27/06/00

THE PREVENTION OF PLASTIC AND CHEQUE FRAUD:

A BRIEFING PAPER

Prepared for Home Office Research, Development and Statistics Directorate[1]

Michael Levi

University of Cardiff School of Social Sciences

Introduction and Background

Inevitably, there is a tension between the provision of services in a market society and the management of crime risks in both public and private sectors. As central media of exchange in global networks, credit, debit and charge cards can never avoid the risk of crime entirely: the primary goals of corporations are profit maximisation rather than maximum crime reduction. There will always be *some* conflicts of interest between the key private sector groups – card issuers, consumers (and individual crime victims), merchant service providers, and retailers – and between individual firms within those sectors. However, the objectives of this paper are to summarise

1. The history of plastic and cheque fraud prevention efforts;

2. some of the key difficulties that lie in the way of further fraud reduction; and

3. ways in which those issues have been managed and can plausibly be improved without violating commercial rights, in the interests of all victims. (Such victims include businesspeople whose profits are cut as well as individuals whose cards or personal data lead them to become victims of burglary, car crime, pickpocketing, robbery and of identity theft or impersonation.)

This is not just a matter of cost-benefit allocation and of who suffers financially from fraud: the experience of having one's card lost or stolen is sufficiently common - over 110,000 industry-recorded cases in the year to end March 2000 - to create reasonable anxiety among customers and other members of the public, quite apart from any correct or, more commonly, exaggerated media stories about e-commerce risks which conflate fraud levels with consumer dissatisfaction over products and services purchased on the Net. Some forms of risk – the skimming of cards and identity theft – may give rise to particular anxieties on the part of citizens and those to whom they relay their experiences, some of which anxieties can be managed better than at present by card issuers and by 'not for profit' industry bodies such as the Credit Industry Fraud Avoidance System (CIFAS). These phenomena are of social as well as purely commercial interest.

[1] The Research, Development and Statistics Directorate exists to improve policy making, decision taking and practice in support of the Home Office purpose and aims, to provide the public and Parliament with information necessary for informed debate and to publish information for future use. *The views expressed in this report are those of the author, not necessarily those of the Home Office (nor do they reflect Government policy).*

Credit, Debit and Charge Card Fraud Losses 1991-99 (£million)

	Other	Card not present	Application Fraud	Counterfeit	Mail non-receipt	Lost and stolen	Ratio to turnover	Total
1991	1.6	0.4	2.0	4.6	32.9	124.1	**0.329**	**165.6**
1992	1.0	1.3	1.4	8.4	29.6	123.2	**0.292**	**165.0**
1993	0.8	1.6	0.9	9.9	18.2	98.5	**0.202**	**129.9**
1994	0.5	2.5	0.7	9.6	12.6	71.1	**0.128**	**96.9**
1995	0.3	4.6	1.5	7.7	9.1	60.1	**0.090**	**83.3**
1996	0.5	6.5	6.7	13.3	10.0	60.0	**0.092**	**97.1**
1997	1.2	10.0	11.9	20.3	12.5	66.2	**0.096**	**122.0**
1998	2.3	13.6	14.5	26.8	12.0	65.8	**0.093**	**135.0**
1999	3.0	29.5	11.4	50.6	14.7	80.1	**0.117**	**189.4**

Key Judgements

After falling by around half between 1991 and 1995, plastic fraud losses have risen steadily and are now running at 14 % more in money terms than the 1991 figure, and rising fast. In relation to the continuing growth in card turnover, the losses are less than a third of the 1991 rate, but with the prospect of plastic fraud doubling in the next two years and with recorded fraud statistics rising by a third during 1999, action is needed.

The pattern of fraud is changing. The big growth areas are in counterfeit and in fraud where the card is absent (CNP fraud). The proportion of fraud on UK cards committed outside the UK has doubled in the past decade and will soon reach a third of all losses.

The full roll-out of chip cards by 2003 will not deliver the expected benefits unless imaginative solutions are found to stimulate the more rapid take-up and activation of chip terminals. This implementation, plus devising systems and processes for verifying cardholder identity, are the two key developments with the largest potential pay-off.

Other areas worth pursuing include better cross-industry liaison over card applications, better multi-agency targeting of fraud 'hot spots' and an improved industry/police rapid response capability.

Costs and Risks of Plastic and Cheque Fraud

One can express data about the risks and impact of fraud in a number of different ways:

1. *Absolute numbers of stolen cards* (not always reliably differentiated from lost ones by victims or in issuer or police records – the fewer stolen rather than lost, the lower the recorded crime rate);

2. *Absolute fraud loss figures* (with an uncounted grey area of bad debt that may in fact be fraud by cardholders);

3. *Fraud to turnover* (in some respects a better measure because it takes into account rising expenditure patterns) or fraud per card;

4. *Fraud to profit* (which – if better data were available - would measure how much business has to be done to make up for the losses); and

5. *Fear of fraud* (by cardholders, potential cardholders, retailers and bankers), which can have a chilling effect on commercial activity or, conversely, can lead to inappropriate decisions by those who have insufficient awareness of the true risks they are taking or creating.

This logic applies to retailers as well as to card issuers and merchant acquirers (who pay the value of card transactions to retailers in exchange for a percentage of the expenditure on cards). We have little idea what the costs of crime control in this area are, since there are no industry aggregate costs, nor have the costs to police, courts and penal system been calculated: ironically, because of the low and perhaps declining resource expended in police investigations, police and subsequent criminal justice costs may be modest. What we know is that:

- Plastic fraud costs fell consistently from £165.6 million in 1991 to its 'low water mark' of £83.3 million in 1995: from 0.33% to 0.09% of card turnover. These falls were due to the considerable efforts of the card industry and retailers as a whole in sharing applications fraud data, secure card delivery to risky addresses and bank branches, and increased on-line authorisation and off-line checking against lost and stolen card files. *The key gains from these activities still hold good today and, unless relaxed, can be expected to continue to do so. It is worth reminding ourselves that at the 1991 fraud to turnover rate, the 1999 fraud losses would have been £532.6 million.*

- Since 1995, APACS card issuer fraud costs have risen consistently to £189.4 million in 1999 (0.117 % of turnover). In addition to these costs, the 1999 British Retail Crime survey indicates a one third increase to £13.5 million of retail store card fraud and charge backs to its members, application frauds of £1.6 million and cheque fraud of £12.8 million. (Cheque frauds at point of sale are charged to retailers if the sum is over the guarantee limit or signatures, etc. are deemed inadequate). Finally, in 1999, the British Bankers' Association reports £32.4 million actual fraud (up 22%) and £310.47 million *potential* loss from cheques not backed by guarantee cards (mostly under £5,000, where personal scrutiny is low and it considered not cost-effective).

- Fraud to turnover rates vary considerably, with credit cards (0.155%) and charge cards (0.139%) bearing a much higher risk than debit cards because of the much larger sums that people can expect to obtain from the former. (Fraud to turnover is 0.106 % for Visa Delta, which are international debit cards and 0.051% for Switch, which are domestic and utilisable only at point of sale). As for ATMs, except for rare serious technical faults and 'dummy terminals', risks are low because frauds can be committed only if the Personal Identification Number (PIN) is compromised, or if the card is stolen after the gang or individual has found a way of viewing the cardholder typing in the PIN at an ATM.

- Data for the first quarter of 2000 show large rises in counterfeit and Card not Present fraud. Everyone interviewed expected plastic fraud to rise substantially, perhaps doubling by 2002 due largely to greater counterfeit, CNP (both e-commerce and in unstaffed terminals) and international fraud, which by-pass many of the highly effective controls introduced during the 1990s. For example, on some mobile phone companies, fraud reached 14% of turnover in the first five months of 2000 (though part of this will be notional costs of telephone calls). Most of the higher value Card not Present fraud is charged back to the retailers, but these charge-backs are costly in administration to banks and card schemes and they aggravate retailers, who complain that merchant acquirers do not provide them with sufficient data to make good risk judgments on the identity of customers. (The latter problem is now being addressed.)

- *It would be a mistake to see the rise in fraud* ***solely*** *as a 'new economy' issu*e: fraud on lost and stolen cards went up almost as much as Card not Present fraud. In the period January to March 2000, compared with the same period in 1999, whether measured in absolute terms, per card or per turnover, fraud losses on every single card type except ATM standalone and cheque guarantee cards rose. Losses from credit, charge and debit cards all went up by 50% or more: although straight line extrapolation is dangerous, there is no reason to expect any reduction in growth rates until reduction measures are in place. Except via impersonation, higher prices and crimes committed solely for cards, the consumer is largely insulated from these costs directly: it is the financial institutions and the retailers who are the primary sufferers.

- Without further research, the 29.1% rise in the number of cases of recorded cheque and credit card fraud to 179,343 for England and Wales in October 1998—99 (of which 76,355 were in the two London areas) is difficult to explain purely in relation to changes in reporting or recording practice or in any other artefactual way. Some issuers are requiring customers to obtain a crime number before they can obtain refunds on lost and stolen cards (to try to deter frauds by cardholders themselves), but there has not been time to ascertain how common such a practice is. Other informants state that there has simply been an increase in the number of frauds and in the number of cards stolen, so the statistics reflect the real picture.

- The total fraud reduction to 1995 could not be explained by a drop in stolen card availability or by policing/offender incapacitation. The subsequent rise may owe something to an improvement in criminal market efficiency – cards which were formerly discarded may now be sold on or used for longer because of a perceived reduction in risk of police action However, there are no national data on the proportion of lost & stolen cards that are fraudulently used, which might illuminate the 'secondary card market' issue.

- Identity checking and matching with known previous frauds continues to cut fraudulent applications. Comparability over time is difficult because of the continual rise in membership of the Credit Industry Fraud Avoidance System, which co-ordinates data on names and addresses involved in verified fraud. During 1999, 36,316 frauds were identified and reported to CIFAS in the banking sector, saving an estimated £47 million, while 25,948 frauds were reported in the retail credit (including store cards) sector, saving an estimated £9 million. In addition 17,608 frauds were identified as 'first party fraud' in which the cardholders themselves were implicated. The largest growth category in applications fraud was the creation of false identities, and fraud investigators reported a considerable rise in the number of occasions in which stolen ID was used as a false identifier to get credit both from APACS members and retail credit grantors. Though the evidence for this or any other forms of fraud 'migration' – a term which, properly applied, implies a direct substitution - is modest, the industry suggests that this rise in ID fraud may be a substitute for repeat fraud using their own details this is plausible as an organised criminal response to improvements in crime control, in this case to get around CIFAS controls over applications from previous defaulters. A rise in impersonation fraud may also owe something to aggressive marketing competition, with many new entrants into the card-issuing market and with pre-approved card applications being readily used by successor tenants after their intended recipients have left. Secure card delivery to past risky areas led to dramatic falls in fraud on stolen unsigned cards. However, the recent rise may be due to fewer cards being delivered to customers via collection from bank branches, as well as new entrants failing to appreciate the risks arising from normal postal deliveries. A method of mitigating these risks is to require customer activation of new cards, at which point identification procedures can take place: this has been very successful in cutting losses for businesses such as American Express, Marks & Spencers and MBNA.. There were 6,304 new charge, credit and debit cards issued in 1999 (plus many store cards and others not part of the APACS stable) and this generates 'good' criminal market opportunities for those offering accommodation addresses and postal services as well as losses to card issuers.

- At retail points of sale, lower card floor limits and more electronic authorisation/'hot card' files have cut dramatically fraud after cards have been reported stolen, from 70 % in 1991 to 40 % in 1996 to 20% today. Since 1991, numbers of transactions requiring authorisation have doubled to 55-60% in 1999. Cheque card fraud dropped markedly when more banks provided stolen cheque and card data to firms operating electronic 'negative files' against which cheque and card transactions could be checked. The authorisation rate may increase further with the advent of chip 'smart' cards, though retailers may resist this due to the effects of such electronic communications on till through-put speed.

- Modelling of customer transaction patterns, assisted by neural network generic models such as Falcon, has helped many issuers identify and prevent fraud before customers notice cards have been stolen or copied. Issuers vary in the way that they use these models, but their use partly explains the huge high-low variations between APACS members in losses per card of all types.

- Control of fraud committed by or in collusion with merchants has been enhanced by the National Merchant Alert Service database of 'struck-off' merchants and by greater checks by some acquirers on merchants' fraud to turnover rates. (Data protection currently forbids such prevention systems in some EU countries.) However, competitive pressures and the reduction of investigative staff within some sections of the merchant acquirer industry have led to incomplete information sharing among acquirers, and this facilitates merchant fraud. Moreover, the identification and 'incapacitation' of individuals working for otherwise honest merchants requires the ability to identify *persons* as well as *'hot spots*' for Common Purchase Points for skimming, avoidance of authorisation controls, etc., and this may be difficult, especially when criminal groups or networks target employment opportunities for this purpose.

- Public-private policing co-operation led to successful international prosecutions of counterfeiters and closure of manufacturing plants overseas and in the UK, where it is more a cottage industry, although the velocity of such frauds appears to be increasing and the time from card number compromise to first use is decreasing. Card details are often stored and sent electronically to Italy or the Far East, where they are immediately encoded onto cards and used before the retailers or issuers suspect anything.

Credit, Debit and Charge Card Fraud Losses by Place of Misuse (£m.)

	UK Merchant (Card present)	Card not present (UK)	ATM	Bank counters	Non-UK	Total
1991	127.9	0.4	3.7	8.6	25.0	**165.2**
1992	130.2	1.0	3.4	8.6	21.8	**164.0**
1993	95.8	1.3	2.5	6.9	23.4	**128.5**
1994	65.5	2.2	3.2	5.0	21.0	**94.7**
1995	49.5	4.3	3.5	4.8	21.2	**79.0**
1996	57.3	6.0	4.4	3.9	25.4	**97.1**
1997	72.2	8.2	8.2	4.3	29.1	**122.0**
1998	74.8	11	9.7	4.7	34.9	**135.0**
1999	93.5	22.5	12.3	6.5	54.6	**189.4**

The greater part of the frauds occur at the point of sale, domestically and, increasingly - 30% in 2000 and 28.8 % in 1999,compared with 15.1 % in 1991 and 26.2 % in 1996 - internationally. A multi-pronged approach to a set of carefully defined, data-informed sub-problems is more likely to achieve a managed reduction – especially in the short term – than is any one Big Idea, for there are many severe technical difficulties in implementing strategic initiatives, as issuers have found in the chip card roll-out. Below are two initiatives that show what can be achieved:

- Operation Valentine was a tactical initiative in a major retail chain during March and April 2000, involving the creation of specific neural network rules for the selected stores and codes identifying them separately; staff training on skimming and counterfeit cards (with simple recognition packs); and increased rewards of £100 for all cards captured during the period. Intentionally, there was no external publicity before or during the trial (though inside information may have leaked to some criminals). This generated a substantial rise in the number of cards retained compared with the same period in the previous year, a strong fall (from 0.40% to 0.12%) in the fraud to turnover ratio, and (£4,000 to less than £1,500 per month) in the fraud levels in the trial stores. Further refinement is ongoing, though some of the fall may be attributable to a 'Hawthorn effect' of closer monitoring and training. One practical difficulty is that some stores take the view that card capture rewards should go to the business, not to the individuals, and this would reduce staff motivation. However, the experiment suggests that the retail environment can be manipulated positively.

- A successful investigation into suspected counterfeiting of CDs and other products as well as in the skimming and counterfeiting of cards led to several arrests by the City of London police in a case which has yet to come to trial. Substantial material was found, and card data allegedly obtained by a network of waiters of East European origin were relayed rapidly overseas. This parallels other operations in which Italian and Chinese waiters, and Sri Lankan and other Asian petrol retail staff send skimmed card details to their ethnic gang contacts in countries of origin.

PLASTIC FRAUD PREVENTION RECOMMENDATIONS FOR THE FUTURE

Aggressive marketing drives and concern about new and smaller entrants obtaining a 'free rider' on prevention investment by major players reduces co-operation.. Reduction measures suppress fraud but do not permanently displace or remove it, since fraud levels will soon rise dramatically again if the measures are relaxed. Prevention measures may work best in a variety of combinations, and increased reliance on technology makes it necessary continuously to develop contingency plans in the event that the technology is compromised: counterfeiting and Card not Present (increasingly, Internet) fraud have been the fastest growing areas in recent years – in the first quarter of 2000, they constituted over half of card fraud losses, compared to 5% in 1991 and 12.3% in 1995 - and everyone interviewed expects this rise to continue. Until chip terminals become more common overseas and retailers abroad are better able to run checks on card purchasers, cross-border fraud may rise: it takes no longer (and more reliable) to go from London to Paris or Brussels as from London to Liverpool, and budget flights have brought down the cost of travel for fraudsters as well as others. But most plastic criminals prefer to use cards locally or regionally, for convenience and predictability, and are unlikely to become international criminals.

Key future issues to be addressed are:

1. *Card authentication: deeper roll-out of chip card*s. There have been technical difficulties about type approval, but by the end of 2001, three quarters of the 390,000 or so bank-owned terminals will be chip-ready; by end 2002, all of them should be. The roll-out of credit cards began mid-1999 and debit cards in mid-2000. By the end of 2003, the majority of cards will be chip. However, most of the turnover occurs in terminals owned by large stores who have their own electronic systems and find it both expensive and difficult to integrate, nor will they obtain any obvious economic benefit. With a more harmonious working relationship, most of the technical issues have now been resolved, though large retailers still complain about the extra seconds per customer taken for chip (which will increase further if PIN is adopted). There are ongoing high-level discussions about the extent and form of economic incentivisation of retailers, especially in the light of criticisms of banks and card schemes in the Cruikshank Report (pp.98-100). So introducing and activating more chip terminals would reduce counterfeiting and skimming of card details in a 'card present' environment.

2. *Cardholder verificatio*n. Chip may guarantee that the card is genuine but it currently does not show that the person presenting the card or card number is entitled to use it. There is currently no industry agreement on cardholder verification, though there is substantial support for PIN at the point of sale among issuers and among retailers, who are currently suffering losses from charge backs imposed when the signature is not accurate or where the card is absent. A difficulty is that there would have to be major investment of money and time and that pay-back would occur only some five years hence, after full implementation to avoid consumer and retailer confusion. One survey showed that over 85% of customers would find PIN acceptable at point of sale (as in France). There are technical difficulties, such as a need for mobile PIN machines in hotel and leisure facilities, the absence of PIN-select possibilities among issuers who do not have ATM terminals, and overseas environments where either PIN is not used or is not linked. Unless mandated, PIN may have only a modest effect in Card not Present fraud risks. Retailers experience problems because of lack of commonality in what is printed on till receipts. Especially in Card not Present situations, the planned roll-out this autumn of an Address Verification System and the CV2 numbers printed on the card signature strip that cannot be 'read' from a magnetic stripe should be useful as a temporary control on counterfeits and 'skimming'. Plans include linking the UK to the US, but optimally, they may need to be extended to continental Europe to prevent some fraud displacement to e-commerce suppliers there and

elsewhere. In the medium term, for CNP, card and cardholder verification may need to be achieved by chip card readers in computer keyboards and by small portable fingerprint readers to send prints digitally across the system. Given that people retain keyboards for a long time, such 'chip slots' should be introduced as soon as possible.

3. *Applications fraud.* Industry can help by pooling applications data to trusted third parties for a faster review of suspiciousness triggers where a number of plastic cards are taken out by the same person and/or at the same address within a short period. There needs to be greater commonality than at present in evidence of identity required for new business from individuals and businesses, and further consideration should be given to the establishment of systems to log all stolen documents that can be used for identity purposes centrally, and to permit or even mandate checking (at a cost) against such a database. Training of telephone credit application and authorisation staff to be sensitive to cues of speech and incongruities of statements and attributes of callers, to help pick out the potential fraudster, has potential. The verification of identity is a particularly difficult issue in a non face-to-face environment.

4. *Better identification of and intervention in risky place*s. Management information has improved substantially within the industry, but more refined merchant codes (as in Operation Valentine above) would be useful to enable better identification and targeting of card crime 'hot spots' for prioritised local action rather than the inevitably more difficult national changes in systems and operations. This could be allied to better retailer and public education.

5. *Improved policin*g. Resources will never be available for complete policing of all crimes, but quite apart from issues of fraud losses to major corporate taxpayers, the consequences of impersonation can be very serious for individual cardholders. Although most plastic and cheque crime will continue to be local, there are considerable inconsistencies in the way that organised fraud is dealt with by the 22 out of 35 respondent English/Welsh constabularies and four of six Scottish ones that have some formal cheque squad functions at present. Some constabularies (including non-Metropolitan ones such as Bedfordshire and Hertfordshire, as well as Metropolitan ones such as the City of London) are both committed and efficient, but some others do not appear to be inclined to get any serious grip. One possibility is further enhancement of the APACS Fraud Intelligence Bureau, a centralised, 'rapid response' group seconded from the card industry, and of its liaison with police, possibly industry-funded, to deal actively with emerging attacks on smart card systems. This has already produced valuable, clear practical guidance for police and retailers on how to recognise and deal with skimming. Another possibility is an industry and/or government-funded central squad. As digital camera technology and time recording become more accurate, there is enhanced potential for stored CCTV to be reviewed by investigators in the light of identified fraud transactions, with a greater yield from reactive as well as organised crime investigations.

Many existing fraud reduction measures could be more consistently and rigorously implemented, and this should be the immediate focus, along with measures to increase the downside risks for offenders to discourage them from improving their techniques through unpunished attempts. Given implementation time lags, and the fact that the earlier that crime reduction measures are put in place, the more money is saved, speedy decisions on key strategies are necessary.