



Office of Thrift Supervision
 Department of the Treasury

Richard M. Riccobono
Deputy Director

1700 G Street, N.W., Washington, DC 20552 • (202) 906-6853

July 15, 1999

MEMORANDUM FOR: Chief Executive Officers

FROM: Richard Riccobono *Richard M. Riccobono*

SUBJECT: Year 2000 - Related Fraud Prevention and
 Year 2000 - Related Fraud Advisory

The OTS, and the other Federal Financial Institutions Examination Council (“FFIEC”) agencies, recently issued two documents that supplement previous interagency guidance on Year 2000 customer awareness.

The first document encourages you to alert your customers and employees about fraudulent schemes involving the century date change. It describes some actions they should consider to enhance customer awareness, internal controls, and security. Please provide this document to your financial institution’s auditor and security officer.

The second document is a consumer advisory that provides examples of potential Year 2000 fraud related schemes and outlines some steps your customers can take to protect themselves from fraud. We urge you to distribute this advisory to your customers. The advisory may be copied and distributed as is, or the advice it contains may be incorporated into other documents you are planning to send to your customers on Year 2000 readiness.

Copies of these two documents are attached. They are also available on the OTS Web site at (www.ots.treas.gov). Additional information on internal controls and security procedures may be found at:

- *“FFIEC Information Systems Examination Handbook,”* Section I Chapters 9 and 12.
- *“American Institute of Public Accountants Professional Standards, U.S. Auditing”* (AU) Section 316, “Consideration of Fraud in a Financial Statement Audit,” and AU Section 319,

“Consideration of the Internal Control Structure in a Financial Statement Audit.”

- **“Bank Protection Act of 1968, as amended,”** as noted in the Consumer Affairs Examination Manual Section 450.

As always, we are interested in your questions and concerns regarding the Year 2000 date change. Please contact the Year 2000 Coordinator at your regional office (listed in the Millennium and on our Web site); Dorothy Van Cleave, National Year 2000 Coordinator at (202) 906-7380; or Jennifer Dickerson, Director, Technology Risk Management, at (202) 906-5631 for further assistance.

Attachments



Press Release

For Immediate Release

July 6, 1999

FFIEC Releases Guidelines on Year 2000 Fraud Prevention

The Federal Financial Institutions Examination Council (FFIEC) today issued guidance urging financial institutions to review their fraud prevention programs to ensure that they are protecting themselves and their customers from Year-2000 related fraud.

The FFIEC acted out of concern that criminal elements will try to defraud financial institutions and their customers using the Year 2000 as cover. The FFIEC guidance encourages institutions to enhance internal controls and security procedures and to communicate with customers about how to protect against Year 2000-related fraudulent schemes.

The FFIEC also issued a consumer advisory that financial institutions can provide to their customers. The "Year 2000-Related Fraud Advisory" alerts customers to several fraudulent schemes involving the Year 2000 and provides advice on how to avoid becoming a victim of these schemes. Specifically, customers are advised that they should:

- Never give out account information, credit card or social security numbers, or other personal information to someone they don't know, unless they have initiated the contact;
- Report any suspicious requests for confidential account information;
- Receive and review account statements on a timely basis and contact their financial institution to report any suspicious request for confidential account information; and
- Contact their financial institution with any question about its Year 2000 readiness.

To protect themselves against Y2K-related fraud, the guidance urges financial institutions to take a number of steps to strengthen their internal controls. Financial institutions are urged to:

- Review security measures pertaining to cash storage, automated teller machine use, branch activity and electronic transfers;
- Train tellers and customer service representatives to recognize potential risks of Year 2000-related fraud to their financial institution and customers;
- Alert appropriate law enforcement authorities of known or suspected criminal activities; and
- Limit access to computer systems.

The FFIEC Year 2000-related fraud prevention guidance notes that federal regulators have been working closely with banks, thrifts and credit unions for several

years to ensure that they take steps to prepare for Year 2000 and protect customers. The federal financial regulators believe financial institutions are making excellent progress and expect the industry will be prepared for the century date change.



Federal Financial Institutions Examination Council

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.

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:
Year 2000 - Related Fraud Advisory

Year 2000-Related Fraud Advisory

Concerns about possible Year 2000 computer problems present opportunities for criminals to defraud customers of banks, thrifts, and credit unions. Be assured that the federal regulators have been working closely with your federally insured financial institution to ensure that it has taken steps to prepare for Year 2000. Financial institutions are making excellent progress, and we expect the industry will be prepared for the century date change. This alerts you to some fraudulent schemes involving the Year 2000 and advises you on how to avoid becoming a victim of these schemes:

- Individuals posing as representatives of credit card issuers have called cardholders and asked them to disclose confidential information, such as account numbers. Callers told credit card holders that their cards would not work after January 1, 2000, unless they attached a new magnetic strip to the back of the credit cards. Callers then asked for account numbers and other information so that they could mail the strip to the cardholders. In reality, callers were trying to trick cardholders into disclosing personal information like their account number, social security number, address, and other information that would allow them access to the card holder's account.
- Individuals posing as financial institution employees, auditors, or others have called customers and asked them to transfer money from existing accounts to "special Year 2000 safe accounts" while the institution corrects Year 2000 problems. Callers then ask for account numbers and authorization to transfer the money to one of these "special" accounts. In reality, the callers were attempting to gain enough information to steal the customer's money.

Please note that no bank, thrift, credit union, or credit card issuer will call you to request your account numbers, personal identification numbers (PIN), or other account information for Year 2000-related purposes. They already have this information.

To help protect yourself from becoming a victim of fraud, the regulators recommend that you:

- Never give out account information, credit card or social security numbers, or other personal information to someone you do not know, unless you initiate the contact. Remember that no financial institution will call you to ask for personal account information.
- Contact your financial institution to report any suspicious request for confidential account information. Don't hesitate to make these calls. If you're being approached, chances are others in your community or around the country are also being targeted.
- Be sure you receive and review your account statements on a timely basis. Fraud can involve attempts to change your address so your account statements are mailed to others.
- Check the accuracy of account statements when you receive them. Make sure that you have authorized all the charges made to your account and report any discrepancies.
- Contact your financial institution if you have any question about its Year 2000 readiness.



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

Additional Information About Year 2000 Fraud

For further information on Year 2000-related fraud issues see the following sources:

- The FFIEC's "A Y2K Checklist for Customers," at <http://www.ffiec.gov>
- The "FDIC Consumer News" at <http://www.fdic.gov>, or call the FDIC's Compliance and Consumer Affairs office at 1 (800) 934-3342
- The Federal Trade Commission's Consumer Alert: "Y2K? Y 2 Care: Protecting Your Finances from Year 2000 Scam Artists" at <http://www.ftc.gov>, or call the FTC Federal Information Center toll-free at 1 (888) USA-4-Y2K

For more information about financial institutions' Year 2000 readiness, customers may contact:

State-chartered banks that are not members of the Federal Reserve System are supervised by:
Federal Deposit Insurance Corporation

(800) 934-3342

Internet: www.fdic.gov

Banks with state charters that belong to the Federal Reserve System are supervised by:
Federal Reserve Board

(202) 452-3693

Internet: www.federalreserve.gov

Federal credit unions are supervised by:
National Credit Union Administration

(703) 518-6330

Internet: www.ncua.gov

National banks are supervised by:
Office of the Comptroller of the Currency

(800) 613-6743

Internet: www.occ.treas.gov

State and federally chartered savings associations are supervised by:
Office of Thrift Supervision

(800) 842-6929

Internet: www.ots.treas.gov