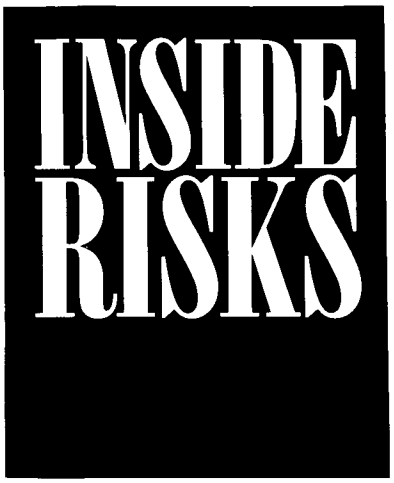
Peter G. Neumann

FRAUD BY COMPUTER



Computer-related financial fraud continues to be a problem. Here are a few cases from the Risks archives.

Frauds

- Volkswagen lost almost $260 million as the result of an insider scam that created phony currency-exchange transactions and then covered them with real transactions a few days later, pocketing the float as the exchange rate was changing. This is an example of a salami attack—albeit with a lot of big slices (*SEN 12,* 2, Apr. 1987, 4). Four insiders and one outsider were subsequently convicted, with the maximum jail sentence being six years, so their efforts were not entirely successful!
- Losses from automatic teller machines (ATMs) are numerous. The archives include a $350,000 theft that bypassed both user authentication and withdrawal limits, $140,000 lost over a weekend due to a software bug, $86,000 stolen via fabricated cards and espied authentication numbers (PINs), $63,900 obtained via the combination of a stolen card and an ATM program error, and other scams.
- Other frauds include a collaborative scam that acquired 50 million frequent-flier miles, an individual effort that gained 1.7 million miles, a collaborative effort involving millions of dollars worth of bogus airline tickets, and a bank computer system employee who snuck in an order to Brinks to deliver 44 kilograms of gold to a remote site, collected it, and then disappeared.

Thwarted Attempts

- The First Interstate Bank of California came within a whisker of losing $70 million as the result of a bogus request to transfer funds over the automated clearinghouse network. The request came via computer tape, accompanied by phony authorization forms. It was detected and cancelled only because it overdrew the debited account. The FBI is investigating (*SEN 17,* 3, July 1992).
- First National Bank of Chicago had $70 million in bogus transactions transferred out of client accounts. One transaction exceeded permissible limits, but the insiders managed to intercept the telephone request for manual authorization. However, that transaction then overdrew the Merrill-Lynch account, which resulted in the scam being detected. Seven men were indicted, and all of the money was recovered (*SEN 13,* 3, July 1988, 10).
- The Union Bank of Switzerland received a seemingly legitimate request to transfer $54.1 million (82 million Swiss francs). The automatic processing was serendipitously disrupted by a computer system failure, requiring a manual check—which uncovered the bogosity. Three men were arrested (*SEN 13,* 3, July 1988, 10).
- The Pennsylvania state lottery was presented with a winning lottery ticket worth $15.2 million that had been printed *after* the drawing by someone who had browsed through the on-line file of still-valid unclaimed winning combinations. The scam was detected because the ticket had been printed on card stock that differed from that of the legitimate ticket (*SEN 13,* 3, July 1988, 11).
- On Christmas Eve 1987, a Dutch bank employee made two bogus computer-based transfers to a Swiss account, for $8.4 million and $6.7 million. Each required two-person authorization, which was no obstacle because the employee knew someone else's password. The first transaction was successful. The second one failed accidentally (due to a 'technical malfunction'), which was noted the next working day. Suspicions led to the arrest of the employee (*SEN 13,* 2, Apr. 1988, 5).
- An ATM-card-counterfeiting scam planned to make bogus cards with a stolen card encoder, having obtained over 7,700 names (with personal identifiers, PINs) from a bank database. An informant tipped off the Secret Service before the planned mass cash-in, which could have netted millions of dollars (*SEN 14,* 2, Apr. 1989, 16).

Conclusions

In general, computer misuse is getting more sophisticated, keeping pace with improvements in computer security. Access controls can hinder outsiders. Fraud by insiders, however, remains a problem in many commercial environments (often not even requiring technology, as in the U.S. savings and loan fiasco, now exceeding $1.5 trillion). High-tech insider fraud can be difficult to prevent if it blends in with legitimate transactions.

Most of the preceding thwarted attempts were foiled only by chance, which is not reassuring, particularly because more cautious perpetrators might have been successful. We do not know the extent of successful frauds. Financial institutions tend not to report them, fearing losses in customer confidence and escalations in insurance premiums. This leaves us wondering how many successful cases have *not* been detected, or have been detected but not reported. Better system security, authentication (of users and systems), accountability, auditing, and real-time detectability would help somewhat. More honest reporting by corporations and governmental bodies would help reveal the true extent of the problems, and would be beneficial to all in the long term. Otherwise, computer-aided fraud will continue.