HOME OFFICE RESEARCH AND STATISTICS DIRECTORATE

RESEARCH FINDINGS No. 71

PREVENTION OF PLASTIC CARD FRAUD

Michael Levi and Jim Handley

As a result of a review commissioned by the Home Office on what might be done to reduce fraud, several recommendations were adopted by the credit and cheque card industry. The study reported here examined the impact of these measures alongside others taken by the industry and the police. Future trends and the extent to which business and the police are geared up to meet them are also examined.

KEY POINTS

- Plastic fraud fell from £165.6 million to £97.1 million between 1991and1996. As a proportion of card turnover, fraud levels dropped from 0.38% to 0.09%.
- Identity checking and matching with known previous frauds has cut fraudulent applications.
- Secure card delivery to identified high risk areas has cut fraud on stolen unsigned cards.
- In shops, lowering the maximum allowed without authorisation and more electronic authorisation/ 'hot card' files have cut fraud after cards have been reported stolen.
- Modelling of customer transaction patterns has helped banks identify and prevent fraud before customers notice their cards have been stolen or copied.
- Public-private policing co-operation has led to successful international prosecutions of counterfeiters.

Between 1988 and 1990, the cost of cheque and credit card fraud rose dramatically, from £69.3 million to £150.3 million. A review of what might be done to reduce fraud made recommendations which were largely adopted by the plastic card industry (Levi et al.,1991). The follow-up study reported here examined the impact of these measures. 'Plastic card' is used to include charge cards, cheque cards, credit cards and debit cards. Plastic card fraud fell substantially during the 1990s. As can be seen in Table 1, it almost halved in 1995 compared with 1991, then rose to £97.1 million in 1996 – still less than two-thirds of the 1992 peak.

Reduction of plastic fraud is desirable because it:

- reduces the direct financial losses suffered by card-holders, issuers and retailers
- improves public perceptions of the integrity of the system
- increases the acceptability of automated banking systems.

Reducing the range of opportunities to offend is the key to success, particularly when all those involved act together as 'capable guardians':

- card issuers
- merchant acquirers (those who license traders to accept cards)
- retailers.

The scale of savings represented in Table 1 is even clearer when the ratio of fraud to turnover on sales of goods is examined – from 0.38% to 0.09%. Projected losses were calculated using the ratio for

Table 1 Projected savings from fraud prevention measures during the 1990s

	1991	1992	1993	1994	1995	1996	
	£m	£m	£m	£m	£m	£m	
Total plastic fraud losses	**165.6**	**165.0**	**129.8**	**96.8**	**83.3**	**97.1**	
Fraud losses (excluding cash)	153.3	153.0	120.5	89.7	75.0	88.8	
Non-cash fraud as a percentage	%	%	%	%	%	%	
of non-cash turnover	**0.38**	**0.32**	**0.22**	**0.14**	**0.10**	**0.09**	
Projected non-cash fraud losses	£m	£m	£m	£m	£m	£m	
(at 1991 rate of 0.38% turnover)	153.3	181.4	207.6	243.3	287.0	356.3	
Difference between actual and							Total
projected loss		**28.4**	**87.1**	**153.6**	**212.0**	**267.5**	**748.6**

Note: Plastic transactions and fraud involving cash on conservative grounds have been eliminated because the rate of Automated Telling Machine and 'over-the-bank-counter' fraud is much lower and creates an artificially large 'benefit'.

1991 for the subsequent years and the bottom line in Table 1 shows the difference between actual and projected loss for 1992 – 1996. This amounts to a total 'saving' of £748.6m by 1997.

How have these fraud reductions been achieved? Changes in institutional recording practices and in the underlying rates of crimes (such as burglary or theft from cars) do not explain significantly this drop in fraud or the recent upwards trend, which is expected to continue.

CURRENT ANTI-FRAUD MEASURES

Some existing mechanisms for fraud prevention are discussed below. Measures relate to different aspects of the credit card process:

- the card issuing stage
- card production and distribution and security device improvements
- actual retail card-use
- policing.

The card issuing stage

The search for discrepancies in multiple fraudulent applications (i.e. multiple applications for credit from different sources by the same person/persons) has been helped by improved technology and participation within the card industry and right across the credit-granting industry. The Credit Industry Fraud Avoidance System (CIFAS) has an on-line computer file which lists frauds on specific names and addresses. During 1997, 31,107 frauds on banks (of which half were attempts) and 28,221 frauds on retail credit (of which a quarter were attempts) were reported. Members reported direct prevention benefits of £21.3 million in banking and £9.4 million in retail credit from these checks for 1997 alone (excluding the small cost of membership and the greater cost of staff time in processing reports). Commercial systems such as Experian's Detect have reduced multiple applications fraud across different industry sectors. The real effect may be greater because repeat offenders may not attempt such frauds at least until controls are relaxed.

Card production and distribution

'Card not received' fraud has fallen from £32.9 million in 1991 to £10 million in 1996, outweighing the cost of data analysis and courier services. This is due to better identification of 'risky addresses'. Cards are then securely delivered or card-holders asked to collect them.

Physical security devices have been improved to make counterfeiting more difficult. For example, use of laser-engraved photographs and signatures makes impersonation harder. Fraud on Royal Bank of Scotland cards, with engraved signatures and photographs, has been reduced substantially. Their cost effectiveness is enhanced by taking into account the cost of action against fraud, reduced disputes with retailers over signatures (which can be retrieved easily from the database), and the elimination of tampering with signature strips.

The retail card-using stage

Steps taken have included:

- improved modelling of individual card-holders' expenditure patterns. This helps to identify possible fraudulent transactions made after cards are stolen or when genuine cardholder details are used to create counterfeit cards ('skimming'). Card-holders can be contacted to verify transactions

- increasing the proportion of card transactions needing authorisation from issuers (from 10% in 1991 to 45% in 1996) by lowering the maximum allowed without authorisation, using financial incentives to retailers to implement the technology

- increasing card-issuer participation in 'hot card' schemes such as CardClear and improving technology to transmit lost and stolen card data electronically and rapidly to retailers. This has reduced frauds occurring after the card has been reported lost or stolen from 70% in 1991 to 40% in 1996. Cheque card fraud dropped markedly when

Transax Equifax obtained stolen cheque and card data from more banks

- greater control of fraud committed by or in collusion with merchants. This includes better checks on national VISA-administered databases of 'struck-off' merchants and merchants' fraud rates

- improving liaison and education campaigns with press, retailers, cardholders and police ('Card Watch').

Fraud at retail point of sale was reduced from £124.1 million in 1991 to £60 million in 1996 as a combined effect of these measures.

Policing
This has been the area of least progress in dealing with plastic fraud. Modest efforts to develop fraud intelligence – mainly relating to cheques – and some major intelligence-led investigations of 'organised crime' networks have led to convictions of some high-rate offenders. But currently there are 'cheque squads' in only 25 out of 43 police forces, and many deal only with intelligence collation and with cheques rather than plastic fraud.

SUGGESTIONS FOR FURTHER PLASTIC FRAUD PREVENTION

Prevention measures may work best in a variety of combinations, and increased reliance on technology makes it necessary to continuously develop contingency plans in the event that the technology is compromised. Measures suppress fraud but levels soon rise dramatically if measures are relaxed. Though still a modest proportion, counterfeiting and telephone/mail order fraud have been and are expected to be the fastest growing areas. Although cross-border fraud has a great deal of potential risk, its incidence has been static and most 'plastic criminals' prefer to use cards locally or regionally, for convenience and predictability.

Some key approaches to combating plastic fraud involve action by card-issuers, retailers, the police – in partnership with issuers, acquirers, card schemes and merchants – and the government.

Suggested action by card-issuers:

- further tightening of controls over potentially fraudulent addresses and data-matching, subject to data protection principles, as well as providing user friendly analysis to reduce risk on speedy credit decision-making

- continuing proactive monitoring of account behaviour, as the shift towards fraudulent use before the card has been reported stolen (pre-status fraud) increases

- training telephone credit application and authorisation staff to spot incongruities or inconsistencies in callers' statements and thus identify potential fraudsters

- encouraging greater care by card-holders through industry-wide agreements. For example, charging for a replacement after the second or third loss – even if this does run counter to the 'report early' advice. Card-holders could be reimbursed if they find their original card subsequently. Continuing warnings about the risks of leaving cards in high-risk locations such as cars

- improving Management Information Systems to help focus educational and technical efforts on the highest risk geographical and business sector areas. Refined store and individual level data on where stolen cards are most likely to be used would help concentrate attention cost-effectively on local anti-crime initiatives such as robbery prevention

- forming a centralised 'rapid response' group seconded from the card industry and the police. It would deal actively with emerging attacks on smart card systems, pool cases of 'skimming' and liaise with the police and, possibly, high-risk retailers. There should be continuous monitoring of the Internet to reduce the risk of 'phantom' firms capturing card-holder details for later counterfeit use – the card schemes (Visa, MasterCard, and American Express) should also be involved.

Joint action by card issuers and retailers:

- methods of identifying the card-user more closely with the valid card-holder at point of sale should be developed, e.g. the Card-holder Verification Mechanism. A point-of-sale check against personal data on the new chip card could prevent fraudulent transactions and leave forensic evidence for automated search and proof in court. Iris-scans, voice-prints, digital signature verification and PIN at point of sale can be used as prevention but are less useful than fingerprints for search and arrest, since they are not included in police records

- methods of identifying those who order goods and services in 'Card Not Present' situations such as telephone and mail order purchases could be developed. At the least, purchasers should have to quote their unique identifier (CVC2/CVV2) numbers from the card

- enhancing store-staff awareness, including local supermarkets and off-licences. This could reduce the scope for fraudsters' attempts and therefore losses per card

- subject to data protection rights, helping to identify and generate evidence against staff-fraud, which may require video and/or manual surveillance

- rewarding the vigilant and those who prevent the greatest losses, with praise and/or with money. Incentives should apply at the point where they are most likely to have an impact, i.e. the actual store-staff member, as soon as possible after the incident. Alertness in identifying mismatches between the number on the front of the card and the electronically produced card receipt number should be rewarded by more than the usual £50

- increasing 'hot card' capacities and more widespread sharing of 'hot card' files

- with the arrival of chip cards, restricting (or prohibiting) the typing-in of card details at the point of sale, to prevent the evasion of smart card protections.

The police

Following Levi et al.'s report in 1991, an ACPO working group was set up which made six recommendations. These should be re-examined and implemented where appropriate. Other suggested actions by the police in partnership with issuers, acquirers, card schemes and merchants are:

- more effort could be made to connect 'runs of use' by teams, e.g. by fingerprint, modus operandi, CCTV pictures and handwriting analysis. Proper audit trails on procedures are important, both as part of proactive investigations and in persuading local traders to store videos for longer periods than at present. Technical and cost changes in data storage should make this easier and cheaper. Such audit evidence increases the probability of guilty pleas and further savings in costs and time for witnesses

- continuing with 'arrest packages' by cheque/ bank squads. Treating plastic fraud as part of a system of financing and organising property crime can yield information on other crimes such as burglary and robbery. Unless the card-user is the original thief, police may have to use the fraudster to get to the card 'fence' who in turn may inform against the original criminal, perhaps following surveillance

- increasing risks for collusive merchants by use of informants and 'sting' operations

- liaising with high-risk retailers to arrest attempted fraudsters at the point of sale

- using local data to co-ordinate police, bank and retailer activity. In London, 20% of street robbers obtain plastic cards from victims, who can be prompted to tell the police (and find their card number). The police or victims can tell the banks to block the cards rapidly and police can ask local retailers to contact them immediately if the card is used.

Suggested action by government:

- a rational and intellectually consistent crime recording system should be implemented. Each fraudulent use of a cheque and plastic card should be treated as an individual crime in each force/division at the point of use

- some inter-force crimes fall outside the parameters of the National Criminal Intelligence Service or the new National Crime Squad, but require too much investigation to interest the average divisional or even force CID. Investigative resourcing should be encouraged for these

- prosecution difficulties generated by the current legislation relating to plastic fraud should be reviewed, and inferences from this should be integrated into general reform of the law of deception.

REFERENCES

LEVI, M., BISSELL, P. AND RICHARDSON, T. (1991) *The prevention of cheque and credit card fraud.* Crime Prevention Unit Paper 26. London: Home Office.

For more details, see *The prevention of plastic and cheque fraud revisited* Home Office Research Study No 182. London: Home Office. Available from Information and Publications Group (address below).

Michael Levi is Professor of Criminology at Cardiff University and Jim Handley is a lecturer in Psychology at the University of Glamorgan. The Association for Payment Clearing Services, representing banks and building societies, funded this study. RSD assured quality and independence of the findings.

The Research and Statistics Directorate is an integral part of the Home Office, serving Ministers and the Department, its services, Parliament and the public through research, development and statistics. Information and knowledge from these sources informs policy development and the management of programmes; their dissemination improves wider public understanding of matters of Home Office concern.

'Research Findings' are produced by the Research and Statistics Directorate. Series Editor: Carole Byron.
For further copies contact: Information and Publications Group, Room 201, Home Office, Queen Anne's Gate, London SW1H 9AT. Telephone: 0171 273 2084.

ISSN 1364-6540