In this series, I’ve been reviewing aspects of forgery. In the previous column, I looked at fake credit cards. In this column, the topic is anti-fraud measures for spotting fake or stolen credit cards.

* * *

In recent years, with the rise of telephone and Web-based commerce, many merchants are using an additional feature on today’s credit cards: the verification number printed on the back of the card. Operators and forms are increasingly asking for part of this verification number to ensure that the consumer has physical possession of the card. Because this “serial number” is not yet easy to generate from a given account number, it is still difficult for a forger to invent one that matches the account number.

One of the most effective anti-fraud measures in use by credit-card companies is pattern matching similar to what is being used successfully in intrusion-detection systems. Computer programs monitor each card-holder’s usage patterns; any large deviation from the norm can alert a human supervisor who can decide whether to interfere with the automatic approval process. At that point, a card-carrier can be told that a charge has been refused and is then asked to phone the agent at the issuer’s security center. Usually a brief discussion suffices to authenticate the user. Although some people seem to resent this measure, it seems to me to be a minor inconvenience given the possible benefits of preventing large fraudulent purchases. Certainly I have always felt grateful and thanked the agent cheerfully for intervening.

A few credit-card issuers integrate portraits of the authorized user on their cards as a deterrent to fraud. Indeed, some years ago the Royal Bank of Scotland agreed to issue two cards to a transvestite customer – one for each persona.

Why don’t we insist on the same, rather modest, level of security for credit cards as for bank cards? What would be wrong with requiring a PIN (personal identification number) to be entered by the user at the time of payment? Well, retailers tell me that the ordinary public does not like security measures and so if implementation is piecemeal, the stores where PINs are used will either be or perceive themselves to be at a competitive disadvantage with respect to other stores.

What about smart cards, then? They no longer cost very much and they would be much harder to counterfeit. Well, the problem there is a fundamental one: credit-card companies and banks don’t pay for the losses incurred through fraud, so they have little incentive to improve security. In one of my security classes, a security officer from a large national bank explained that interest rates on unpaid balances are calculated using about half of the rate to cover losses and frauds. I once had a credit card whose balance was guaranteed by a term deposit with the issuing bank; indeed, the interest rate on that card was 8% when everyone else was stuck with 16% for late payments. With all the users who pay interest on late payments, the banks have no significant
cost of doing business the old, fraud-laden way.

The one factor I see as influencing this problem is the rising toll of identity theft. More about that in another column.

* * *

For guidance on fraud avoidance for businesses, see the Federal Trade Commission’s list of resources at <http://www.ftc.gov/ftc/business.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.