Suspicious Activity Reporting

FIL-124-97
December 5, 1997

TO: CHIEF EXECUTIVE OFFICER
SUBJECT: *Guidance for Financial Institutions on Reporting Computer-Related Crimes*

The Federal Bureau of Investigation, working with FDIC staff, other federal banking agency representatives and other federal law enforcement agencies, developed the attached guidance for reporting, in Suspicious Activity Reports (SARs), violations of the federal criminal statute relating to computer crimes, 18 U.S.C. Sec. 1030 (Fraud and Related Activity in Connection with Computers).

The guidance is intended to facilitate timely and accurate reporting of apparent violations of 18 U.S.C. Sec. 1030 to law enforcement and bank supervisory agencies. The document describes the provisions of the law and gives some examples of conduct that may violate it. Instructions on how to report violations in a SAR are also included.

Please ensure that all personnel in your organization responsible for reporting suspicious activity receive the attached guidance immediately. If you have any questions, please contact your FDIC Division of Supervision Regional Office.

Nicholas J. Ketcha Jr.
Director

Attachment: (see below)

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, N.W., Room 100, Washington, D.C. 20434 (800-276-6003 or 202-416-6940).

GUIDANCE CONCERNING THE REPORTING OF COMPUTER-RELATED CRIMES BY FINANCIAL INSTITUTIONS

This guidance is provided in order to explain the federal criminal statute relating to computer crimes, 18 U.S.C. Sec. 1030, and to ensure the timely and accurate reporting of apparent violations of the statute to law enforcement authorities.

BACKGROUND

Regulations issued by the Federal Reserve, OCC, FDIC, OTS, and NCUA generally require banks, thrifts, credit unions, the U.S. branches and agencies of foreign banks, and other types of financial institutions to file Suspicious Activity Reports (SARs) whenever they detect any known or suspected federal criminal law violation or suspicious activity. The SAR system facilitates the reporting of suspected criminal activity and money laundering in a standard format to a single collection point, from which the information may be rapidly disseminated to appropriate law enforcement agencies. SARs play

a critical role in collecting information about criminal activity affecting the financial community. Under the five financial institutions supervisory agencies' current SAR rules, a financial institution is required to report any known or suspected criminal law violation involving an insider, regardless of amount. A financial institution is also required to report any known or suspected federal criminal law violation that involves or aggregates more than $25,000 in the event no suspect can be identified--a threshold that drops to $5,000 if a potential suspect can be identified.

The current SAR form includes in Part III, Box 37, a listing of 17 various categories of criminal law violations and suspicious activities that a financial institution can check. The categories include check, credit and wire transfer fraud, defalcation/embezzlement and mysterious disappearances, and also include a general category under "Other" that is to be used in the event the offense or activity does not appear to fit any of the delineated types of crimes. There is no category in Part III, Box 37, specifically reserved for violations of the provisions of the U.S. criminal code relating to computer crimes--18 U.S.C. Sec. 1030 (Fraud and Related Activity in Connection with Computers).

CRIMINAL LAW RELATING TO COMPUTERS

Computers and computer networks are at the heart of operations of a modern financial institution. Criminals--both inside and outside of financial institutions--recognize the potential vulnerability of computer systems. Consequently, financial institutions must be cognizant of the federal computer crime law, 18 U.S.C. Sec. 1030. This statute specifically includes as a "protected computer," among other computers shielded by the statute, any computer exclusively for the use of a financial institution, or, if not exclusively for such use, used by or for a financial institution where the conduct constituting the offense affects that use.

Financial institutions should pay particular attention to three provisions of 18 U.S.C. Sec. 1030. Section 1030(a)(2) specifically prohibits intentionally accessing a protected computer to obtain certain kinds of information without authority or in excess of authority. Not only does it generally prohibit improperly obtaining information from any "protected" computer, but it specifically prohibits improperly obtaining information contained in a "financial record" of a financial institution. The provision may also apply to an individual who hacks into a financial institution computer system. "Financial record" is defined as information derived from any record held by a financial institution pertaining to a customer's relationship with the institution.

Another provision applicable to financial institutions is the prohibition on using a "protected" computer without authorization or in excess of authorization to commit fraud. The provisions of 18 U.S.C. Sec. 1030(a)(4) criminalize the knowing use of a protected computer without authorization or in excess or authorization with intent to defraud, and by means of such conduct furthering the intended fraud and obtaining anything of value. Thus, an individual who intentionally uses another person's home banking software and purloins that person's password in order to transfer money fraudulently into his or her personal bank account has committed a crime.

The third provision--18 U.S.C. Sec. 1030(a)(5)--with applications to financial institutions is the prohibition on intentional access without authorization that results in "damage" to a protected computer. Damage is defined to include any impairment to the integrity or availability of data, a program, a system, or information that causes loss aggregating at least $5,000 in value during any one-year period. An example may involve a disgruntled former employee who maintains a "back door" into the computer system and uses it to introduce a virus that disrupts the system. Another example may involve an intruder who causes a system outage by flooding an institution's computer system with e-mail requests for information.

Other provisions of 18 U.S.C. Sec. 1030 applicable to financial institutions include subsection (a)(6), which outlaws trafficking in passwords knowingly and with intent to defraud. Subsection (a)(7) prohibits transmitting threats to cause damage to a protected computer with intent to extort money or any other thing of value from any legal entity, specifically including financial institutions. This prohibition applies regardless of whether any actual damage is caused, or whether the offender actually had the ability to cause such damage.

A violation of 18 U.S.C. Sec. 1030 can result in a fine or imprisonment for up to ten years.

GUIDANCE

A financial institution should report on a SAR any activity that appears to be violative of 18 U.S.C. Sec. 1030. If a reportable offense is detected, a financial institution should check Box 37r, marked "Other," and describe as completely as possible in Part VII, the narrative section of the SAR, the nature of the illegal or suspicious activity.

For an electronic version of 18 USC Sec. 1030, visit http://law.house.gov/usc.htm