CRIMINAL TENDENCIES

Computerised crime can net you millions of pounds – or hefty jail sentence. Andrew Baron took a look through the records to discover how some famous crimes were perpetrated...

For 20 years and more the spectre of computer fraud has been raised time and time again by the media. A widely-held belief is that reported computer crime is only the tip of a very large iceberg, with most cases going unreported.

Express often receives phone calls from bank employees claiming that one of the Big Five has been stripped of millions but it won't publicise the fact for fear of panicking customers.

There is also a belief that much computer fraud is a victimless crime; it goes unreported because no one notices it, a bit like the drunk driver who gets home safely despite being three times over the legal limit.

Defining computer crime as 'the manipulation or corruption of a computer', the overwhelming majority of crimes involved are input or output frauds. The machines are incidental, the frauds would happen anyway. We visited the City of London Police who told us the problem of hackers invading mainframes and stealing vast sums of money or data is largely a myth. In this field, crime where it occurs does so usually as the result of either an in-house thief or someone on the inside collaborating with an external buyer or supplier.

Of the computer-related crimes that do happen in Britain most – when detected – are pretty mundane. In the States however there have been some quite spectacular frauds. So we decided to undertake a little investigation of our own – here are some of the more colourful cases we've encountered.

SALAMI ZAPPING

In 1985, a programmer in an American mail-order company created a salesman and gave him the name Zwana. Zwana earned his commission by rounding down entries from other salesmen and transferring the odd cents to his fictitious account.

The fraud was only discovered after two years when, as a PR exercise, the company's marketing department took the first and last salesmen on the payroll and audited them. Zwana was clearly the last in the alphabet. This kind of scam, the 'salami technique', gets its name because the fraudster takes a very thin slice off everybody else's account. It is also known as application zapping and is very rare, and for a good reason. To set up an application zap – rounding down the genuine accounts and setting up false ones – requires a great deal of technical expertise. Anyone with the ability to do it can almost certainly find easier and safer ways to rip off the company. In fact, the Zwana story is almost certainly apocryphal; in another commonly-told variation of the same scam, the name Zzwicke is used.

Another old chestnut is that of the fraudster who tells the company: "Pay me half of what I stole and I'll show you how I did it". This and 'Zwana' are urban legends in the making.

Another variation on the salami technique is the story of a computer crook working for a US oil company. He was responsible for dealing with garages in a certain area, and set up a fraud specifically to help garage owners. Co-ordinating all the relevant invoices, he gave the garages a discount and arranged for himself to be paid a commission. The sum involved was miniscule, 2.5 pence per gallon, but it soon mounted up to £26,000. The company only caught on when he went on holiday and the price scales reverted to normal. He was sacked, prosecuted and given a four-month prison sentence.

One fraudster included a two per cent discount for prompt payment. It is not known if the judge gave him a discount on his sentence, but he was well and truly nicked.

Even more enterprising was the clerk with five years' service who, over a period of six months, made off with £47,000. He used the system to set up fictitious companies complete with letter headings. Invoices authorised by him went to special holding accounts.

To cap it he included a two per cent discount for prompt payment. It is not known if the judge gave him a discount on his sentence, but he was well and truly nicked.

MEGAFRAUD

A Third World country was negotiating a loan of some £2.5 billion for a number of development projects. For reasons which are not made clear, the president and vice-president decided to keep the deal secret, not just from the public but from the rest of the government as well, so it was arranged through a financier with connections in the Middle East whose contacts demanded anonymity.

Arrangements were made through four institutions, two of them companies in Hong Kong, one a long-established Swiss bank and the fourth a Norwegian bank. The Swiss bank was to provide the deposit and drawing facilities, and the lender's representative was paid a non-returnable one per cent fee and security in the form of a large amount of negotiable securities.

The shroud of secrecy surrounding the deal suited everyone, ostensibly for political reasons. But at the eleventh hour one of the borrowers smelt a rat and arranged for some discreet enquiries to be made. Within 24 hours it became known that the Norwegian bank was a front and the man who had set it up was wanted by the police in Hong Kong. The Swiss bank was genuine, but the two Hong Kong companies were also fronts.

The man behind them had already been involved in a scam which had led to the collapse of a Malaysian institution and was known to have links with organised crime in North America and in the Far East.

Fortunately, once the authorities had been alerted they moved quickly: the con men were arrested, the advance fee was recovered and further criminal connections were uncovered. Just as importantly, no one lost face, but this could easily have become one of the biggest successful bank computer frauds in history.

LARGEST CORPORATE FRAUD

It's one thing to know your customers, but when everyone, including the Chairman of the Board is on the take, checks and balances don't count for much. The biggest computer fraud in history started in the mid-60s without the aid of a computer, but by the time the scandal broke in 1973, the web of deceit had been cast so wide that it required a mainframe to keep track of all the dodgy dealings incorporated into it, which included over 60,000 fake insurance policies.

This became known as the great Equity Funding fraud. The Equity Corporation of America was one of the hottest stocks on Wall Street; its success was based on the theory that by dealing in both mutual funds and insurance policies it could make both forms of investment highly attractive.

The idea was that customers would invest in the mutual fund and the company would pay the customer's life insurance out of this, recording the payment as a loan, thus freeing capital which could be used elsewhere. In 1969, Chairman of the Board Stanley Goldblum began an aggressive programme of corporate expansion and acquisition. This inflated the share price and Goldblum and friends were able to unload company stock at a tidy profit.

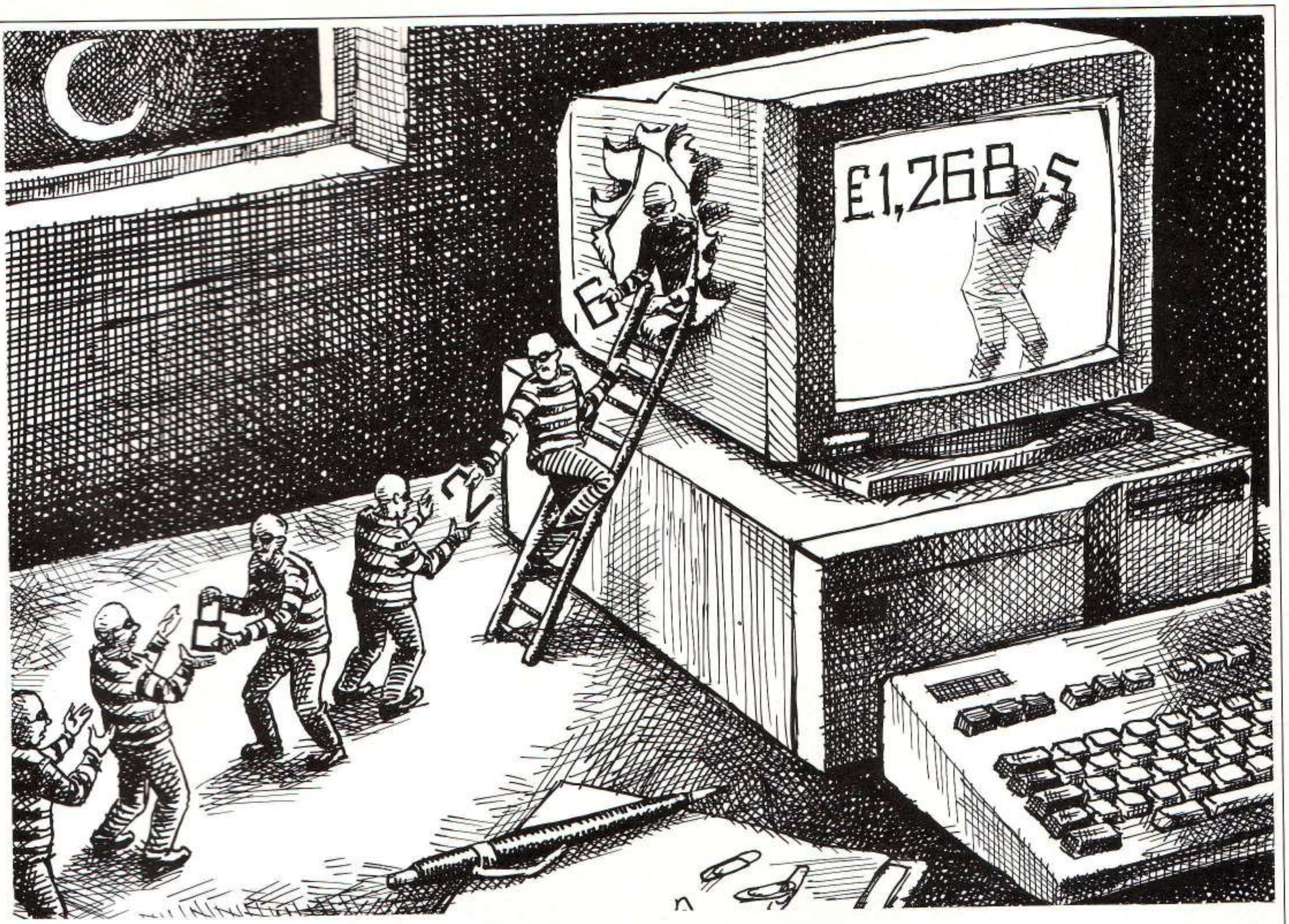
Of course, nobody gets something for nothing, and the expansion was increasingly funded by using the computer to generate 'dead souls', bogus records which were sold to re-insurers. A whole department was specially assigned to this task, and the company even began to run 'fraud parties' at company headquarters which lasted well into the night.

A mere $144,000 was siphoned off into the accounts of particular conspirators, presumably as hush money; the rest stayed in the company until by the spring of 1971 the fraud had grown to such proportions that Goldblum and company needed to generate up to 50,000 new bogus files just to keep it running.

As the scale of the fraud grew, so did the fraud parties, and the company got in deeper and deeper. All fake policies were assigned a special code and the computer was instructed to exclude them.

The bubble was finally burst in March 1973 when a former employee reported the dead souls racket to the police and to a Wall Street analyst. By this time the company had 97,000 policies on file, 64,000 of them fake, and was valued at $737 million of which $185 million was non-existent.

Goldblum and several other conspirators received jail sentences.



$2,000,000 IN ONE TRANSACTION

As well as the biggest, the Equity Funding fraud is possibly the most complex computer fraud on file, but one fraudster netted a cool $2,000,000 in one transaction, and he didn't even have to touch a keyboard.

Opening an account with a New York bank with a substantial sum, he claimed to be a manufacturer of metal furniture on the West Coast and said further that he would soon be opening a plant in the New York area so his account would be receiving a large fund transfer. Which it did, $2,000,000. It was only after he had withdrawn the money and disappeared that it was discovered that both the transfer and his West Coast account were bogus. Further enquiries led to the person who had wired the transfer, his former girlfriend.

She had resigned from her bank job shortly after he had ditched her. Before he disappeared, her boyfriend had asked her to play a joke on a friend of his who, he said, worked as a computer operator in New York. The joke was, of course, to wire $2,000,000 to his account at the New York bank where his imaginary friend worked, which she did. Both the money and the boyfriend had promptly vanished, leaving the bank $2,000,000 out of pocket and the former girlfriend with a lot more than a broken heart.

MAGNETIC INK

A somewhat more complex fraud involved the doctoring of cheques and paying-in slips. One enterprising gent who opened a bank account in Washington procured a special typewriter, one which was equipped to type in magnetic ink, and added the code from his paying-in slips to some blank paying-in slips. Then he left these in the tray at the bank and every time someone paid in with one, the computer would credit the payment to his account.

Altogether a quarter of a million dollars was redirected in this way; he cleared out $100,000 and cleared off with it before the bank got wise. The same scam was perpetrated independently in both New York and Boston.

A variation on this scam involved not paying-in slips but cheques. This time the enterprising individual found a printer to print his own cheques, but with a minor alteration. The three-digit branch code was altered to that of another bank, and several large cheques were fed into the system. The Federal Reserve computer accepted them subject to clearance, but because they were returned to the wrong banks the people processing the cheques assumed there had been a routine error and redirected them.

> *At one point he had a $25,000 switchboard delivered to a manhole in the road at 2am. He picked it up in a second-hand van and nobody questioned him.*

Once a cheque had been presented it continued to be passed back and forth, and the fraud only came to light when they became too frayed to be handled automatically. By that time the perpetrator had withdrawn $1 million in cash and disappeared.

TURN AROUND

Finally, we should mention the case of 21-year-old Jerry Neal Schneider. He seems to have had a fascination with telephone and electronic communication equipment, so much so that he began rummaging through the trash cans outside the Pacific Telephone and Telegraph Company and salvaged a number of operating and management guides.

Later, when he became an engineering student he decided to put these publications to good use. Unfortunately he gave different accounts to different people, so we'll never know exactly how he did it, but by various ruses, including posing as a company employee, he discovered the code numbers, account numbers and the fundamentals of PTT's ordering system. In June 1971 he ordered $30,000 worth of equipment and picked it up the following night. Then he set up his own company: Los Angeles Telephone and Telegraph Company to buy equipment which was charged to PTT's account, and sold on his own to private suppliers. At one point he had a $25,000 switchboard delivered to a manhole in the road at 2am. He picked it up in a second-hand PTT van and nobody questioned him.

Before long he had set up a 6,000 square foot warehouse and employed 10 people! In January 1972, he refused an employee a raise; the disgruntled worker reported him to the police, whereupon Schneider was arrested and charged with a million-dollar fraud. However, at his trial the prosecution was able to prove a mere $5,000 worth of fraud, and after plea bargaining Schneider served 40 days of a 60 day sentence on a prison farm. PTT filed a six-figure civil suit against him which he settled for a princely $8,500 then, after selling his story to a film company, he set up in business as a computer security consultant. Which goes to show: if you can't beat 'em, join 'em!