3501 Fairfax Drive - Room B7081a - Arlington, VA 22226-3550 - (703) 516-5588 - FAX (703) 562-6446 - http://www.ffiec.gov

Financial Institution Letter

FIL-66-99
July 6, 1999

# Year 2000 - Related Fraud Prevention

To: The Board of Directors and Chief Executive Officers of all federally supervised financial institutions, service providers, software vendors, federal branches and agencies, senior management of each FFIEC agency, and all examining personnel.

The Year 2000 computer problem may create opportunities for fraud against financial institutions and customers. In response, the Federal Financial Institutions Examination Council (FFIEC) encourages financial institutions to alert their customers about fraudulent schemes involving the century date change and to mitigate their own risks by continuing to follow and, where necessary, enhance internal controls and security procedures.

## Customer Awareness Efforts

Bank, thrift, and credit union customers need to be informed about Year 2000-related fraudulent schemes so they can avoid becoming victims of these illegal activities. Informed customers can help institutions identify many types of fraud. As noted in the February 1999 FFIEC Year 2000 Customer Communication Outline and the May 1998 FFIEC Guidance on Year 2000 Customer Awareness Programs, each financial institution should educate its customers about the institution's Year 2000 readiness efforts. These efforts should include information identifying potential risks to customers associated with the century date change, including possible fraudulent schemes.

As a supplement to an institution's customer communications, the FFIEC has prepared the attached advisory to inform financial institution customers of this problem. The "Year 2000-Related Fraud Advisory" encourages customers to become educated about these fraudulent schemes and to take steps to minimize their risks by, for example, reviewing the accuracy of financial statements and receipts and promptly reporting suspicious or irregular activities. Customers should be advised how to contact the institution if any fraudulent activity is suspected.

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision

The FFIEC encourages financial institutions to distribute the attached advisory to all customers and to provide additional information on Year 2000 concerns using the FFIEC's "The Year 2000 Date Change" brochure, the FFIEC's "A Y2K Checklist for Customers," and the Federal Trade Commission's Y2K fraud advisory, "Y2K?

Y 2 Care: Protecting Your Finances from Year 2000 Scam Artists." Copies of these documents are available on the FFIEC and FTC Web sites (www.ffiec.gov and www.ftc.gov), or by calling the FFIEC at (202) 872-7500, or the FTC at (888) USA-4-Y2K.

Institutions also should consider addressing Year 2000 preparedness and fraud prevention in customer newsletters, hotlines, and outreach events. Financial institutions may contact their primary federal regulator if they have questions about Year 2000-related fraud issues and other Year 2000 concerns.

**Internal Controls**

Century date change efforts should not distract financial institutions from continuing to maintain adequate fraud deterrence measures. They should continue to have strong internal controls to prevent, detect, and correct Year 2000-related problems. For example, financial institutions should continue to:

- Train staff, particularly first line employees such as tellers and customer service representatives, about potential Year 2000-related fraud risks to their financial institution and customers, and discuss appropriate responses
- Inform appropriate law enforcement authorities of known or suspected criminal activities by filing Suspicious Activity Reports in accordance with the FFIEC agencies' reporting rules
- Limit access to remediated computer code to those with a need to know (i.e., trusted employees and vendors that have undergone security checks)
- Protect against unauthorized access, such as "trap doors," by maintaining appropriate change management control procedures, including those that address verification of software changes
- Verify that financial postings and reconciliations are performed properly and promptly
- Monitor large suspense accounts and unreconciled accounts
- Ensure that verifications and call backs are performed for wire transfer instructions received by facsimile

**Security Procedures**

Financial institutions should review and adapt, as necessary, security procedures to protect against Year 2000 related criminal activity. In this regard, management should review security measures pertaining to cash storage, automatic teller machine use, branch activity, and electronic transfers. As part of this process, management should continue to review blanket bond coverage, conduct general and specialized training for appropriate employees, and adjust staffing requirements as needed. In addition, institutions should ensure they have clear procedures for coordinating with law enforcement agencies and parties that provide security, such as courier, armored car, vault, and alarm services.

Attachment