The recent disclosure that WorldCom concealed almost $4 billion of expenses as if they were asset acquisitions and thus falsified its accounting reminds me of the very opposite kind of fraud – one that involves lots of little thefts instead of one gigantic theft. In the _salami fraud_, criminals steal money or resources a tiny bit at a time. Two different etymologies are circulating about the origins of this term. Some claim that it refers to slicing the data thin – like a salami. Others argue that it means building up a significant object or amount from tiny scraps – like a salami.

The classic story about a salami attack is the old “collect-the-roundoff” trick. In this scam, a programmer modifies the arithmetic routines such as interest computations. Typically, the calculations are carried out to several decimal places beyond the customary 2 or 3 kept for financial records. For example, when currency is in dollars, the roundoff goes up to the nearest penny about half the time and down the rest of the time. If the programmer arranges to collect the discarded fractions of pennies in a separate account, a sizable fund can grow with no warning to the financial institution.

More daring salamis slice off larger amounts. The security literature includes case studies in which an embezzler removed $0.20 to $0.30 from hundreds of accounts two or three times a year. These thefts were not discovered or reported: most victims wouldn't bother finding the reasons for such small discrepancies. Other salamis have used bank service charges – increasing the cost of a check by $0.05, for example.

Credit card thieves with thousands of stolen account numbers sometimes steal only a little from each card, on the theory that most people won’t even notice or won’t bother reporting a minor expense that they don’t recognize.

A specific example of salami fraud occurred when a ring of criminal hackers operating in the United States, England and Spain stole the telephone calling card numbers of 140,000 subscribers of AT&T Corp, GTE Corp, Bell Atlantic and MCI Communications Corp. These thefts are estimated to have resulted in US$140 million of fraudulent long distance calls – but the thieves used y cycled through the list of cards, placing only one fraudulent call on each card.

In another scam, two programmers made their payroll program increase the federal withholding amounts by a few cents per pay period for hundreds of fellow employees. The excess payments were credited to the programmers' withholding accounts instead of to the victims' accounts. At income-tax time the following year, the thieves received fat refunds from Internal Revenue.

In January 1993, four executives of a rental-car franchise in Florida were charged with defrauding at least 47,000 customers using a salami technique. The federal grand jury in Fort Lauderdale claimed that the defendants modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles. From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from $2 to $15 per customer – rather thick slices of salami.
but nonetheless difficult for the victims to detect. [NOTE: I have looked for information about the results of the accusation, but have been unable to find any. If any reader can help me with the details of what happened after the indictment, I will gladly publish a note in this newsletter with thanks.]

The next article in this pair continues with more examples of salami frauds.

* * *


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@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

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.