In my last column, I introduced the Notice of Proposed Rulemaking (NPRM) to help protect customers of banks and other financial institutions against identity (ID) theft. The NPRM was published in July 2006 by a consortium of US federal regulatory agencies. They issued a list of warning signs (“red flags”) of ID theft that financial institutions should act on to prevent ID theft.

The specific red flags are listed in Appendix J (pp 111-114) of the NPRM. The 31 warning signs including the following highlights (I am summarizing):

- Information from a consumer reporting agency
  - Fraud alert
  - Notice of address discrepancy
  - Pattern of activity inconsistent with history and usual activity of applicant or customer
  - Closure of an account for cause or abuse of privileges
- Documentary identification inconsistencies (forgeries, bad photos, wrong information)
- Personal information inconsistencies
  - Addresses don’t match
  - Inconsistent Social Security Number versus date range
  - Correlation with known frauds
  - Fictitious addresses or mail drops
  - Bad phone numbers or answering services
  - Incomplete applications
- Address changes
  - Immediate change of address after establishing account
  - Undeliverable mail despite continued activity
- Anomalous use of the account
  - Bulk purchases of easily-fenced goods (TVs, jewelry etc.)
  - Failure to make payments (or to pay after first payment)
  - Changes in payment patterns
  - Major change in spending patterns
  - Sudden use of a formerly-inactive account
- Notice from customer or others
  - Observed fraud
  - Failure to receive statements
  - Notification of successful phishing attacks
  - E-mail from phishing attacks returned to actual institution
- Other red flags
  - “The name of an employee of the financial institution or creditor has been added as an authorized user on the account.”
  - “An employee has accessed or downloaded an unusually large number of customer account records.”
“The financial institution or creditor detects attempts to access a customer’s account by unauthorized persons.”

“The financial institution or creditor detects or is informed of unauthorized access to a customer’s personal information.”

“There are unusually frequent and large check orders. . . .”

“The person opening an account or the customer is unable to lift a credit freeze placed on his or her consumer report.”

These guidelines are useful not only for financial institutions: they also illustrate many principles of normal operations security (OPSEC). Being sensitive to anomalous behavior is important not only for normal security but also for resource management. Look for outliers in resource utilization, outliers in the first derivative (growth rates) of such utilization and in the second derivative (changes in slope) as well.

In my third and last column on this topic, I’ll review some of the comments filed on this NPRM.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 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.