Criminal Justice and the Future of Payment Card Fraud

by Michael Levi
and Jim Handley

ippr 2002

1860301673

Contents

ippr
30-32 Southampton Street
London
WC2E 7RA
tel +44 (0) 7470 6100
fax +44 (0) 7470 6111
email info@ippr.org.uk
www.ippr.org.uk

charity number: 800065

ippr is the leading independent think tank on the centre left. Through our well-researched and clearly argued political analysis, our publications, our strong networks in government, academia and the corporate sectors, we can play a vital role in maintaining the momentum of progressive thought.

Acknowledgements

The authors would like to thank (in alphabetical order): Andrew Brown (NCIS), Detective Inspector Tony Drain (City of London Police), Peter Hurst (CIFAS), Robert Littas (Visa International), Paul Lucraft (Europay), John Simpson (BRC), Ian Spencer and colleagues (Barclaycard), DC Nick Sutton (Bedfordshire Police) and John Wilkinson (APACS) for contributing data, informed opinion, insight and helpful comments on an early draft of this paper.

IPPR would like to thank Barclaycard, The Bar Council, the Calouste Gulbenkian Foundation, the Esmee Fairbaim Foundation, Group 4 Falck and the Institute of Legal Executives for their support of this research.

The Authors

Michael Levi is Professor of Criminology at Cardiff University's Criminological Research Centre. He specialises in research on financial and organised crime and its control, and is currently funded by the ESRC Future Governance Research Initiative in a study of the making and implementation of financial crime policy around the world. His books include The Phantom Capitalist; Regulating Fraud and Money Laundering in the UK and his most recent book White-Collar Crime and its Victims(with Andy Pithouse) will be published by Oxford University Press in 2002. He published earlier studies on payment card prevention for the Home Office and the banking industry in 1991 and 1998.

Jim Handley is Principal Lecturer in Psychology in Occupational Psychology at the University of Glamorgan. He has previously researched diagnostic reasoning in complex process control industries and inter and intea-organisational issues involved in payment card fraud for the Home Office and banking industry.

The Forum

IPPR's Criminal Justice forum has been established to devise policy proposals on the future of the criminal justice system in England and Wales. Drawing together leading thinkers in the field, the Forum aims to be a catalyst for cutting-edge research and high level debate on the strategic questions facing the criminal justice system. The Forum has commissioned papers, and opinion research and is holding seminars and conferences on a range of criminal justice issues.

For further information about the Forum's programme of work, please contact IPPR Research Fellow, Clare Sparks on 020 7470 6128 or c.sparks@ippr.org.uk

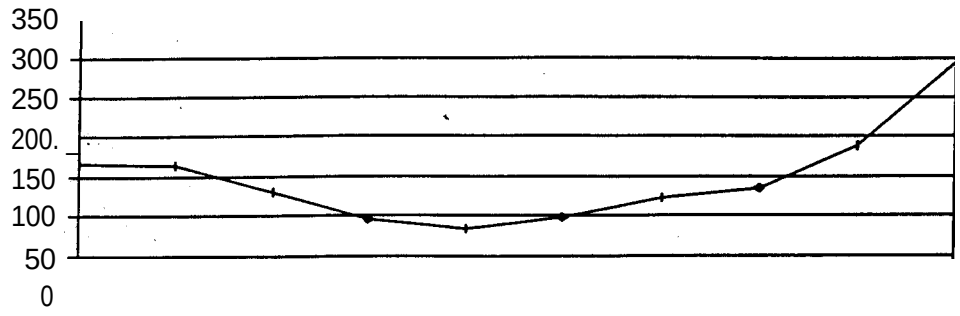
1. Background and historical summary:

the last ten years

Plastic payment cards are ubiquitous in the contemporary commercial environment, providing a convenient and generally secure medium with which people conduct a wide range of transactions. Their convenience, combined with extensive advertising and selective mass mailings, has resulted in relentless growth of their possession and use, with approximately 86 per cent of British adults holding one or more cards, and around 103 million cards from approximately seventy issuers currently in circulation. The volume of transactions across all kinds of cards has increased threefold over the last decade. Debit cards particularly have risen in popularity (at about twice the rate of growth for that of credit and charge cards 1) and by 1999, they were for the first time used more often to purchase goods and services than for making cash withdrawals at bank counters and at the 34,339 ATMs.

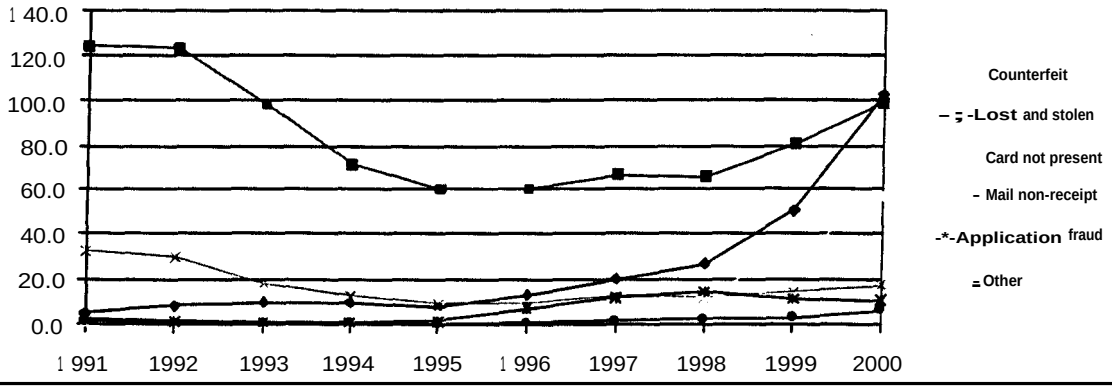
However, with new commercial opportunities come new crime opportunities, and the continual battle between the industry and criminals has made the past decade something of a roller-coaster ride for the payment card industry. At the beginning of the 1990s, plastic card fraud stood at around £165 million per annum, after a dramatic rise in the late 1980s. The Home Office commissioned Levi Report was followed by a raft of measures which significantly reduced the fraud rate, despite the increase of card use: the low point in 1995 saw fraud losses at just over £83 million. However, from 1995 to the present there has been a consistent, year on year rise in the absolute amount of fraud losses on payment cards, approaching £300 million in 2000 (see Figure 1 below.) The police recorded 170,100 cases of cheque and credit card fraud in the 12 months to September 2000 (Home Office 2001), but the vast majority of cases remain unreported to them, since there is little prospect of action against which to offset the issuer or acquirer staff time and cost involved, and reporting `dud' cases undermines the credibility of the commercial victims and their representatives the next time they want to see some action taken.

Figure 1: Fraud on payment cards 1991-2000 (£millions)



Closer examination reveals that within this overall rise, there has been a significant change in the *pattern* of fraud. Fraud on lost and stolen cards (which has, until now, constituted the largest proportion of loss) stands at 80 per cent of the 1991 level, and fraud on cards diverted in the mail is around half its 1991 level in absolute terms. All other categories of fraud are higher than they were in 1991. Fraud on counterfeit cards has now surpassed that on lost and stolen cards and stands at more than twenty-two times the 1991 level. Fraudulent transactions where the card is not present (CNP) have shown a startling rise (albeit from initially low levels) to one hundred and forty two times the 1991 level. (See Figure 2 below.) There is genuine cause for concern about the current trend, but these figures need to be interpreted in the context of steadily increasing card use (and corresponding opportunities for mis-use) and number of cards in circulation. As in previous period, there is no simple relationship between payment card frauds and their criminal precursors - theft and robbery - and counterfeiting/card not present fraud further split off fraud opportunities from the necessity to commit a traditional property crime.

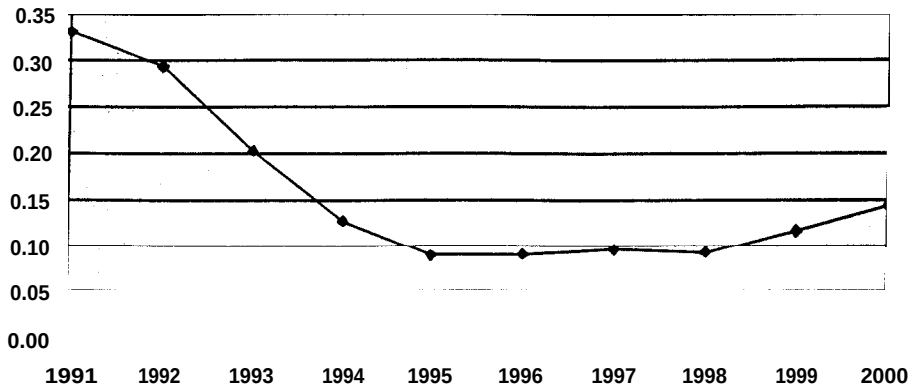
Figure 2: Categories of payment card fraud loss 1991-2000 (£millions)



As can be seen from Figure 3, the *falling* ratio of fraud to turnover throughout most of the 1990s is one of the most consistent trends in the figures presented here. Despite an upturn over the last two years, the rate of fraud to turnover currently stands at 0.145 per cent - less than half of its 1991 level - though current trends may make substantial inroads into this gap. Ideally, one might want to look at fraud as a proportion of profits to show how hard the industry would have to work to replace its fraud losses, but in the absence of reliable industry-wide profit data, turnover will have to suffice.

Each card type has a substantially different fraud to turnover rate: credit cards represent the highest risk (0.20 per cent), followed by charge cards (0.14 per cent) and debit cards (0.10 per cent). Furthermore, though the company data are confidential, there have always been wide variations in the fraud experiences of different card issuers within each card type. For credit cards, the most fraud-prone card issuer suffers approximately twenty-one times more fraud per card than does the least fraud prone. For debit cards and charge cards, the difference is less, but

Figure 3: Card issuers' losses as proportion of turnover (1991-2000)

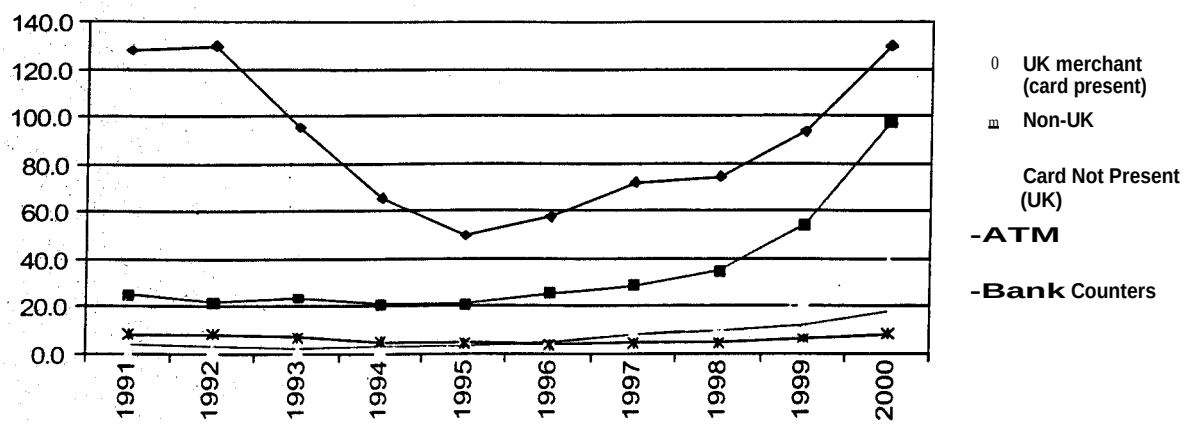


note: scale is in 9b - so the 1991 figure of .329 means about a third of one percent

it is still in the order of six times more for the most fraud-prone. This reflects *inter alia* different marketing strategies and regional take-up rates from card issuers (often at different stages of the maturity of their target `audience'), differences in card security measures, and criminal perceptions of the comparative risks of fraudulent use of different cards.

Sometimes, one can be too readily seduced by the percentage rate of change of sub-types of fraud, especially by 'hi-tech' risks. An overview of changing patterns in the distribution of plastic fraud is particularly infonnative. Figure 4 (below) shows the significant fall in fraud through the early 1990s, (largely due to increased on-line authorisation of transactions, the introduction of 'hot-card files' and a number of other measures). UK merchants still pass the majority of all fraudulent transactions on physically present cards, but there is also significant growth both in fraudulent transactions on UK issued cards used overseas and also in CNP transactions within the UK. Perhaps surprisingly, in the light of all the publicity and concern about card not present fraud - only some of which involves the media favourite, the Internet - the trend line shows a less steep rise for this than for other types. 2

Figure 4: Place of Misuse 1991-2000 (fraud values £millions)

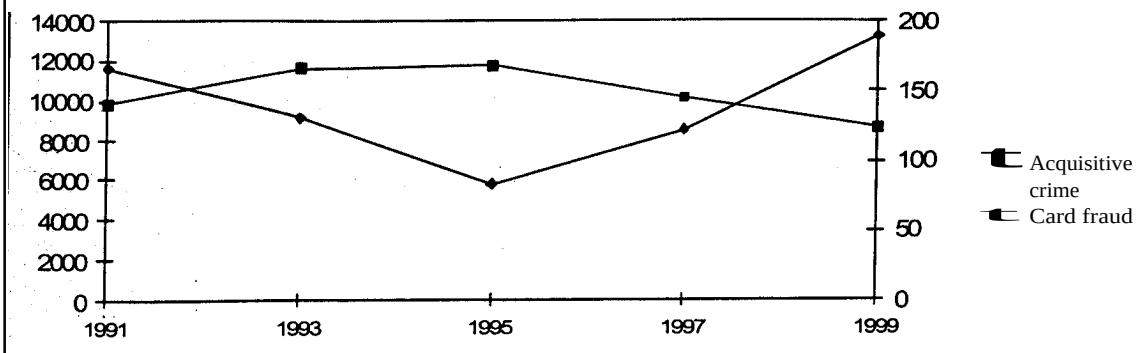


Although not separated out in these data, mobile phone companies have suffered particularly high losses with `top ups' of phone accounts on counterfeit, lost/stolen or compromised cards. (Some estimates are that at one point, 13-14 per cent of all top ups made with cards were fraudulent.)

It is difficult to estimate accurately the volume of electronic commerce, for Internet transactions are not currently distinguished from other CNP data: though the card schemes have mandated an electronic commerce indicator on transactions, full implementation is some way off. Consequently, there are only estimates of what proportion of CNP fraud is on the Net. The majority of losses seem to be distributed between low value/high volume transactions (such as books, CDs, pornography) and high value/low volume (such as flights, computer equipment). Some estimates are that e-fraud accounts for approximately 12.5 per cent of CNP (by volume) and so, less than 3 per cent of all current plastic fraud, suggesting that we should keep the e-risks in perspective. Industry initiatives to encourage e-commerce by guaranteeing that the cardholder will be protected from any fraudulent use may tempt some into first party fraud. (There is a high rate of customer repudiation of e-commerce transactions anyway, which imposes a considerable financial burden on those who have to deal with them.)

A cursory comparison of the broad trends of plastic fraud and acquisitive crime shows that they follow rather different trends (consistent with displacement but not clear evidence of it) (see Figure 5 below) though some analyses reinforce the notion that individual `species' of payment card fraud require specific knowledge, skills, social networks and other resources that make displacement between them problematic (see Mativat and Tremblay 1997). Although much card fraud still arises from lost and stolen cards (and, to a lesser extent from mail interception), the possibilities of remote fraud - disintermediated in a sense from what is often termed `primary crime' such as burglary and robbery, have expanded markedly, enabling these different rates of change to occur.

Figure 5: Acquisitive crime (number of incidents) & plastic card fraud 1991-1999 (£millions)



Source. The 2000 British Crime Survey England and Wales. Home Office Statistical Bulletin 18/00 (October 2000) APACS (Association of Pavment Clearing Services)

2. Projections

Short-term projections - The next five years

Predicting the future in such a complex and dynamic domain is fraught with difficulty, and accurate projections beyond five years would require mystical abilities neither possessed nor claimed by ourselves or any of our respondents.[3] Nevertheless, reasoned arguments can be constructed for predicting that within an overall rise in fraud levels, some varieties of fraud will continue to rise, some will remain relatively static and some will fall. From 1999 to 2000, fraud on lost and stolen cards increased by 24 per cent, while counterfeit and CNP fraud virtually doubled. The industry estimates (making some sensible assumptions about growth and the effects of ongoing and planned future prevention measures) that by 2005, the gross rate of plastic fraud will be in the order of £450 million per annum.[4] (that is, half as much again as today's nominal level). This needs to be broken down in to its component parts.

Fraud on lost and stolen cards is predicted to rise, but at a much reduced and falling rate from 2002 on, from which time the rollout of chip cards and introduction of PIN at point of sale (p.o.s.) will have more and more of an effect.[5]

Applications fraud is predicted to rise at a relatively stable and modest annual rate of 10 per cent in the next 5 yrs, contained by the success of CIFAS (the UK Fraud Avoidance System) and fraud data matching making for more rapid identification of 'mail drops' and other vulnerable locations. As new controls are brought into play to deal with counterfeit and lost and stolen cards, the temptation to invest in applications fraud will increase, especially as the criminal investment costs are quite modest.

Counterfeit is expected to continue to grow but at a reducing rate of increase year on year with the growing penetration of chip cards (and PIN at p.o.s.). By 2005 it may be more than twice as high as fraud on lost and stolen cards.

CNP fraud is expected to continue to rise, but at a reduced rate until 2003 due to the effects of the introduction of checks using the card security code and on-line cardholder information verification. (AV2/CVS.) After 2003 it is expected to fall steadily.

As a subset of CNP, e-fraud on cards is expected to rise with the anticipated surge in e-commerce generally, and with current estimates being that e-fraud represents perhaps 3 per cent of total card fraud on 1-2 per cent of total transaction volume, the Internet might seem to be a disproportionately risky medium. This would be a misleading generalisation though. Closer scrutiny of the data shows that some sectors (such as on-line gambling, pornography and Internet Service Providers - ISPs) account for the majority of fraud on-line, and e-commerce encourages use of payment cards in what, in face to face entertainment are traditionally cash-intensive areas. Nevertheless, most other areas are relatively free from fraud.

Longer term speculations - twenty years on

To have predicted the current volume and kinds of plastic card fraud from 1980 or even 1990 would have been an impressive feat. It is probably more difficult to predict what will happen over the next twenty years, and to do so with confidence would invite justified ridicule. Although this requires our making assumptions which may turn out to be mistaken, we do find certain features to be more plausible than others, however. In an uncertain world, versatile and flexible responses allow the greatest possibility of adaptation to yet future threats.

A number of factors are likely to contribute to changes over this period: continued growth of international markets, expansion of the Internet as a commercial environment, integrated databases, mass/mobile communications, travel and access to information, moves toward a `24/7' culture with changing patterns of work and leisure. Technological changes, particularly in the bio-sciences, genetics, nano-technology and changes in social demographics are also likely to change the environment in which payment card occurs.

Various projections have attempted to describe possible trends, and common themes that may have some bearing on the issues the Criminal Justice System (CJS) and payment card industry operate include:

> Projections of demographic trends over the next 20 years or so predict an ageing population but also (over the next decade) an increasing number of 15-20 year olds (Government Actuary's Department, 1998). Both because of a possible growing inequality of disposable income between these groups and because of continuing high expectations of instant access to products fuelled by advertising, card fraud might become a convenient and attractive (to juveniles) method of `affordability' or redistribution. Despite the presence of CCTV, we find it plausible that there will be a rise in actual and/or threatened muggings to get money for drugs and conspicuous consumption, as a street equivalent to the rise in robberies of cash in transit as safes became better protected. Furthermore, although we do not anticipate a major increase in card crime by the elderly (for cultural reasons), it should not be forgotten that fraud is the only major property crime that is not inhibited by age and mobility.
>
> It currently seems inconceivable that the developments in power, miniaturisation and falling costs of ICT will abate. Its use for e-commerce, `home shopping' using the Internet, a variety of mobile devices and Interactive Digital Television (IDTV) may well characterise a major trend in consumer behaviour. Unless there are very secure transactions on these media, this could be a large growth area for plastic fraud. Also, information on how to compromise (hack into) erstwhile secure systems, which is already shared on the Internet, will spread more quickly and widely.
>
> An increase in electronic delivery of a number of products (music downloads, video, information software etc.) may provide attractive targets and generate low cost/high

volume fraud which would be particularly difficult to police. Currently in fraudulent transactions of this nature, where the card is not present to be checked, fraud costs are charged back to the retailer, though planned changes (see below) to this system will redistribute the pattern of costs.

Though the skill `entry requirements' to engage in plastic fraud are rising and are likely to continue to do so as more sophisticated technological security is introduced, the cost of technology is falling and with it, the barriers to techno-crime. Furthermore, the potential rewards of breaking these measures are also increasing dramatically. More sophisticated criminals with specialised knowledge might be tempted to take the challenge of high tech. security protecting high value reward, especially if the cost (including apprehension cost) of unsuccessful criminal attempts is low. The risk of internal compromise of payment systems is likely to become an important issue.

The issue of personal identity may become more important. The payment card industry is not seriously considering the use of any biometric method of cardholder identification for at least ten years, but in the longer term, if robust technology makes this possible and convenient to the point that it becomes a trusted procedure then compromising such a security method could become a particularly attractive proposition for technically sophisticated fraudsters. There must be appropriate provision for dealing with misuse and how liabilities are apportioned.

Anonymity in distant transactions already contributes to the attraction of CNP fraud and will continue to do so well into the future, particularly if changing employment trends lead to greater social mobility.

Cash remains king of convenience for small purchases and despite concerted efforts by the card industry to introduce `electronic purse' cards, they have not found widespread acceptance. If they do, they will bring their own (and different) problems.

3. The criminal justice system and payment card fraud

The role of policing and government in this arena remains controversial. A large measure of devolved prevention in a policing-free environment has already occurred and, whatever the industry complaints, full reporting of all payment card fraud for criminal justice intervention would involve staff and other costs that are logistically impossible for the industry and would be unlikely to be welcomed by them or by the police or government. Though it acknowledges the recent rise in plastic card fraud, the government's recent set of proposals for modernising the Criminal Justice System makes no specific recommendations for dealing with card fraud in the future (Attorney General's Office et al 2001). Nevertheless, a number of the general recommendations can be interpreted in relation to card fraud.

The need for public-private and cross-sectoral collaboration is relatively uncontroversial. Without the assistance of financial institutions' Management Information Systems (MIS), the detection and investigation of plastic card fraud already lies outside the easy grasp of most police forces. More contentious is the issue of how the costs of such co-operation are distributed. Financial institutions and retailers have a legitimate expectation, when they are victims of costly fraud, that this crime will be vigorously investigated. However, plastic card fraud is a particularly difficult crime to police and investigations can be costly in terms of the resources involved and despite the strong emotions evoked, for example, by identity fraud (discussed below), the policing of card fraud also receives little direct populist pressure from media or established victim representatives or community safety groups (see Levi and Pithouse, forthcoming). Although there are precedents for technical support and training and for the funding of specific police operations by financial institutions, questions need to be asked about the principles underlying such partnership funding. Other crimes might also be costly or difficult to investigate - should the victims of such crimes have the option of funding special investigations or indeed should they be required to do so if their pain is to be pursued by public bodies? Is the criterion purely one of affordability or `deep pockets' and if so, should wealthy individuals also be required to pay extra for police attention? Although private funding does not detract from police resources available (and represents something of a return to the pre-19th century tradition), the public perception of this arrangement might be that de facto there would be `one law for the rich another for the poor' - in other words, those prepared to pay get better policing - whereas financial institutions might feel as if they are unreasonably being asked to `pay twice' for policing. Nevertheless, privately funded policing can be developed positively, as in a recent initiative in which the industry's keen pursuit of such partnerships has resulted in advanced negotiations towards a jointly funded (APACS and government) police investigative unit to be established on a trial basis in 2002. One of the

anticipated advantages of such a unit is that it will be able to operate nationally, across traditional police force boundaries, just as offenders do. There may however also be a need to ensure consistent and professional involvement of prosecutors at an early stage to ensure that this investigative work is not wasted.

There is clearly also a need for investigative forces to (at least) keep pace with criminal technical skills, and to have forensic services sufficient to bring such cases to trial. Technological advances in security in the plastic card industry have been met by innovative and adaptive advances in plastic card crime. There is no reason to suspect that this situation will change either in the short or long-term. ICT and analytic skills are widely regarded as essential in a wide range of employment, and policing certainly needs to keep pace with these changes if it is to have any realistic chance of controlling such crime. Whether the new Hi-Tech Crime Unit will have payment card fraud counterfeiting or skimming within its remit in practice remains open to question, as there will be many demands upon its resources and paedophile netporn has a higher populist appeal. In the light of the need for close liaison between the card industry, retailers and the police, there may be much merit in the location of such a unit close to the APACS Fraud Intelligence Bureau.

Violent and non-violent crime for gain have risen over the past twenty years, and payment card fraud has probably risen as fast as any type. The government's analysis is that approximately half of all crime can be attributed to about 10 per cent of the total of estimated active criminals (Attorney General's Office et al 2001). It is very likely that an even greater disproportion exists in plastic card fraud and advanced security will increase this imbalance, with a small number of technically sophisticated offenders causing the greatest amount of damage to the system. For them, the advantage of merging with organised crime networks is to enable larger `hits' to be made within a short period of time than is possible when one works alone, even using multiple card not present transactions. There is keen interest in targeting policing efforts, and this pattern would suggest that this is an intelligent strategy for card crime, though moves such as establishing a DNA database (which is projected to include the whole active criminal population by 2004) might have minimal effect on plastic card fraudsters who typically leave little if any forensic trail and who, due to the growing international nature of their operation, will be difficult to track and apprehend.

Over the last twenty years the probability of an offender being apprehended has fallen and, currently less than a quarter of the crimes recorded by the police result in a prosecution (compared to 40 per cent in 1980). However, whether the perception that fraudsters are escaping unpunished will undermine confidence in the CJS or the payment card industry depends on a complex range of beliefs about the roles, responsibilities and capability of both. Figures from the 2000 British Crime Survey (Home Office, 2000b) show that fear of payment card fraud is a real issue, with 50 per cent of respondents reporting being fairly worried or very worried about credit/bank card fraud - more than for mugging/robbery (44 per cent) or

physical attack (43 per cent) and approaching theft from cars (53 per cent), theft of cars (57 per cent) and burglary (57 per cent). Even if very worried is taken as the more serious criterion of concern, credit/bank card fraud (16 per cent) is still comparable with mugging/robbery (17 per cent), physical attack (18 per cent) and burglary (19 per cent). As police-recorded cheque and credit card fraud has a detection rate of about 25 per cent (Home Office 2000c), [7] most victims of impersonation by card fraud will not have their impersonator caught (assuming there is not a very high re-victimisation rate). Among the objectives outlined in the report on reform of the CJS are: `To promote confidence in the CJS by increasing the number and proportion of recorded crimes for which an offender is brought to justice' and `To ensure by 2004 that crime and fear of crime ...are lower than in 2001' (Attorney General's Office et al, 2001).

In order to do this, there must be more detailed research into the psychological and emotional effects of payment card on the individual: our pilot interviews suggest that people are perhaps surprisingly affected, rather than viewing it as just corporate losses.

Changing demographic and economic trends, patterns of immigration, employment and social mobility in addition to technological changes might provide opportunities and motivation for more and more varied forms of payment card fraud. The largest problem for the payment card industry today (counterfeit `skimming') was virtually non-existent twenty years ago. The future will certainly provide opportunities for frauds that we cannot yet imagine. Whatever plans are made to inhibit future fraud should be flexible, adaptive and varied.

Organised crime has been implicated in plastic fraud and there are current plans to combat the rewards of `becoming organised'. These include new legislation (including the Proceeds of Crime Bill 2001) and a range of other measures. Research indicates that some organised crime groups[8] engage in a range of activities (such as drugs, counterfeiting, other theft). Payment card fraud would seem an ideal candidate for the involvement of such crime gangs for a number of reasons: potential rewards are great; the nature of the crime requires both resources and networks to successfully complete on a large scale; and the anonymity offered by modern technology and cross-border opportunities make it ideally suited for such groups.

Much current fraud is facilitated by existing social networks, which are necessary for providing opportunities for compromising cards at retail points of sale, sharing the necessary information, equipment and resources for counterfeiting. The amount of detail recorded in official crime statistics could be refined to include payment card fraud and, to the extent that this might change to include a combined measure of crime and crime seriousness, the anxiety data from the BCS 2000 cited earlier would suggest a greater appreciation of the importance of payment card fraud at variance with the way it currently is viewed in most police forces. The recent Home Office Review of Crime Statistics [9] recognises that the level of detail of reporting of certain categories of fraud is inadequate and proposes co-operation between the

Home Office, Serious Fraud Office, and the banking and insurance industries, which would certainly be necessary to address adequately the problem of payment card fraud but would go well beyond that. The report also stresses the importance of conducting problem-focused studies[10] Detailed and accurate geographic level data (for example, postcode information) would be useful for crime pattern analysis to understand better how payment card fraud is organised and to inform both operational and policy-making decisions. For example, where large retail chains are victims or intermediaries of fraud, store-level data are needed to pinpoint possible staff involvement or to clear staff who otherwise might be under suspicion.

4. Discussion and recommendations

One of the developments in the understanding of professional crime is to break down the prerequisites for `making crime happen' into `scripts' which criminals have to follow. Thus, relatively independent of the medium of fraud or security counter-measures, there are things that fraudsters need to do. First, card information has to be acquired (by making a fraudulent application for a genuine card, stealing a card, `skimming' card details of another person's card or generating an account number with a program from the Internet). For counterfeiting, certain equipment and materials are required and some preparation and work has to be done to produce passable cards. Fraudulent transactions then need to be made, whether face to face transactions or card not present. Any goods from these transactions need to be received. (If ordered remotely, this may involve some work, for example, in setting up a delivery address for a telephone or Internet order.) These goods may then be exchanged for cash in the criminal market place. Throughout this process, the fraudster needs to avoid detection by the industry and - a separate risk set - arrest, prosecution and punishment by the criminal justice system. The critical stages and `weakest links' in this process are most likely to be: acquiring cards or card details and successfully conducting the transaction. However, by itself, prevention of one transaction or set of transactions may not provide much deterrence for future attempts: there is a wide scope for criminal experimentation at relatively low cost and risk.

As the above discussion suggests, it is unhelpful to analyse payment card fraud as a unitary phenomenon: it is rather a number of related activities with different modus operandi, knowledge and skill requirements. The benefits of prior control measures endure and without their continuation, those frauds would spring up again (though how consistently and rigorously these measures are implemented is open to question). Although a, number of quite different, equally plausible arguments might be constructed for implicating different parties as carrying the responsibility for dealing with plastic card fraud, it is those who suffer most from it and have the necessary resources to address it that have so far taken the challenge of development and implementation of prevention measures. These include security information encoded on cards, setting up transaction authorisation systems, screening applications, maintaining 'hot-card' lists, developing 'chip-card' technology, education and `awareness' campaigns, proactive monitoring of account behaviour, maintaining and improving MIS and data sharing.

It is a common cognitive mistake to assume that if one no longer has a visible problem or if one has a reduced problem, there is no longer any need to maintain prevention. There is certainly no reason to abandon measures that have been effective until now, and the overall reduction in fraud to turnover rate throughout most of the 1990s is testimony to the effectiveness of measures already implemented. There is no reason why frauds currently prevented would not return controls were relaxed. However, unless a completely secure

payment system is devised, then there will inevitably be some risk, and greater use will normally provide more opportunities for fraud. It also needs to be remembered that there are costs for all crime prevention efforts and an optimum level (which will vary, depending on priorities and circumstances) beyond which diminishing returns render further investment impractical. There will inevitably be some `acceptable' level of payment card fraud, whether this is made explicit or rather shown in the behaviour of financial institutions, retailers and the CJS. Given the complexity of the crime, the variety of methods involved and diversity of points of compromise, the approach most likely to yield the best returns on investment is a number of initiatives targeted at specific `weakest links' in the process: these may change over time and will have to be re-examined regularly.

When implemented, the roll-out of chip cards and readers is expected to curtail fraud at the most fraud-prone locations (UK merchant, card present). However, (in the short term at least, unless there is widespread introduction of computer/telephone chip readers for the purchase of high risk product lines) it is unlikely to make any difference to card not present transactions and to non-UK transactions where chip-reading equipment is not installed. The latter problem is being addressed by the introduction of a card security code and by on-line checks on cardholder information for CNP transactions. A relatively small proportion of fraud takes place at ATM cash dispensers (where a stolen card is useless without its associated PIN), and even less at bank counters (which better quality CCTV has made a riskier environment for the fraudster). At a cost, plans to introduce PIN authorisation at point of sale terminals in conjunction with chip cards should significantly reduce the losses from counterfeit cards here. The key is to make fraud risks manageable and containable, and to have an implementable, flexible reserve response strategy should there be a major breach.

Attempts to address the issue of plastic fraud have, in the past, necessitated co-operation across a number of traditional organisational boundaries. This will continue to be the case. This complex environment involves a much broader set of stakeholders than is commonly appreciated outside the industry. It includes card issuers and retailers with different stakes in existing technology and some proprietary systems that cannot simply be grafted onto; merchant acquirers who process transactions on cards; credit reference agencies and others such as CIFAS who screen applications for cards; the global card networks such as Visa and MasterCard and American Express; domestic card networks such as Switch; and others. 11 Containing the rise of fraud in an expanding supply market characterised by new entrant card issuers with targets to hit and by competition between only modestly profit-making merchant acquirers places many obstacles in the way of security enhancement by consensus. Within the financial sector, the notion that `fraud is not a competitive issue' has been widely promoted as a binding cultural theme, and the Plastic Fraud Prevention Forum (PFPF) under the umbrella of the Association for Payment Clearing Services (APACS) has facilitated communication and co-operation between a variety of stakeholders since 1990. In our view, even though the

benefits of collective fraud prevention may benefit new and smaller entrants disproportionately, the re-energising of such action is important to sustain. However, maintaining public confidence in the medium has to be a major concern of the card industry, and this may inhibit necessary action because of fear of negative publicity, especially on the part of a technophobic media seldom willing or able to treat risk sensibly.12

Despite all the improvements in industry MIS, the complexity of actual frauds is hard to code and recapture. It is difficult to see for example how best to categorise fraud on a card that was stolen from a victim's wallet, fraudulently used to make a purchase at a department store, to order computer equipment by phone and then had the account information `skimmed' and re-encoded on another card and again used fraudulently to top-up a mobile phone's call-time. This would cross the categories of Lost/stolen, counterfeit and CNP. Comprehensive and mutually exclusive categories are characteristic of an efficient taxonomic system, and although this is a particularly complex, multidimensional field, it might be worth reconsidering the categories used to analyse fraud, to enable tracking of the multiplicities of abuse of particular cards, which may tell us something about changes in offender networks and skill sets.

To rely on a single system or measure of prevention, no matter how sophisticated, is courting disaster and a mixed package ofprevention measures will remain necessary. The CJS, payment card industry and retailers will need to keep pace with technological advances in order to meet yet unanticipated threats with rapid, adaptive responses. The following problems all need to be addressed and regularly reviewed.

Card authentication

Although cards are already equipped with various security features (such as holograms, embossing, micro-printing) which ensure that making an exact copy of a card is difficult and expensive, they are not necessarily an effective means of preventing counterfeiting. Such refinements on cards might be difficult to replicate, but in order to be accepted, a counterfeit needs only to surpass a minimum critical threshold of credibility, the level of which will vary extensively depending on the training, vigilance and motivation of p.o.s. staff.

Spotting counterfeit cards is not a trivial issue, with so many different issuers and varieties of cards in circulation. One issuer's training material for p.o.s. focuses on ten different features for staff to check. Focusing on more objective recognition of a smaller number of identifiers which are most difficult and costly to counterfeit might be more effective than loading an excess of imperceptible features on to the card and requiring these staff to perform such a cognitively and perceptually challenging task. The vigilance of p.o.s. staff needs to be encouraged but more importantly, their capability needs to be strengthened. Cards carry a motif which is visible only under ultra-violet light and a recent initiative involves supplying small light units to retailers to check for the presence of this motif. There is also some

investigation of small units that can be used to verify the validity of the hologram on the card. Objective checks such as these are preferable to subjective judgements that are more likely to lead to confrontation and unnecessary customer alienation, on the one hand, or to an excessive reluctance to challenge, on the other. Devolution of policing responsibilities to p.o.s. staff, requiring them to confront and apprehend offenders, raises its own problems,[13] but a more thoroughly established protocol for denying card authorisation, retaining the card and ensuring any reward reaches the person who captures it might be expected to add to motivation for vigilance at this critical point. Admittedly, most cards (though we are not aware of any break down data) are `detected' by systems rather than by the personal vigilance of retail staff, but it nevertheless seems appropriate and effective to us that the individual (rather than the firm) who captures a card should receive the reward personally and promptly. Rewards to the value of £ 10 million were paid out in 2000 and - though there is no evidence of abuse - some kind of monitoring of the number and frequency of rewards to particular individuals should be undertaken to identify possible collusion so that rewards for captured cards don't become another source of income for fraudsters.

Shortening the period of fraudulent use of lost/stolen cards has been facilitated by authorisation and hot-card files, the proportion of fraud that occurs after a card has been blocked has fallen significantly from 70 per cent in 1991 to 40 per cent in 1996, and 20 per cent in 1999. Informants tell us that the velocity of fraudulent card use has increased and that fraudsters, only too aware that there is a narrow window of opportunity before a card is blocked, have adapted their behaviour accordingly. The process of authorisation is also costly (telecommunications and slowing down of transactions) and there is an optimum level beyond which authorisation or screening costs outweigh the fraud savings. Nevertheless, short-term cost benefit analysis can leave the opportunities open to a blitz on particular risk-prone areas, so in the current environment of rapidly rising fraud, particularly on CNP transactions, there is a tendency to set the rate of authorisations as high as possible in fraud prone sectors.[14] Finding a more effective way of encouraging cardholders to be more vigilant with their cards and promptly report cards that are lost or stolen potentially could help here, though `skimming' card information for subsequent counterfeit leaves the cardholder unaware that their account is being misused, as they can still be in possession of the card. In this sense, the link between what normally would be regarded as `capable guardians' and fraud reduction is lost, and business must fall back upon its own internal resources to effect guardianship.

A more secure p.o.s. environment is likely to be generated once acceptable incentives have been developed to permit implementation of anti-counterfeiting measures: this is a commercial issue and not one for us to contribute to in this context. Full chip card implementation is currently envisaged by 2003 and the card industry's collective position is that (as has been the case in France) once a mature `chip and PIN' environment is established, then there will be no fallback procedure (if the chip transaction fails, then the transaction on the basis of the

magstripe information will not be accepted on that card.) This will require a robust chip card system and comprehensive installation of p.o.s. equipment. Some of the market dynamics differ between the UK and France, and some dissidents in the industry are convinced that fallback procedures will continue to operate for some time. 15

The card schemes intend that incentives for the implementation of both chip cards and terminals will involve a shift in the liability for the fraud to the least protected party. If the card issuer has implemented chip enabled cards but the retailer is not using chip reading terminals, then the retailer should carry the cost for the fraud, and vice versa. The implementation of chip cards and readers at p.o.s. is already underway, and the shift in liability is due to come into effect from 1 st January 2005. The prevention gap in `card not present' situations and where chip-reading equipment is not installed is being addressed by the introduction of the use of a card security code and on-line checks on cardholder information for CNP transactions (CV2/AVS).

Cardholder verification

The fact that a genuine card is presented for a transaction is of course, no guarantee that the person using it is the rightful cardholder. The value of signature as a direct prevention device rather than an (unquantifiable) deterrent has been questioned sufficiently for various alternatives/additional checks to have been considered. Although chip cards would facilitate a biometric alternative to the signature, none is expected to practicable for at least a decade. The use of fraud detection systems such as `Falcon' and others to model the typical spending behaviour of individual cardholders and to monitor on-line authorisations for unusual spending patterns which may be predictive of fraud has been very successful, and is vital in dealing with abuse of cards that have not been stolen as well as of stolen cards that have not yet been reported. The further development of such systems and their rate of utilisation is a cost-benefit decision for card issuers and requires readjustment in the light of losses.

There is no doubt that the PIN is a more effective check than signature on unauthorised transactions, but requires conversion of p.o.s. technology and retailer collaboration. Furthermore, the facility of changing one's issued PIN to a more memorable one is widespread and is convenient for cardholders. Hopefully, the new system will maintain this facility. If cardholders have a number of cards, (as is common) remembering many PINS may prove to be a problem. With sophisticated technical systems, the weakest link is often human error and more might be tempted to write their PIN down, increasing the risk of compromise not just for that card but for the range of cards they carry with them.)

Though the net effect is likely to be overwhelmingly positive and projected result in a considerable reduction of fraud, there are some concerns (and anecdotal evidence from countries where it is used) of unwanted side-effects of the introduction of PIN at p.o.s. There are reports of cases of criminals `shoulder surfing' in supermarket checkout lines to note the

PIN number entered on the keypad and then signalling to accomplices to steal the victim's card, and as observed earlier, personal threats against cardholders to divulge PINs may be expected to increase, and may be hard to distinguish from first person frauds with invented excuses. Details such as the procedures if a card is blocked after failed attempts at entering the correct PIN (which might easily happen if cardholders are required to remember a number of different PINS for different cards) are not yet decided. Confirming a transaction by entering a PIN is likely to be faster than using a signature, though whether or not the entire transaction time is increased or decreased by using PIN and chip, there will be some issues of compatibility of systems that will need to be addressed, and currently have not been resolved. The industry is also implementing a system of using a `card security code' and verification of cardholder information (CV2/AVS) to deal with CNP fraud which it is envisaged will curtail the rise of this kind of fraud, if not reduce it in absolute terms.

Applications fraud

Verification of the identity of an applicant for a card is the essential issue. The moves that have been made to share information for identity matching for fraudulent applications for cards should be continued. (It seems reasonable to assume that once the necessary knowledge and skill to obtain cards in this way have been acquired, they will be used repeatedly.) CIFAS reports having saved the banking and credit card industry £78.6 million of fraud in 2000 by spotting suspicious applications for cards. Some card issuers (for example, MBNA, Marks and Spencers, American Express) require cardholders to activate the card using some form of identification. Applying for cards by telephone reduces the risk for the fraudster and makes this a more attractive source of cards. Training card applications telephone staff to elicit and distinguish verbal cues to deception, though problematic, may have incremental utility over and above the CIFAS system for applications from those not recorded on the system. We are not in a position to evaluate new technology like `Truster' and `Absolute', intended to identify stress points in oral conversations, and it should be remembered that there are no universal physiological or behavioural correlates of deception.

Identification of points of compromise

The evidence so far suggests that points of compromise for the `skimming' of cards generally follows urban population centres and the great majority of `skimming' of card numbers for has been so far been identified as taking place at petrol stations and restaurants (though, this could easily change). Warning customers of particularly risky kinds of location might be a sensible approach, as maintaining universal vigilance is unlikely.[16] Although MIS can identify common purchase points which suggest potential points of compromise, (though adequate identification of merchants necessitates a more complete and accurate database at the individual store rather than chain headquarters level), speedy action (perhaps via a pooled investigative resource such as the FIB within APACS or by the card schemes) is required to investigate and prosecute collusive merchants.

The problem of collusive merchants who act as a conduit for fraudulent transactions has been addressed by the National Merchant Alert Service which tries to identify dishonest merchants and keeps a database of 'struck-off' merchants. In some cases of fraud on the Internet it is difficult for the acquiring banks to identify merchants, as some use `consolidators' to pool transactions. There is scope for additional scrutiny by merchant acquirers to identify merchants who generate disproportionate rates of fraud, though the simple fact of a greater amount of fraud than would normally be expected does not always allow identification of the individuals involved, as many retail outlets have a number of staff with high rates of turnover, some of whom may be serial fraudsters at successive sites as well as being connected through ethnic or other networks. The growing trend of international fraud (predominantly in France, Spain and the US) puts a strain on efforts in this direction, though. As global e-commerce develops there will be a growing need for a coordinated European or global level merchant alert file, requiring banning orders on fraudulent merchants to be implemented across jurisdictions. Making retailers/merchants more aware that systems are in place that identify disproportionately high fraud rates and potential consequences of this such as being struck off may also serve as a deterrent, subject to the need to keep monitering criteria secret.

Legislation and policing

The priority given to police investigation of plastic card fraud differs in different parts of the country: not all forces currently have dedicated cheque/plastic card squads. [17] Although plastic card fraud is difficult to police, leaves little if any forensic evidence, may involve a trail of offences that cross police authority boundaries, unless there is a realistic risk for offenders of being apprehended and, if convicted, receiving a sentence that is significant to them and to others, then it seems unlikely that the cost-benefit analysis of the criminal would lead them to give up on the activity. Not only at the level of the Hi-Tech Crimes Unit do changes need to be made in the abilities of the police to handle technological changes in the organisation of thieving. As time advances, low-tech crime will increasingly be the province only of the less skilled among the socially excluded, and it is essential that the CJS keeps pace with technological and other advances, in detection and investigation as well as legislation. Policing requires appropriate training, equipment, resources and structures. There is a growing trend for payment card fraud to cross national boundaries and, looking forward there seems little reason to suspect that this will diminish. Organisational structures and systems may have to change in order to adequately deal with this problem. It might be a useful exercise to survey police cheque and credit card squads to ask them what kind of co-operation or help they would ideally want from overseas governments and police forces in order to more effectively police card fraud.

In 1999, Interpol headquarters established a card counterfeit collation and distribution centre, funded by sectors of the industry internationally, currently, American Express, Discovery (a

US card issuer), MasterCard International and Visa International. Interpol have set up a secure, very high picture resolution Internet site - accessible by password to authorised persons only - into which details of counterfeit cards, counterfeiting equipment and recovered cards are fed. Each item is analysed, series are grouped together, and if there is one feature that is different (for example, the hologram), then it is given a new identification number even though other features may be common to other detected counterfeits. One can see any other card and search on any particular features for others. Both the industry and the police send information in, and the separate law enforcement database enables the law enforcement bodies (but not the private sector) to review the intelligence that relates to the cards and equipment. This is a quality speedy input and dissemination system that improves the capacity of the authorities to deal with card counterfeiting more effectively: the extent to which it used depends on how much resource the individual police forces wish to put into tackling the problems, but after a sceptical start, interviews suggest that it is being used more often for cross-referencing cases on a global basis, and for pooling intelligence about card design. This has not only made the collation of criminal evidence easier and more coherent, enabling crimes in different countries to be put together, but also has made preventative intervention quicker, since commonalities can be spotted earlier and - where nation states can be cajoled into action - the evidence can be used to justify taking out counterfeiting plants and other resources for crime. There is a sense in which the industry could do this collectively itself, but the component of police action - and especially multi-national action - would then be missing, so it is in both parties' interests to operate this system.

Criminal behaviour

Those who successfully engage in plastic card fraud on any significant scale are generally bright, entrepreneurial and innovative. They have demonstrated an ability to operate adaptively and respond to initiatives aimed at curtailing their activities. There seems no reason to doubt that this will continue to be the case. As long as the opportunities exist, the activities will continue. Although technological advances can certainly be a source of fraud prevention tools (chip cards, fraud detection systems etc) they can also provide tools for the fraudster to circumvent prevention measures (cheap, portable 'skimming'/re-coding devices, electronic transmission of compromised/'skimmed' card numbers across continents, etc). It is important to focus efforts at detection and prevention on weak points in the system and to re-analyse and refocus prevention measures adaptively as well as being proactive in anticipating new threats and developing new security measures before the old ones are compromised.

Displacement between kinds of fraud might seem to be a potential problem as one target is hardened, another becomes a relatively more attractive proposition. But reviewing the pattern of plastic fraud by category does not seem consistent in general terms with this line of argument. Whether criminals' decisions about their activities (what, where, when, how and how often etc) follow rational decision-making, ' satisficing'[18] or optimal foraging principles,

we would predict that displacement is most likely to occur between crimes that have some overlap in requisite criminal skills, knowledge and social networks and in the direction of `line of least resistance' in terms of potential risks and benefits: in other words, we have to look at those areas that are closest in cognitive capabilities, contacts and technology to the particular type of payment card fraud that we are trying to deal with. Some components of payment card crime - the resale of fraudulently obtained goods - are universal; some are common though with individual variations dependent on personal plausibility - use in Harrods versus use in Woolworths; and others are much more varied - forming a dummy company to process fraudulent transactions, or setting up a card counterfeiting factory. Though changing economics might lead to a shift in the popularity of different kinds of fraud. Investigators tell us that the cost of a good quality counterfeit card has dropped from about £700 three years ago to £50 today, possibly driven down by criminal market forces of supply and demand, with competition amongst those producing counterfeit cards; and sources suggest that the market value of `skimmed' card numbers can vary between £5 and £25 per number.

Costs of card fraud

Although it is not possible to document comprehensively how all the costs of plastic card fraud are distributed,[19] it would be a mistake to focus only on the more easily measurable such as the monetary losses suffered by financial institutions and retailers and to ignore other meaningful societal and individual costs that are more difficult to count. There are a number of ways of calculating the costs of card fraud: the number of cards stolen; absolute fraud loss figures (though some proportion of what is currently categorised as `bad debt' might add to these figures), the proportion of fraud to turnover and the proportion of fraud to profit (which may be the most significant factor in moderating card issuers' view of the trade-offs between increasing card use and opportunities for fraud). Measures which are harder to estimate and may be impossible to adequately quantify include: the fear of fraud; increased prices and/or interest rates; the consequences of the proceeds of fraud being used to finance other crimes; and the impact on the cardholder of being impersonated (and perhaps feeling violated and that their good name has been tarnished). Nevertheless, these deserve serious attention. The British Crime Survey reports the following emotional responses to burglary (in descending order): anger, shock, fear, difficulty sleeping, and crying/tears. To the best of our knowledge, similar research has not been conducted on victims' responses to having been impersonated in card fraud, though our informal interviews suggest that at least some find the experience of knowing that there is someone impersonating them and committing fraud a deeply disturbing thought.

Some research has been conducted on cardholders' card use following their impersonation in fraud. (Though there are methodological difficulties in making sensible comparisons here). There are complex and somewhat conflicting results, with some suggestion of a bimodal

distribution of behaviour, with some cardholders using those cards less than before and some using them more than before. There might be a number of reasons for this: increased use might be an attempt to re-establish their good name; they might be reassured (if the issuer perhaps spotted the fraud before they did and by the way the retailer dealt with them); decreased (or ceased) use might derive from anger at being, charged on their statement with costs that they have not incurred; and diminished confidence in the card issuer and/ or in the payment card system. They might not understand how the fraud could be due to a criminal if their card has never left their possession and so blame the card issuer or the system. If they do understand that their card information could have been compromised and that someone could be impersonating them even though they are still in possession of their card, they might feel that their identity has been violated. Further research would be needed to illuminate these findings and these should not simply measure spending behaviour, but a wider range of potential effects on the individual.

The involvement of organised crime networks and groups in payment card fraud presents some subtle difficulties. No data exist or plausibly can be generated about the proportion of such frauds that are committed by crime groups rather than the relatively autonomous behaviour of individuals meeting up, if at all, quite casually. To the extent that crime groups can be inhibited by more general moves against them, whether legislative (changes in conspiracy law or proceeds of crime forfeiture) or more ground-level (providing better inter-force linkages for crimes below National Crime Squad thresholds but above those that comfortably can be dealt with by divisional CID) then there is some scope for optimism, and more use might be made of dealing with payment card fraud as part of a tactical response to crime groups, even if the police do not rank the crime very seriously. Overall, though we do not find `Wars on Crime' to be a helpful metaphor, both the sectors of industry and commerce and the police, assisted where appropriate by government, need to continue with their data-driven dialogues, constantly updating tactics in an interactive crime reduction process. If this paper does not propose any `Big Bang' solution, it is because the underlying themes and causes are complex, and the industry has a long history of incomplete proposed total solutions - such as biometrics - which have not been robust enough or cheap enough to merit adoption. The struggle for better and quicker data, and the energy to act should continue to drive fraud costs well below their `natural' level: this is a worthy enough aspiration, even if it is unsatisfyingly undramatic.

5. Summary of discussion

Payment card fraud needs to be addressed as a number of related activities with quite different modus operandi and skill requirements rather than as a single, unitary phenomenon. The complex, dynamic and adaptive nature of this crime render present or future reliance on a single method of fraud prevention (no matter how seemingly secure) inappropriate. Furthermore, existing prevention measures need to be maintained and regularly reviewed to prevent the frauds that prompted their implementation from springing up again.

Card authentication: New measures are currently being implemented to tighten up security, though issues of sharing costs and liabilities between stakeholders will need to be resolved. Fraudulent use of cards can be blocked by retail staff and on-line systems, though devolution of policing to point of sale staff raises its own problems and objective checks are preferable to subjective judgements. Cardholder vigilance in safeguarding their cards from loss, theft or compromise should also be encouraged.

Cardholder verification: Determining that a transaction is being conducted by the legitimate cardholder is an important safeguard in preventing fraud. As biometric identification systems seem likely to remain prohibitively costly for implementation at a great number of retail locations for some time, this issue can be addressed by current plans to move towards secure PIN entry system which will replace more easily forged cardholder signature. The introduction of a card security code and use of cardholder information to verify transactions will go some way to addressing this problem for transactions where the card is not physically present (telephone, mail order and e-commerce).

Applications fraud: Information sharing between card issuers is a valuable precaution which makes multiple fraudulent applications more difficult and should be continued. Card `activation' on receipt by the genuine applicant is used by some card issuers and might be considered by others. Telephone applications for cards provide a relatively low risk environment for fraudsters (though receiving cards will remain a problem for them). Staff training may help to address the identification of fraudulent applications, though it should be remembered that there are no completely reliable vocal indicators of deception.

Identification of points of compromise: Refinement of Management Information Systems could allow more precise identification of points of compromise. Cardholder vigilance would be enabled by warning of particularly risk-prone locations. `Merchant

alert' database systems could be extended to operate on European and global levels to identify 'struck-off merchants and facilitate banning orders on fraudulent merchants to be implemented across jurisdictions.

Legislation and policing: A consistent, dynamic and adaptive approach (both at a national and international level), with well-developed communication networks and collaboration between all stakeholders is required to adequately deal with the numerous challenges for policing and legislation presented by payment card fraud. Ways of making resources available for this need to be explored.

Costs of card fraud: The significant financial losses incurred as a result of payment card fraud are already well documented. Beyond these, there are individual, organisational and societal costs which need to be researched and taken into account in the planning and development of future prevention and harm reduction measures.

References

Attorney General's Office, Lord Chancellor's Department, Home Office (2001) *Criminal Justice: The Way Ahead.* Published jointly by the Home Office, the Lord Chancellor's Department and the Attorney General's Office (February 2001).

Department of Trade and Industry (2000) *Turning the Corner.* Report of the Foresight Crime Prevention Panel

Home Office Research Development and Statistics (2001) *Recorded Crime England and Wales, 12 months to September 2000* London: Home Office

Government Actuary's Department (1998) *National Population Projections*

Home Office (2000a) *Review of Crime Statistics: A Discussion Document.* London: The Home Office (July 2000)

Home Office (2000b) *The 2000 British Crime Survey England and Wales.* Home Office Statistical Bulletin 18/00. (October 2000).

Home Office (2000c) *Criminal Statistics in England and Wales. Statistics Relating to crime and Criminal Proceedings for the year 1999,* London: Home Office (December 2000)

Levi M and Handley J (1998a) *Prevention of plastic card fraud,* Home Office Research and Statistics Directorate Research Findings no.71. London: Home Office.

Levi M and Handley J (1998b) *The prevention of plastic and cheque fraud revisited.* Home Office Research Study 182. London: Home Office Research and Statistics Directorate.

Levi M, Bissell P and Richardson J (1991) *The prevention of cheque and credit card fraud.* Crime Prevention Paper 26. London: Home Office.

Levi M and Pithouse A *White-Collar Crime and its Victims,* Oxford, Clarendon Press. (Forthcoming).

Mativat F and Tremblay P (1997) `Counterfeiting credit cards. Displacement effects, suitable offenders and crime wave patterns'. *British Journal of Criminology, 37,* 2.

Endnotes

1 Though part of the rate of growth rise is a statistical artefact due to the lower start base for debit cards.

2 Though this may well change if and when e-commerce accounts for a more significant proportion of payment card transaction volume.

3 The high failure rate among dot.com start-ups and the fact that we are all still in our current employment suggests that our faith in predictions is at best tempered with caution about outcomes.

4 However, if these assumptions are over optimistic, the level of fraud could easily be far higher than this.

5 Projected to be around £154 million by 2005 (and £103 million with PIN).

6 See, for example, Department of Trade and Industry, 2000 and *Criminal Justice: The Way Ahead.* Published jointly by the Home Office, the Lord Chancellor's Department and the Attorney General's Office. (February 2001).

7 The proportion of such clear-ups that are due to `secondary detections' confessions by those already apprehended, is unknown.

S It is commonly believed that there is large-scale `organised crime' involvement in plastic fraud, though evidence of the nature and scale of organisation is difficult to come by and definitions of `organised' in this sense arc fairly loose and varied. There is clearly a need for more research into the organisation of plastic card fraud.

9 Home Office Review of Crime Statistics: A Discussion Document (July 2000). Recommendation 16: *'The Home Office with the Serious Fraud Once should develop new routine information on fraud, in co-operation with the banking and insurance industries. '*

10 Recommendation 59: *' The main thrust of the analyses of crime statistics... ...should be directed towards topical ad hoc concerns and problem-related studies. and not the release of statistical tables repeated from one rear to the next.*

11 Though CIFAS is involved in preventing credit fraud more widely, not just payment card fraud.

12 One major credit card company is reported to have instructed shops that had experienced fraudulent use of its cards not to report this to the police. Whether this was to prevent potentially damaging publicity or concern not to overburden the police with cases that had no realistic possibility of successful investigation, it would bias recording of the figures. *(Home Office - Review of Crime Statistics: A Discussion Document (July 2000) pp. 29-*30.)

13 We appreciate that violence to staff is an important issue in the retail industry, but there are no industry data on the extent of violence against staff in this particular context. We recommend that, if possible, such data should be collected in future.

14 Though this will have limited utility for blocking the use of `skimmed' cards whose owners are oblivious to any compromise until a statement arrives listing fraudulent transactions that they have not made. Monitoring physically impossible combinations of transaction activity (for example, temporally contiguous transactions at geographically distant locations) might be one way to speed up the detection of such fraudulent use.

15 It seems rational to us that judgements will need to be made on the balance between the costs and benefits of prohibiting fallback procedures and these may well differ in different retail sectors, between card issuers and across a range of other circumstances.

16 Though clearly the obvious alternative for the cardholder (use cash) is anathema to the card industry.

17 Only 22 out of 35 respondents to consultation in England and Wales and four Scottish constabularies.

18 adequate to meet immediate needs but neither necessarily maximising nor optimising the potential gains.

19 It is certainly possible to argue that the customer ultimately picks up the bill - in terms of increased prices of goods, services and interest charges.