Forgery (1): Classic Cases

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Criminals have produced fraudulent documents and financial instruments for millennia. Coins from ancient empires had elaborate dies to make it harder for low-technology forgers to imitate them. Even thousands of years ago, merchants knew how to detect false gold by measuring the density of coins or by testing the hardness of the metal. Cowboys in Wild-West movies occasionally bite coins, much to the mystification of younger viewers.

In his entertaining 1978 book about computer crimes, Thomas Whiteside provides two particularly interesting cases of computer-related forgery. The most ingenious involved a young man in Washington, DC, who printed his own account's routing numbers in magnetic ink at the bottom of the deposit slips you usually find in bins at any bank. He replaced the blank deposit slips by the doctored ones. Hundreds of people used these slips to deposit money to what they assumed would be their accounts. The victims wrote their own account numbers in, handed their money and the slips to tellers, and their accounts were apparently credited as usual. In fact, however, all the slips with magnetic ink were automatically sorted and processed, diverting $250,000 of other people's money into the criminal's bank account. When customers complained about their bouncing checks, the bank discovered too late that the thief had fled, taking $100,000 along with him.

If a teller had observed that customers were writing in account numbers different from the magnetically-imprinted codes at the bottom of each deposit slip, the fraud would have been impossible.

The other case cited by Whiteside concerned checks which were fraudulently printed with the name and logo of a bank in New York but with the routing numbers and false account number from a totally different bank on the west coast. The criminal deposited the check at a third bank. The check would automatically be routed by the Federal Reserve System according to the magnetic ink codes, ending up in the processing hopper of the west coast bank. There, not having a valid account number, the check would pop out for human handling. The clerk responsible for exceptions would immediately see the prominent logo of the New York bank and send it there by mail. Days would pass before the check ended up in New York. Of course, the New York bank's automatic check processing equipment would respond to the fake routing code and send it back to the Fed, and so it went in an endless loop. Apparently the farce ended only when the checks became so worn that they required physical repair. The inconsistency was finally noticed by a human being and the deception was discovered. Unfortunately, by this time the thief had absconded with about $1 million.

Once again, human awareness and attention could have foiled the fraud.

* * *

More about forgeries in the next column.
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.