FINANCIAL TIMES THURSDAY JULY 9 1992

Foiling the forgers

By Louise Kehoe

Use a credit card to shop in London and you can expect to see the sales clerk scrutinise the signature on the back of your card to see if it matches the one you have scribed on a sales slip.

Now fly to New York and pull out the plastic again. The chances are that your signature will not even merit a second glance, but the card will probably be "authorised" by swiping it through a slot in the side of a telephone, or built into the cash register that reads information on the magnetic stripe on the back of the card and transmits it, via telephone lines, to a central computer.

Retailers and banks have adopted varying methods of validating credit card transactions in different parts of the world. All, however, address the universal problem of growing credit card fraud.

Losses from card fraud have risen alarmingly over the past two years. Visa International measured fraud and counterfeit losses on its credit cards last year at $623.4m, up 52 per cent on 1990. In the UK, the Home Office estimates card fraud cost £165m last year, up from £150.3m in 1990.

Technology is widely seen as the chief weapon in the fight against card cheats, but applications must take account of regional differences.

Automated signature verification holds greater promise in markets where credit card signatures are routinely checked, whereas in the US, the process would have to be disguised to make it acceptable to cardholders, who see this type of authorisation as an insult to their integrity.

Perhaps because the British are accustomed to having signatures checked, the technology is a focus of research and development in the UK.

AEA Technology, a unit of the former Atomic Energy Authority, has developed a signature verification system based upon a "neural network" an array of computing elements that mimics the thought processes of the human mind.

Rather than simply analysing elements of the signature, like a conventional computer system, the "Harwell Countermatch" also views the signature as a whole in the way as a **person** might get an overall impression of its appearance. The signature is mapped against a sample which can be recorded on the magnetic strip or semiconductor memory in a credit card.

The AEA system overcomes one of the drawback's of automatic signature verification by learning as it goes and picking up on the natural variations in a signature. So the accuracy of the system improves with use.

In trials where forgers attempted to copy signatures, the system detected over 95 per cent of forgeries, while less than 1 per cent of authentic, signatures were rejected.

Barclaycard, the largest issuer of credit cards in the UK, is testing signature verification, voice recognition and fingerprint matching. All are seen as long-term ways to avoid credit card fraud at the point of sale.

Signature verification is widely seen as the most acceptable form of automatic verification because it is less intrusive and does not require significant changes in the familiar procedures involved in using a credit card.

In the US, point-of-sale credit card verification is the exception, rather than the rule. However, Visa is conducting a trial of electronic signature capture in Gap clothing stores. While the aim of this experiment is to eliminate paperwork, it would be feasible to incorporate signature verification into the system without any change which is perceivable by the customer.

Nobody in the credit card industry sees signature verification as the sole solution to credit card fraud, and there is a broad consensus that the focus of prevention must move away from the point of sale toward authorisation networks. The UK's high telecommunications costs.are therefore a serious drawback, inhibiting merchants and bankers from accessing remote data processing centers.