



“IT Trends/Risks and Recent FFIEC IT Guidance”

Cindi Bonnette, FDIC

John Carlson, OCC

Bob Engebret, OTS

Jeff Kopchik, FDIC

October 11, 2001

FFIEC Risk Management Planning Seminar

Presentation Overview

- FFIEC IT Subcommittee Activities
 - Interagency Guidance
 - Interagency Security Event Monitoring
- Technology Trends and Risks
- Authentication
- IT Outsourcing and Vendor Management
- Security and Privacy
- Q &As

FFIEC IT Subcommittee Activities

FFIEC Information Technology Examination Handbook

- Ongoing Project to Update 1996 Handbook
 - No Longer Only Paper Based
 - Format Changed to Sections or Booklets
 - Risk Based Procedures vs Checklists
- Monitor Emerging Technology Issues
 - Wireless, Aggregation, Electronic Signatures, Electronic Banking Trends, etc.

FFIEC Information Technology Symposium 2002

- Scheduled for March of 2002
- Focus on a Specific Technology Issue(s)
- Product can be Informational, Guidance and/or Recommendation for Further Activities

FFIEC Information Technology
Security Event Monitoring
Process

Types of Events Monitored

- Security Events –
 - Events that cause or have potential to cause disruption of services and/or unauthorized disclosure of confidential information.
 - Intrusions, Hacks, Security Breaches
 - Unsuccessful attacks
 - Rumors
 - Physical Attacks (Terrorist Activity)

Interagency Security Event Process

- Alert
- Communicate
- Respond
- Monitor

What Is The Regulator's Role In Security Events

- Ascertain the facts
- Centralize and coordinate the dissemination of information regarding the event. (Discovery through resolution).
- Provide necessary and appropriate support to examiners and institutions.
- Perform an analysis to determine the root cause, the likelihood of a similar problem in the future, and what preventive measures, if any, should be taken.

Overview of Technology Trends and Risks

Technology Developments

- Advances in communications provide networked global access to information and delivery of products/services
 - Internet has reached critical mass (60% of U.S. households)
- Increased competition from other industries and abroad
- Greater reliance on third party providers
- Advances in technology make the component functions of banking more easily divisible
 - Outsourcing many facets of E-banking
 - Providing access to products and services
 - Franchising and branding of a bank's attributes

Bank Technology in 2001

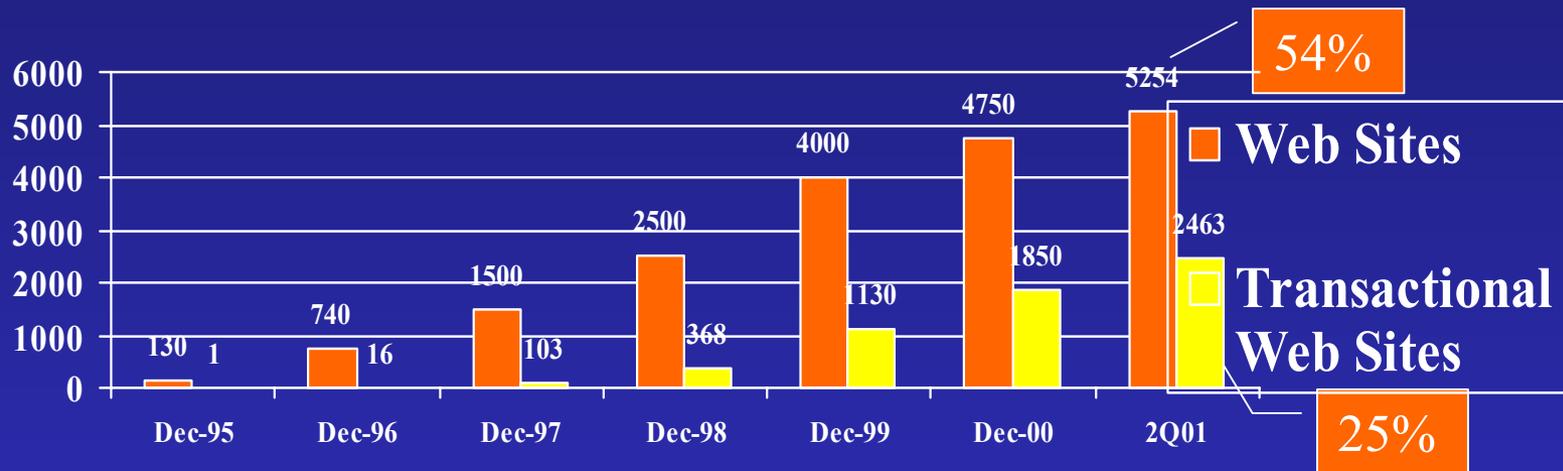
- Investments in technology continue
 - Internet banking
 - Customer relationship management
- More strategic and business-focused
- Greater attention is being paid to vendors stability and financial health
- More experience in identifying system vulnerabilities and responding to incidences

Other Technology-Related Trends

- Outsourcing and “partnering” play a critical role
- “Open” architecture presents opportunities and challenges
- Data exchange standards are evolving
- Cyber-insurance offers new ways to help manage technology risks
- Traditional payment systems are being “extended” to the Internet

Growth Trends in Bank/Thrift Web Sites

1995 - June 30, 2001



2Q2001: 54% of all banks & thrifts have a web site

25% of all banks & thrifts have a transactional web site

Source: Call Report data and informal off-site monitoring

Evolving Bank Technologies

Plotting the trends...



Risks and Supervisory Concerns

Risks and Risk Management

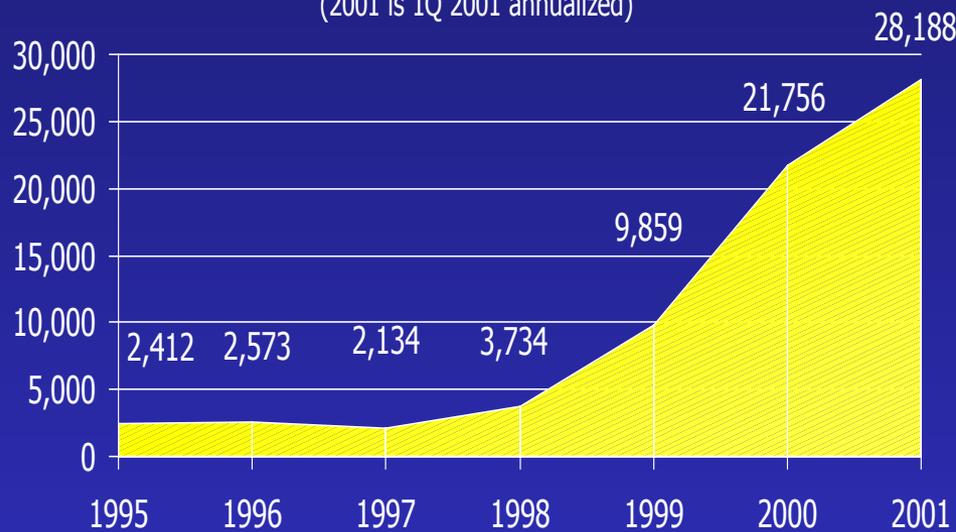
- E-banking challenges:
 - Transaction speed
 - Authentication & verification issues
 - Integration
 - Global reach
- E-banking risks cannot be compartmentalized - risk management must be integrated
 - Strategic and business risks
 - Operational / Transaction risks
 - Reputation risks
 - Compliance risks

Strategic and Business Risk

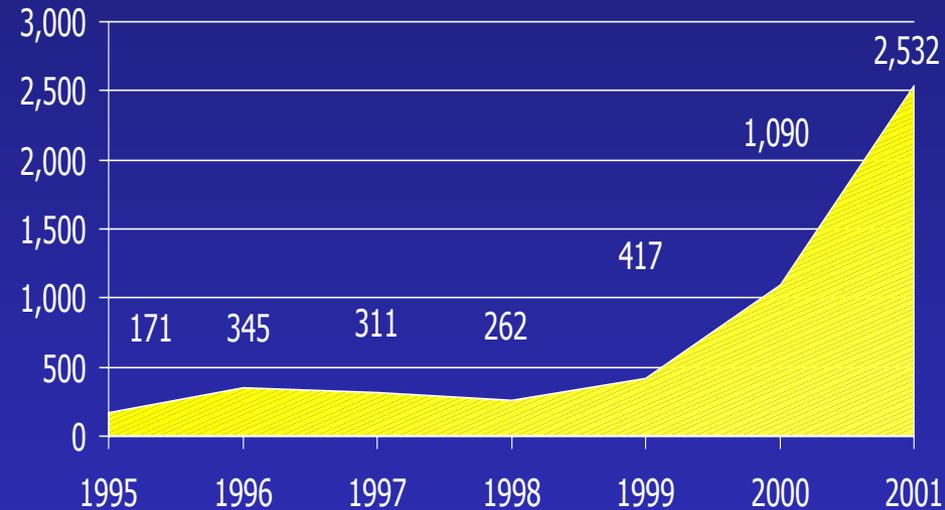
- Uncertain pace of change and evolving standards
- First Mover (“bleeding edge”) vs. wait and see (permanently lose market share)
- Struggle to retain customers in face of intense competition
- Uncertain customer acceptance
- Reliance on third parties
- Financial stability of vendors
- Impact on earnings

Reported Security Incidents and Vulnerabilities

Unauthorized Activity Incidents Increasing
(2001 is 1Q 2001 annualized)



Increasing Number of New Systems Vulnerabilities
(2001 is 1Q 2001 annualized)



Source: CERT/CC -- statistics are not limited to the banking industry and include all reported incidents

Reputation Risk

- Viability of service depends on meeting expectations for availability, confidentiality, data integrity, and overall service quality
- Customer expectation for innovation, additional services
- *Failure to meet expectations can undermine consumer confidence and trust*

Permissibility, Legal, and Compliance Issues

- Technology raises legal issues
 - Permissible?
 - Applicability of state and foreign laws?
 - Validity of electronic agreements?
- Technology creates consumer compliance issues
 - Electronic disclosures delivery
 - Weblinking, customer confusion, and liability
 - RESPA and fee income from weblinking
 - CRA and out-of-area lending
 - Fair Lending and targeted lending efforts
 - Reg. E application to aggregation services

Types of Emerging Services/Applications

- Weblinking/Portals
- Aggregation
- Wireless
- Retail Internet payments (P2P, P2B)
- E-disclosures and E-signatures

Portal Sites/Weblinking Considerations

- Key Concern: Distinguish the bank's products and services those offered by others
- Bank processes to consider:
 - Due diligence on partners
 - Agreements
 - Disclosures
- Relevant issues:
 - Content
 - Customer confusion
 - Performance
 - Security/privacy
 - Compliance/legal issues

Aggregation: Risks and Considerations

- Data from other Web sites may be erroneous or outdated
- Concentration of customer data and authentication data to other web sites makes an inviting target
- Storage and use of other Web site authentication information potentially weakens overall security
- Liability for disputed transactions may arise
- Special messages/disclosures from other Web sites may be lost or misrepresented
- Different data definitions may exist on other Web sites for similarly named data elements

Wireless Banking Offerings and Risks

- Financial institutions are offering wireless access to Internet banking applications
 - Services include balance inquiry, funds transfer, bill pay & brokerage
- Security challenges
 - Need to understand how transactions flow and security measures along the way (end-to-end security)
 - Wireless devices have limited processing power and can be easily misplaced/stolen
- Screen size may present disclosure challenges

Retail Internet Payments: Risks and Issues

- E-payments meet the needs of new market niches (e.g, online auctions, payments between individuals)
- Systems generally involve existing payment systems and networks (credit cards, ACH, EFT)
- Security and fraud concerns
 - Internet connection introduces new risks
 - NACHA amended its operating rules to address Internet-initiated ACH transfers
- Deposit Insurance and consumer protections
 - Depends on system operator and design/funds flow

E-Disclosures and E-Signatures

- Despite enactment of E-Sign Law in 2000, adoption has been slow
- Use of e-disclosures appears to be outpacing e-signatures
- Financial institutions can potentially benefit from efficiencies and cost savings with paperless transactions
- Technologies and effective practices are evolving
- The Fed issued Interim Final Rules for Regs. B, E, M, Z, and DD (October 2001 date for compliance has been postponed)

Authentication: Highlights of
FFIEC Guidance on
“Authentication in an Electronic
Banking Environment”

Authentication

- Reliable customer authentication is imperative for E-banking
- Effective authentication can help banks reduce fraud, reputation risk, disclosure of customer information, and promote the legal enforceability of their electronic agreements
- FIL-69-2001 (8/24/01)- *“FFIEC Guidance on Electronic Authentication”*
 - initially verifying the identity of **new** customers online
 - authenticating **existing** customers online
 - applies to retail & commercial customers
 - technology neutral
- Authentication tools need to consider migration from presentation of in-person credentials to electronic presentation

Authentication Basics

- Methodologies involve 3 factors:
 - something the user *knows* (e.g., password)
 - something the user *possesses* (e.g., ATM card)
 - something the user *is* (e.g., biometric, such as fingerprint)
- Single factor v. 2-factor v. 3-factor authentication
- Tiered single factor system
- Proper implementation is key

Risk Assessment

- Level of authentication used should be appropriate to the level of risk in application
- Method of authentication should be “appropriate and commercially reasonable” in light of the reasonably foreseeable risks in that application
- Currently, single factor authentication (i.e., passwords) is widely used & accepted
- 1-factor may not be commercially reasonable or adequate for high risk applications & transactions!

Risk Assessment

- Evaluate risk based on:
 - type of customer (retail or commercial)
 - transactional capabilities (bill pay, wire, loan origination)
 - sensitivity & value of stored information
 - ease of use
 - size & volume of transactions

Authenticating New Customers

- True online banking includes online account origination
- But, in e-banking environment, reliance on traditional paper proof of identity is decreased
- Alternatives are:
 - positive verification (applicant info matches 3rd party database)
 - logical verification (e.g., zip code matches street address)
 - negative verification (applicant info associated with fraud)
 - electronic credential issued by reliable source (digital certificate)

Authenticating Existing Customers

- Methods to authenticate existing customers:
 - Passwords & PINS
 - Digital certificates & PKI
 - Physical devices such as tokens
 - Biometric identifiers
- Banks should enforce controls to promote the integrity of the authentication method
- Educate customers on responsibilities and precautions
- FIL Appendix contains in-depth discussion

Passwords and PINS

- Most common method because its easy to use and integrate with existing systems
- Three aspects of passwords determine effectiveness: secrecy, length and composition, and system controls

Considerations for Passwords/PINS

FFIEC guidance states financial institutions need to consider:

- Selecting length/composition that balances ease of use with vulnerability to compromise -- minimum of 6 characters
- Locking-out users after excessive number of incorrect passwords -- no more than 5 incorrect attempts
- Disabling passwords after prolonged period of inactivity- 20 minutes
- Requiring new password after appropriate interval
- Implementing secure process for generating, distributing, and storing passwords
- Educating customers and employees on password selection and protection
- Incorporating a multi-factor authentication method for sensitive internal or high-value systems

CERT Advice

- Advice from another country's computer emergency response team (CERT):
- *“Passwords are like underwear: don't share them, hide them under your keyboard, or hang them from your monitor. Above all, change them frequently”*

Digital Certificates Using PKI

- A properly implemented and maintained PKI may provide a strong means of customer ID over the Internet.
- PKI can provide for authentication, data integrity, defenses against customer repudiation, and confidentiality
- PKI minimizes many of the vulnerabilities associated with passwords because it does not rely on shared secrets to authenticate customers and its electronic credentials are difficult to compromise
- More complicated & expensive

Considerations for Digital Certificates

- Defining the method of initial verification
- Selecting an appropriate validity period
- Selecting controls for issuing certificates
- Checking & updating CRL in real time
- Recording in a secure audit log all significant events performed by CA system

Tokens

- Tokens are access devices that represents something the customer possesses
 - smart cards, rings, key fobs, etc.
- Usually part of 2-factor system (e.g., +password)
- Password generating tokens provide an effective defense against password guessing because the token generates a new password at specific intervals

Biometrics

- A biometric identifier measures an individual's unique physical characteristic or behavior and compares it to a stored digital template to authenticate that individual
 - voice, fingerprints, hand or face geometry, eyes, signature, keyboard strokes
- Replaces PIN in 2-factor system
- Banks should consider privacy concerns when using biometric identifiers
 - Some customers may associate fingerprint-based biometric identifiers with law enforcement

Monitoring and Reporting

- Sound authentication system should include audit features to assist in detection of unusual activity & logs to reconstruct events
- Behavioral modeling to analyze unusual transactional activity
- Transaction \$ limits for large items and manual intervention to exceed preset limits
- Monitor IP addresses of incoming requests
- Report suspicious activities to regulators and law enforcement

Conclusion

- Reliable electronic authentication is essential in electronic banking
- Success depends on more than technology- strong policies, procedures & controls
- Effective authentication needs to be:
 - enterprise-wide
 - accepted by users
 - reliable
 - scalable
 - interoperable with future plans
 - commensurate with risk

Outsourcing and Vendor Management

Vendor Management Risk Issues

- Potential for banks to rush products to market without adequate consideration of
 - product risk assessment
 - vendor due diligence
 - contract negotiations, detailing responsibilities and review
 - ongoing monitoring
- Increased use of subcontractor products
- Financial condition uncertainty

FFIEC Guidance: “Risk Management of Outsourced Technology” (11/28/00)

- Key elements of the risk management process:
 - Risk assessment
 - Due diligence in selecting service provider
 - Contract Requirements
 - Oversight of service provider

Regardless of the decision to outsource, the bank remains ultimately responsible.

Outsourcing - GLBA Implications

- GLBA Guidelines to Safeguard Customer Information requires banks to:
 - Exercise appropriate due diligence in selecting its service providers
 - Require its service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines
 - Monitor (where indicated by the bank's risk assessment) its service providers to confirm that they have satisfied their obligations

Note: "Service provider" is defined broadly in the regulation

Regulatory Oversight of Service Providers

- Authority derives from the Bank Service Company Act of 1962
- Interagency exams are coordinated by the FFIEC Information Systems Subcommittee
 - MultiRegional Data Processing Servicer Program (MDPS)
 - Shared Application Software Review Program (SASR)
- Recently, Internet banking service providers have been included in the MDPS program
- Onsite exams are staffed by examiners from all agencies and a joint report is produced

Regulatory Oversight of Service Providers

- Copies of the exam report can be obtained by client banks only from the regional office of their primary federal regulator
- Exam reports are not a substitute for due diligence and oversight by bank management (e.g., regular receipt of independent audits and security reviews)
- The scope and frequency of the exams should be considered when using the reports as a resource

Security: Key Elements of
Interagency “Guidelines
Establishing Standards to
Safeguard Customer
Information”

GLBA Privacy and Information Security Guidelines

- Mandated by Gramm-Leach-Bliley Act
 - Recognizes that there is not privacy without security
- Privacy Regulation requires notice and opportunity to opt out
- Guidelines establishes administrative, technical & physical safeguards to protect the privacy of customers' nonpublic customer records and information
- July 1, 2001 implementation date

Objectives of GLBA Information Security Guidelines

- Ensure security/confidentiality of customer records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer

Security Guidelines Process

Involve Board of Directors

- Board (or an appropriate committee) shall:
 - Approve the written information security program
 - Oversee the development, implementation, and maintenance of the information security program
 - Assign specific responsibility for implementation
 - Review reports (at least annually) from management

Security Guidelines Process

- Identify and assess risks to customer information and protection mechanisms
 - Identify reasonably foreseeable internal and external threats
 - Assess the likelihood and potential damage of these threats taking into consideration the sensitivity of customer information
 - Assess the sufficiency of policies, procedures, customer information systems, and other arrangements

Security Guidelines Process

- In designing and implementing information security program, banks *should consider* the following controls:
 - Access controls
 - Access restrictions at physical locations
 - Encryption of electronic information (transit & storage)
 - System modification procedures
 - Dual control procedures, segregation of duties, employee background checks
 - Monitoring systems
 - Response programs
 - Protect against destruction, loss, damage

Security Guidelines Process

- Test key controls (at least annually)
- Train personnel
- Adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal/external threats to information security

For more information see Web sites of banking agencies

- FDIC: www.fdic.gov
- FRB: www.frb.gov
- OCC: www.occ.treas.gov
- OTS: www.ots.treas.gov
- NCUA: www.ncua.gov
- FFIEC: www.ffiec.gov



Each depositor insured to \$100,000

[SITEMAP](#) [SEARCH](#) [HELP](#) [HOME](#)

Federal Deposit Insurance Corporation

[Deposit Insurance](#)
[Bank Data](#)
[Regulations & Examination](#)
[Consumers & Communities](#)
[Buying From, Selling to FDIC](#)
[Newsroom, Events, & FOIA](#)
[About FDIC](#)

Quick Search

 [Find it](#)
[Advanced Search](#)

Regulations & Examination

- ◆ [Resources for Bankers](#)
- ◆ [Examinations](#)
 - ◆ [Community Reinvestment Act](#)
 - ◆ [Compliance](#)
 - ◆ [Information Systems & E-banking](#)
 - ◆ [Safety & Soundness](#)
 - ◆ [Trust](#)
- ◆ [Laws & Regulations](#)
- ◆ [Examiner Training Program](#)

Examinations: Information Systems & E-banking

Federal regulatory examination procedures specifically address banks' use of data processing in their business.



[FFIEC Information Systems Examination Handbook](#)

The Federal Financial Institutions Examination Council (FFIEC) handbook for conducting examinations of banks' and savings associations' information systems, used by the FDIC and the other federal financial institution regulatory agencies.

[Electronic Banking Examination Procedures](#)

(217Kb PDF file - [PDF help](#) or [hard copy](#))

A supplement to the FDIC [Manual of Examination Policies](#) focusing on banks' and savings institutions' ventures in electronic commerce, to help financial institutions minimize risk for themselves and for their depositors.

[Bank Technology Bulletins](#)

Time-sensitive, highly focused information on bank technology topics.

[Technology Regulations and Publications for Financial Institutions](#)

Hyperlinks to technology-related regulations and other publications issued by the federal banking agencies.

Office



Start



Internet



1:51 PM

Microsoft

File Edit View Favorites Tools Help | Address <http://www.occ.treas.gov/netbank/netbank.htm> Go

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Real.com

Links - OCCnet Directory - OCCnet Home Outlook Web Access SWD BIT FedTravel RealPlayer



Comptroller of the Currency
Administrator of National Banks

[HOME](#) | [CONTACT THE OCC](#) | [DIRECTORY](#) | [SUBJECT INDEX](#) | [SITE MAP](#)

ELECTRONIC BANKING

Search this Site:

[Search Tips](#)

- WHAT'S NEW**
- ABOUT THE OCC**
- BANKER EDUCATION**
- CAREERS AT THE OCC**
- COMMUNITY AFFAIRS**
- CORPORATE APPLICATIONS**
- CRA INFORMATION**
- CUSTOMER ASSISTANCE**
- ELECTRONIC BANKING**

- News, Press Releases and Speeches
- Internet Banking Guidance
- Opinions and Letters
- [Establishing an Internet](#)

- **[OCC News, Press Releases, and Speeches](#)** - These issuances are the most recent OCC news items on Internet Banking activities.
- **[OCC Internet Banking Guidance](#)** - OCC issues guidance to ensure national banks and their service providers and software vendors maintain safe and sound banking practices.
- **[OCC Opinions and Letters on Permissible Electronic Banking Activities](#)** - OCC publishes letters associated with charter approvals and other licensing activities, including interpretive letters.
- **[Establishing an Internet Bank](#)** - OCC has a formal application and approval process to become a chartered national bank, as outlined in the OCC Corporate Manual.
- **[Research and Analysis](#)** - OCC occasionally publishes research and analysis on a variety of topics, including Internet Banking and electronic commerce issues.
- **[International Electronic Banking Supervision](#)** - OCC participates in meetings with foreign bank supervisors and the Electronic Banking Group of the Basel Committee on Banking Supervision to promote effective supervision of cross-border electronic banking activities. The following reports discuss electronic banking risks from an international perspective.

OTS

SEARCH HELP HOME

Office of Thrift Supervision

News & Events	Applications	Supervision	Public Info	Consumer & Community	Data & Research	TFR	About OTS
--------------------------	---------------------	--------------------	--------------------	---------------------------------	----------------------------	------------	------------------

News & Events

- What's New
- Press Releases
- Upcoming Events
- Speeches & Testimony

Applications

- Application Status Reports
- How to File an Application

Supervision

- Laws and Regulations
- Issuances
- Handbooks

Public Info

- FOIA
- Privacy Act
- Publication List
- Public Use Forms
- Enforcement

Consumer & Community

- Community Affairs

Quick Navigation

Updated: Thursday, September 06, 2001 at 3:39 PM EDT

Welcome to the redesigned Office of Thrift Supervision web site. Based on your feedback, we have reorganized the content and information on this site to better serve our visitors. (6/20/01) [New Navigation Assistance](#)

The OTS is the primary regulator of all federal and many state-chartered thrift institutions, which include savings banks and savings and loan associations. The OTS was established as an office of the Department of the Treasury on August 9, 1989. The OTS has five regional offices located in [Jersey City](#), [Atlanta](#), [Chicago](#), [Dallas](#), and [San Francisco](#). Its expenses are funded by assessments and fees levied on the institutions it regulates. This Web site provides access to information on the agency's programs and activities. We hope you find the material informative and helpful.

Office of Thrift Supervision

1700 G. Street, NW
Washington, DC 20552
202-906-6000



You are entering an official United States government system, which may be used only for authorized purposes. Unauthorized modification of any information stored on this system may result in criminal prosecution.

View our [monitoring and privacy policy statement](#).

Board of Governors of the Federal Reserve System

- General Information
- Press Releases
- Testimony and Speeches
- Monetary Policy
- Banking System
- Regulation and Supervision
- Research and Data
- Consumer Information
- Community Affairs
- Reporting Forms
- Publications
- Career Opportunities

Breaking News

- **Draft Check Truncation Act available for comment**
- **Speech by Governor Gramlich on infrastructure and economic development**
- **Compliance date lifted for electronic consumer disclosures**
- **Testimony of Governor Meyer on the securities activities of banks**

20th Street and Constitution Avenue, NW, Washington, DC 20551



The Federal Reserve, the central bank of the United States, was founded by Congress in 1913 to provide the nation with a safer, more flexible, and more stable monetary and financial system.

Today the Federal Reserve's duties fall into four general areas: (1) conducting the nation's monetary policy; (2) supervising and regulating banking institutions and protecting the credit rights of consumers; (3) maintaining the stability of the financial system; and (4) providing certain financial services to the U.S. government, the public, financial institutions, and foreign official institutions.

- [FOIA](#)
- [FAQ](#)
- [Search](#)
- [Site Map](#)
- [Web Publication Schedule](#)
- [What's New](#)
- [Accessibility](#)
- [Disclaimer](#)
- [Privacy Policy](#)

Office

Microsoft

Questions?

Contact Information

Cynthia A. Bonnette

Tel. 202-736-0528

e-mail: cybonnette@fdic.gov

Jeff Kopchik

Tel. 202-898-XXXX

e-mail: jkopchik@fdic.gov



John Carlson

Tel. 202-874-5013

e-mail: john.carlson@occ.treas.gov



Robert Engebreth

Tel. (202) 906-5631

e-mail: robert.engebret@ots.treas.gov

