detection and consequent prevention - it is possible that a central handwriting bureau may be organised by the banks. These developments are driven, of course, by the severe increase in fraud and by the drop in profits that makes those frauds more serious to the industry. Critics might still maintain that the credit issuers are too reluctant to spend large sums to prevent fraud: the issuers might respond that they are simply trying to maximise their cost-effectiveness! Reasonable people can disagree on whether or not the present balance is right.

All parts of the credit industry agree that irrespective of the contribution they make to taxes and community charges, the primary burden of prevention ought to lie on the industry itself, not on the police. We have suggested in this section a number of ways in which the significant improvements in industry-wide co-operation already made could be enhanced further. However, since the initial discussions with the police there has been a sufficiently large reduction in the number of preventable frauds for the police **now** to feel that time spent on investigating the remaining cases is not wasted on the undeserving. If this study has helped to develop an understanding of how, together, the private sector and the police might have a real impact on cheque and credit card fraud, **our** efforts will have been worthwhile.

References

Burrows, J. (forthcoming) *Making Crime Prevention Pay: Initiatives from Business* Crime Prevention Unit Paper 27. London: Home Office

Confederation of British Industry (1990) *Crime: Managing the Business Risk* London: CBI

Forrester, D., Chatterton, M. and Pease, K. (1988) *The Kirkholt Burglary Prevention Project* Crime Prevention Unit Paper 13. London: Home Office

Home Office (1988) *Report of the Working Party on the Costs of Crime* London: Home Office

Hough, M. and Mayhew, P. (1985) *Taking Account of Crime: Key Findings from the 1984 British Crime Survey* London: HMSO

Jack Committee (1989) *Banking Services: Law and Practice Report by the Review Committee* London: HMSO

Levi, M. (1981) *The Phantom Capitalists: the Organisation and Control of Long-Firm Fraud* Aldershot: Gower

Levi, M. (1988) *The Prevention of Fraud* Crime Prevention Unit Paper 17. London: Home Office

Levi, M. (1991) *Customer Confidentiality, Money-Laundering, and Police-Bank Relationships.' English Law and Practice in a Global Environment* London: Police Foundation

Mars, G. (1983) *Cheats at Work* London: George Allen and Unwin

Monopolies and Mergers Commission (1988) *Report on Credit Card Services* London: HMSO

Glossary

APACS - Association of Payments and Clearing Services.

ATM - Automated Teller Machine for drawing out cash.

Charge card - a card which has to be settled monthly, but which allows deferred expenditure, eg. American Express, Diner's Club.

CIFAS – Credit Industry Fraud Avoidance System.

Collusive merchants - merchants who agree to take cheque or credit cards which they know to be stolen or counterfeit.

Debit card - an electronic substitute for cheque and cheque card, which allows transactions to be debited to accounts currently in the same time-lag as a cheque.

EPOS - Electronic Point-of-Sale, where electronic means are used to process transactions.

Externalities - costs that arise outside of the direct transactions (eg. imprisonment costs may arise from detection).

Fidelity bonding - a system of insurance whereby premiums are paid to cover fraud and theft by employees.

Floor limits - transaction levels above which the store must obtain authorisation before allowing credit. Stores who accept such transactions without authorisation are liable for the loss themselves.

'Hot' card file - computerised or written list of lost and stolen cards.

MMC - Monopolies and Mergers Commission,

Merchant acquirers - financial institutions who process all credit card transactions on behalf of merchants.

'On-line' - direct interaction with a computerised database.

POID - Post Office Investigation Department.

'Post-block' fraud - fraud which occurs **after** a card has been reported lost or stolen and its further use prohibited.

'Pre-block' fraud - fraud which occurs **before** a card is reported lost or stolen and action taken to stop its use.

Store cards – cards issued by the store, which allow purchases only at that store or chain of stores, eg. Dixons, House of Fraser, Marks & Spencer, Sears.

Telemarketing – a growing method of fraud by which other peoples credit (or debit) card numbers are used by fraudsters to order goods for themselves by telephone, sometimes via collusive merchants.

Terminated merchant's file – a list of merchants who have been struck off a merchant acquirers roll of traders as a result of their suspected violation of the rules for doing business.

Crime Prevention Unit Papers

1. **Reducing Burglary: a study of chemists' shops.**
   Gloria Laycock. 1985. v+7pp. (0 86353 154 8).

2. **Reducing Crime: developing the role of crime prevention panels.**
   Lorna J.F. Smith and Gloria Laycock. 1985. v+14pp. (0 86252 189 0).

3. **Property Marking: a deterrant to domestic burglary?**
   Gloria Laycock. 1985. v+25pp. (0 86252 193 9).

4. **Designing for Car Security: towards a crime free car.**
   Dean Southall and Paul Ekblom. 1986. v+25pp. (0 86252 222 6).

5. **The Prevention of Shop Theft: an approach through crime analysis.**
   Paul Ekblom. 1986 v+19pp. (0 86252 237 4).

6. **Prepayment Coin Meters: a target for burglary.**
   Nigel Hill. 1986. v+15pp. (0 86252 245 5).

7. **Crime in Hospitals: diagnosis and prevention.**
   Lorna J.F. Smith 1987. v+25pp. (0 86252 267 6).

8. **Preventing Juvenile Crime: the Staffordshire Experience.**
   Kevin Heal and Gloria Laycock, 1987. v+29pp. (0 86252 297 8).

9. **Preventing Robberies at Sub-Post Offices: an evaluation of a security initiative.** Paul Ekblom. 1987. v+34pp. (0 86252 300 1).

10. **Getting the Best Out of Crime Analysis.**
    Paul Ekblom. 1988. v+38pp. (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 Hussain. 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).

17. **The Prevention of Fraud.** Michael Levi. 1988. v+19pp. (0 86252 359 1).

18. **An Evaluation of Domestic Security Surveys.** Gloria Laycock. 1989. v+33pp. (0 86252 408 3).

19. **Downtown Drinkers: the perceptions and fears of the public in a city centre.** Malcolm Ramsay. 1989. v+23pp. (0 86252 419 9).

20. **The Management and Prevention of Juvenile Crime Problems.** Barrymore Cooper. 1989. v+63pp. (0 86252 420 2).

21. **Victim Support and Crime Prevention in an Inner-City Setting.** Alice Sampson and Graham Farrell. 1990. v+27pp. (0 86252 504 7).

22. **Lagerland Lost? An experiment in keeping drinkers off the street in central coventry and elsewhere.** Malcolm Ramsay. 1990. v+38pp. (0 86252 520 9).

23. **The Kirkholt Burglary Prevention Project: Phase II.** David Forrester, Samantha Frenz, Martin O'Connell and Ken Pease. 1990. v+51pp. (0 862562)

24. **Probation Practice in Crime Prevention.** Jane Geraghty. 1991. v+45pp. (0 86252 605 1)

25. **Lessons from a Victim Support Crime Prevention Project.** Alice Sampson. 1991. vi+41pp. (0 86252 616 7)