Credit cards have become extensions of computer databases. In most shops where cards are accepted, sales clerks pass the information encoded in magnetic strips through modems linked to central databases. The amount of each purchase is immediately applied to the available balance and an authorization code is returned through the phone link.

One form of forged cards uses the magnetic stripe. On these fraudulent cards, the stripe contains a valid account code that is different from the information embossed on the card itself. Since very few clerks compare what the automatic printers spew forth with the actual card, thieves successfully charge their purchases to somebody else's account. The fraud is discovered only when the victim complains about erroneous charges on the monthly bill. Although the victim may not have to pay directly for the fraud (the signature on the charge slip won't match the account owner's), everyone indirectly bears the burden of the theft by paying higher credit card fees.

Another form of credit-card fraud involves synthetic account numbers. Credit card numbers include bank identification numbers at the start of the number, some unique digits, and a checksum computed using the other numbers. There are programs available on the Internet for generating credit-card numbers that include valid checksums. Not all of these synthesized card numbers correspond to existing accounts, but criminals – often teenagers – experiment with the numbers by trying them out by phone on unsuspecting retailers until they have winnowed the list down to valid numbers which they can then use for further purchases.

Those of you whose businesses accept credit cards should cooperate closely with the issuers of the cards. Keep your employees up to date on the latest frauds. and train them to compare the name on the card itself with the name that is printed out on the invoice slip. If there is the slightest doubt about the legitimacy of the card, the employee should ask for customer identification or consult a supervisor for help.

The problem continues to be resistance from uneducated users who see a request for identification as an insult. One way of reducing this stupid reaction is to put signs up with a message like those at many bank windows: “We will ask for your ID as a way of protecting you against fraudulent use of your cards and accounts.”

Unfortunately, at many stores, I notice that the staff don’t even bother to look at the signature on the back of the card; I often irritate them by suggesting that it would be a good idea. Usually it turns out to be policy to check signatures, but supervisors fail to monitor compliance. One technique to encourage checking is to write “Check carrier’s ID” on the back of the card in place of your signature. If you choose this method, just be sure that you do in fact have identification with you all the time.

***
In the next column in this series, I’ll look at how credit-card issuers have been implementing anti-fraud measures.

* * *

Some related sites:

AntiFraud < http://www.antifraud.com/ >


CyberSource < http://www.cybersource.com/products_and_services/credit_card_fraud_management/ >

Federal Trade Commission consumer credit protection resources < http://www.ftc.gov/bcp/menu-credit.htm >


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.