OCC Telephone Seminar
Internet Banking Security:
Safeguarding Customer Information

Table of Contents

Speaker Biographies

John D. Hawke, Jr.

Comptroller of the Currency

John D. Hawke, Jr. was sworn in as the 28th Comptroller of the Currency on December 8, 1998. After serving for 10 months under a Recess Appointment, he was sworn in for a full five-year term as Comptroller on October 13, 1999.

The Comptroller of the Currency is the Administrator of National Banks. The Office of the Comptroller (OCC) supervises 2,600 federally chartered commercial banks and about 66 federal branches and agencies of foreign banks in the United States comprising more than half of the assets of the commercial banking system. The Comptroller also serves as a Director of the Federal Deposit Insurance Corporation, the Federal Financial Institutions Examination Council, and the Neighborhood Reinvestment Corporation.

Prior to his appointment as Comptroller, Mr. Hawke served for 3-1/2 years as Under Secretary of the Treasury for Domestic Finance. In that capacity he oversaw the development of policy and legislation in the areas of financial institutions, debt management and capital markets, and served as Chairman of the Advanced Counterfeit Deterrence Steering Committee and as a member of the board of the Securities Investor Protection Corporation. Before joining Treasury, Mr. Hawke was a Senior Partner at the Washington, D.C. law firm of Arnold & Porter, which he first joined as an associate in 1962. At Arnold & Porter he headed the Financial Institutions practice, and from 1987 to 1995 he served as Chairman of the firm. In 1975 he left the firm to serve as General Counsel to the Board of Governors of the Federal Reserve System, returning in 1978.

Mr. Hawke graduated from Yale University in 1954 with a B.A. in English. From 1955 to 1957 he served on active duty with the U.S. Air Force. After graduating in 1960 from Columbia University School of Law, where he was Editor-in-Chief of the Columbia Law Review, Mr. Hawke was a law clerk for Judge E. Barrett Prettyman on the United States Court of Appeals for the District of Columbia Circuit. From 1961 to 1962 he served as counsel to the Select Subcommittee on Education in the House of Representatives.

From 1970 to 1987 Mr. Hawke taught courses on federal regulation of banking at the Georgetown University Law Center. He has also taught courses on bank acquisitions and financial regulation and serves as the Chairman of the Board of Advisors of the Morin Center for Banking Law Studies.

In 1987 Mr. Hawke served as a member of a Committee of Inquiry appointed by the Chicago Mercantile Exchange to study the role of futures markets in connection with the stock market crash in October of that year.

Mr. Hawke has written extensively on matters relating to the regulation of financial institutions, and is the author of "Commentaries on Banking Regulation," published in 1985. He was a founding member of the Shadow Financial Regulatory Committee, and served on the committee until joining Treasury in April 1995.

Mr. Hawke is a member of the Cosmos Club, the Economic Club of Washington and the Exchequer Club of Washington.

Born in New York City on June 26, 1933, Mr. Hawke resides in Washington, D.C. He was married in 1962 to the late Marie R. Hawke and has four adult children, Daniel, Caitlin, Anne and Patrick, and one grandchild, Spencer Patrick Hawke.

Clifford A. Wilke

Director, Bank Technology Division
Office of the Comptroller of the Currency

Clifford A. Wilke is director of Bank Technology at the Office of the Comptroller of the Currency in Washington, DC.

In that position, Mr. Wilke directs the formulation of policy and the development of examination tools and processes to supervise bank technology. He currently is a member of the OCC Privacy Working Group, National Risk Committee, and chairman of an internal team that is examining the issues surrounding Internet banking, account aggregation, and the future interaction of technology within the financial services industry.

Mr. Wilke joined the OCC after 17 years with Mobil Oil Corporation, and Mobil Oil Credit Corporation, where he led the development of the industry's first prepaid and multi-application card products (the Mobil GO CARD and Mobil MCI GO Card), and two of the six teams responsible for the initial development of Mobil SpeedPass. He has served on the board of directors of the Smart Card Forum and was one of the founders and chair of the Smart Card Forum Educational Institute, an organization dedicated to providing quality education in the field of smart cards to members of the public and private sectors.

Mr. Wilke is one of the co-authors of *Smart Cards — Seizing Strategic Business Opportunities*, published by McGraw-Hill and Company.

W. Carter Messick

Bank Technology Analyst

Office of the Comptroller of the Currency

W. Carter Messick serves as a national bank examiner in the Bank Technology Policy Division of the Office of the Comptroller of the Currency (OCC). He is responsible for developing supervision policy, examination guidance, and examiner training. He joined the OCC in 1989 after working as a credit officer at a community bank in Dallas, Texas.

Mr. Messick received his commission as a national bank examiner in 1993 and became a bank information technology specialist in 1994. He has led information technology examinations in community banks, mid-size regional banks, and bank service providers in both the Southeastern and Southwestern districts. From 1997 to March 2001, he served as the Southwestern District's lead information technology expert. In that position, he scheduled the district's information technology specialists and coordinated its Year 2000 and Internet banking examination coverage.

He received a Bachelor of Business Administration degree in finance and computer information systems from Baylor University in1985. He is a certified information systems auditor (CISA) and a certified information systems security professional (CISSP).

Joan Bryant

Bank Information Technology Specialist
Office of the Comptroller of the Currency

Joan Bryant serves as a national bank examiner in the Southwestern District of the Office of the Comptroller of the Currency (OCC). Ms. Bryant joined the OCC in 1990 and currently specializes in bank information technology examinations in the Southwestern District. She possesses a diverse examining background and has led supervisory reviews at community banks and servicers in both the northeast and southwest regions of the country. Ms. Bryant also has served as a resident information technology examiner in the OCC's Large Bank program for more than two years. In addition to her examining responsibilities, Ms. Bryant recently completed a one-year rotation as the lead instructor for the OCC's Internet Banking course for examiners.

Ms. Bryant was graduated from Southwestern University at Georgetown, Texas, where she received a B.A. in accounting. She is also a certified information systems auditor (CISA).

James F.E. Gillespie, Jr.

Assistant Chief Counsel

Office of the Comptroller of the Currency

James (Jeff) Gillespie currently serves as assistant chief counsel responsible for the management of special projects, particularly those that involve electronic banking and Year 2000 efforts.

Mr. Gillespie joined the OCC in 1979 after completing a federal judicial clerkship. He has held management and staff positions in the Legislative and Regulatory Activities Division, the Corporate Organization and Resolutions Division, the Litigation Division, the Legal Advisory Services Division, and the Legislative Counsel Division. He holds a J.D. from Indiana University (1976), where he was graduated summa cum laude and Order of the Coif. He received a B.A. from Ohio Wesleyan University (1971).

Deborah Katz

Senior Counsel

Law Department

Deborah Katz is a senior counsel in the Legislative and Regulatory Activities Division. She participated in drafting the Guidelines for Safeguarding Customer Information. She also has been involved in drafting a regulation implementing the affiliate information-sharing provisions of the Fair Credit Reporting Act and in the development of guidance on the joint final rule on Privacy of Customer Information.

Ms. Katz joined the OCC in 1986. She has been special assistant to the acting chief counsel and the deputy chief counsel, and has worked in the Enforcement and Compliance, Bank Organization and Structure, and Legal Advisory Services divisions.

She received a B.S. from the Edmund E. Walsh School of Foreign Service, Georgetown University, in 1979, and a J.D., from the Benjamin Cardozo School of Law, Yeshiva University, in 1986. She is a member of the New York Bar.

ELECTRONIC POLLING QUESTIONS

1. How many people are at your listening site? Press:

   1 for one person,
   2 for two people,
   3 for three people,
   4 for four people,
   5 for five people,
   6 for six people,
   7 for seven people,
   8 for eight people, or
   9 for 9 or more people listening at your site.

2. Did anyone at your site see the OCC ad for this telephone seminar in the American Banker newspaper?

   1 for yes,
   2 for no.

Internet Banking Security: Safeguarding Customer Information

Clifford Wilke
Carter Messick
Joan Bryant

July 18 & 19, 2001

Comptroller of the Currency
Administrator of National Banks

Internet Banking Security:
Safeguarding Customer Information

OCC Telephone Seminar
July 2001

Introduction and Key Issues
Clifford A. Wilke
Director, Bank Technology

Overview

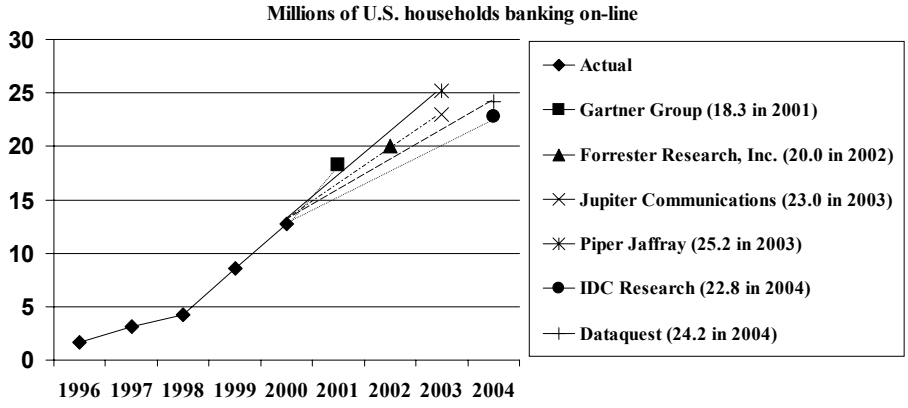
- Introduction
- Internet banking security risk assessment and program implementation
  - Why focus on security and authentication?
  - Where to start the process?
  - What to include in your security program?
  - How to monitor risk and test controls?
  - What about service providers?
- Conclusion
- Questions and answers

Technology Developments

- Advances in communication systems allow prompt delivery of products and services globally.
  - ⇨Internet has reached critical mass (60 percent of U.S. households have Internet access).
  - ⇨Rapid advances challenge the industry and regulators to keep pace.
- The networked environment provides instant, global access to information, products, and services.

U.S. On-Line Banking Usage Growth Projections

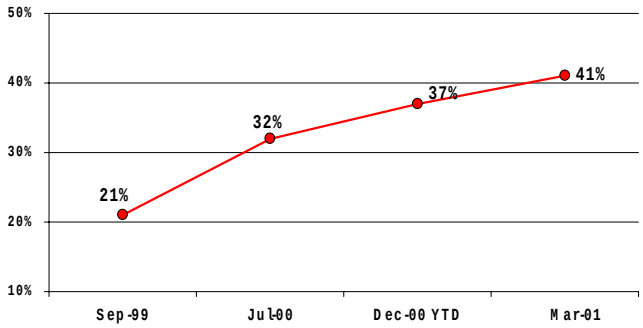
Comptroller of the Currency
Administrator of National Banks



Innovation in Financial Services

- Comprehensive on-line account history
- Financial services aggregation
- Bill payment and/or presentment
- Third-party electronic authentication and digital signatures
- Website hosting
- Wireless access

Growth in Number of National Banks that Have Transactional Websites



Source: Office of the Comptroller of the Currency. "Transactional websites" are defined as bank websites that allow customers to transact business. This may include accessing accounts, transferring funds, applying for a loan, establishing an account, or performing more advanced activities.

Internet Activities of National Banks

- 69 percent of the 2,342 national banks have a website.
- 52 percent of national banks expect to offer Internet banking by year end vs. 21 percent in September of 1999.

OCC Technology Risks Supervision Program

- Guidance
  - ⇨ Emphasis on risk analysis, measurement, controls, and monitoring that are consistent with risk tolerances and abilities
- Examiner training
- Risk-based examinations of banks and third-party service providers
  - ⇨ On-site and quarterly reviews
  - ⇨ Technology integration with safety and soundness exams
  - ⇨ Targeted reviews of banks with transactional websites and electronic banking service providers
- Enhanced application process for electronic banking activities
- External outreach and coordination

Security Self Assessment

- Is information security a priority for your bank's directors and senior management?
- Are you confident in the effectiveness of your written security program?
- Are you and your service providers ready to respond to security incidents?

Polling Question #1

Does your bank provide customers with access to account information through the Internet?

① Yes
② No
③ Not a banker

Internet Banking Security Risk Assessment and Program Implementation

W. Carter Messick
Bank Technology Analyst

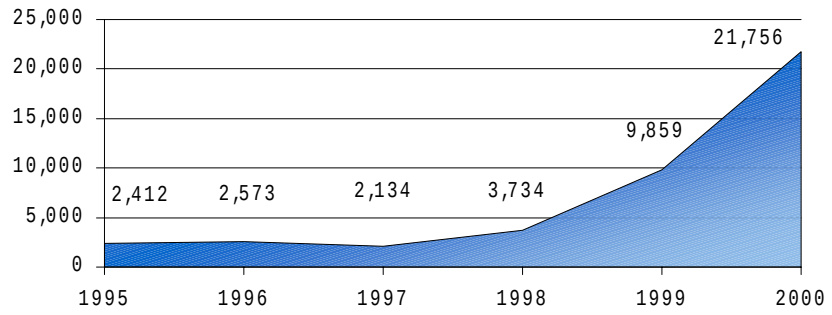
Joan Bryant
Bank Information Technology Specialist

Why focus on security?

Fraud and Intrusion Risk

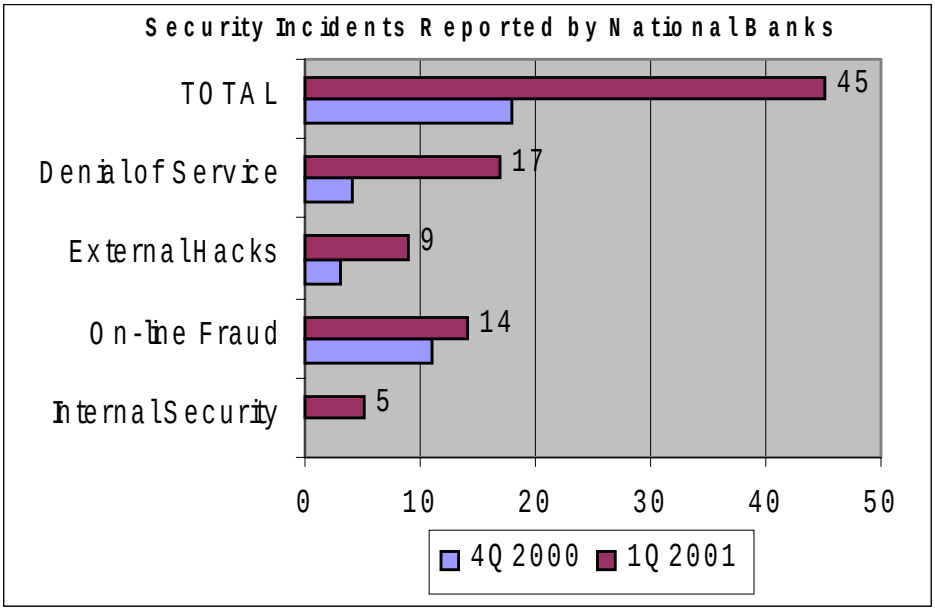
- OCC Alert 2001-4 and recent National Infrastructure Protection Center warnings
- Reports that bank and service provider hacks are increasing
- Identity theft and fraud
  - ⇨Recent Federal Trade Commission Report recorded 45,593 identity theft victims during a 16-month period.

Fraud and Intrusion Risk



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

Fraud and Intrusion Risk



Examination Findings

- Increasing examination coverage
  - ⇨ The OCC examined 863 of the 956 banks offering Internet banking, between July 2000 and March 2001.
  - ⇨ 76 percent of Internet banks reported that they outsourced their Internet banking application and virtually all major Internet banking service providers have been examined.

Examination Findings

Key Success Factors:

- Active vendor management
- Ongoing board involvement
- Sufficient technical expertise
- Proactive network security that effectively prevents, detects, and responds to intrusions
- Strong authentication practices
- Encrypted communications
- Periodic compliance and legal reviews
- Appropriate backup and recovery

Regulatory Requirements

OCC Bulletin 2001- 8: Interagency Guidelines for Safeguarding Customer Information

- Gramm-Leach-Bliley section 501(b) requirements
- Implementation by July 1, 2001 of a comprehensive written information security program appropriate to the size and complexity of the bank's operations
- All aspects of bank operations
- Future examination coverage

Regulatory Requirements

Elements of the Information Security Program required by the Guidelines

- Involve the board of directors
- Assess the risk
- Manage and control risks (including access control, testing and employee training)
- Oversee service providers
- Adjust the program
- Report to the board

Where to start?

Security Objectives for Safeguarding Customer Information

OBJECTIVES		OUTCOME
Confidentiality + Integrity	=	Non-repudiation & Privacy

Risk Assessment

The risk assessment provides the foundation upon which you develop and maintain your information security program.

Risk Assessment

The 501(b) Guidelines for Safeguarding Customer Information require banks to:

- Identify *reasonably foreseeable* internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer-information systems.
- Assess the likelihood and potential damage of these threats, considering the *sensitivity* of customer information.
- Evaluate the sufficiency of policies, procedures, customer-information systems, and other arrangements to control risks.

Internet Banking Threats

Threats

- Theft of data or dollars
- Altered data
- Systems degradation

Types of Attacks

- System penetration
- Planting
- Eavesdropping (a.k.a. sniffing)
- Communications tampering (a.k.a. spoofing)
- Denial of service
- Repudiation

Risk Assessment

Considerations could include...

- Internet connectivity
- Informational or transactional website
- Types of transactions supported
- Types of electronic funds transfers...retail or commercial
- In-house or outsourced systems
- Website hosting or transaction processing for others
- State of your conventional controls over document destruction, faxes, E-mail usage
- Extent of security awareness among your staff
- Extent of existing network security tools and expertise

Is this a one-time process? NO

Polling Question #2

Has your bank completed a security risk assessment?

① Yes
② No
③ Don't know
④ Not a banker

What to include in your security program?

Administrative Controls

- Employee security awareness and training
- Employee background checks
- Security expertise and employee accountability
- Current security configurations with changes that are documented, approved, and tested
- Policies and procedures, that may include:
  - ⇨Employee Internet and E-mail usage, customer agreements, security administration, password administration, firewall policy, third-party access, change control, verification procedures, termination procedures, and information confidentiality.

Administrative Controls

Case 1 - Administrative Controls

- Bank statements had the customers' social security number (SSN) printed on them.
- The bank also automatically activated all customers for Internet banking and used the last four digits of SSN as the default password for the initial log-in.
- A customer moved without logging on to the Internet banking system.
- A new resident moved in and received the customer's bank statement.
- The new resident then used the SSN to log-on to the bank's bill payment application to move money out of the customers account.

Case One - Lessons Learned

- Avoid printing confidential customer information on bank statements or other widely distributed reports.
- Do not use a common identifier like a social security number as part of the log-in process.
- Require customers to request activation of Internet banking service
- Give the customer the option of setting up their own initial password to strengthen its confidentiality

Administrative Controls

Authentication

- Account Origination and Customer Verification
  - ⇨Use of third-party fraud detection services
  - ⇨Tolerance for mismatched application information
- Funds Transfers and Transaction Initiation
  - ⇨Internet-initiated ACH transactions (NACHA rules)
  - ⇨Passwords vs. multi-factor authentication
  - ⇨Review unusual funds transfer activities
- Account Maintenance Changes
  - ⇨Consider out-of-wallet questions
  - ⇨Consider information not found on a bank statement
- Pre-text calls

Administrative Controls

Case 2 - Authentication

- An employee of bank A steals customer account information of several wealthy customers.
- She uses the stolen customer information to originate new accounts on-line with bank B under the other identities.
- She transfers funds from the legitimate accounts at bank A to the fraudulent account at bank B.

Case Two - Lessons Learned

- Bank A should review their employee background check policy
- Bank B should improve their authentication process. If properly used, fraud detection systems can fairly effectively identify potentially fraudulent application information.

Physical Controls

- Media protection and disposal
- Computer hardware protection and disposal
- Limited employee and public access
- Physical segregation of duties

Automated Controls

- Use the security capabilities of applications and operating systems.
- Secure operating systems by removing exploitable files and services.
- Encrypt sensitive communications and data storage.
- Install and update virus detection software on all desktops and servers.
- Subscribe to vulnerability monitoring services for notification of security patches.
- Restrict network access through firewalls, remote access, and physical isolation.

Automated Controls

Firewall Considerations

- **Management Accountability and Expertise**
  - ⇨ Establish responsibility for firewall implementation and monitoring.
- **Hardware Configuration**
  - ⇨ Determine how best to achieve physical security.
  - ⇨ Review system diagram to understand firewall placement.
- **Software Configuration**
  - ⇨ Review firewall rules to determine what traffic is allowed and if all traffic is denied, unless expressly allowed.
- **Change Management**
  - ⇨ Determine the change controls in place that assure prompt and controlled upgrades, including securing remote access.
  - ⇨ Update system for new vulnerabilities.

Automated Controls

Case 3 - Security Patches

- A hacker scans a bank's web server and finds a vulnerability.
- He exploits the vulnerability and gains access to the Internet banking server.
- He downloads the encrypted password file and customer files.
- The bank learns they were hacked several weeks later, but has no idea what the hacker has done with the information.
- They research the vulnerability that was exploited and find that a software fix or patch was readily available.

Case 3 - Lessons Learned

- Banks with in-house systems need to have an effective process to track and install security patches.
- Banks like this one should strongly consider implementing an Intrusion detection systems.
- Banks can detect vulnerabilities themselves by periodically performing vulnerability assessments.

How to monitor risk and test controls?

Security Monitoring and Testing Methods

- System Monitoring
- Intrusion Detection
- Intrusion Response
- Security Audits
- Vulnerability Assessment
- Penetration Testing

System Monitoring

- Security reports and logs
  - ⇨Event reports
  - ⇨Firewall policy exceptions and real-time alerts
  - ⇨Failed access attempts
  - ⇨Periodic reviews of access rights
- Security management software
  - ⇨Enforce security policies across multiple servers (measures policy compliance)
- Change Control Logs

Intrusion Detection

Intrusion detection systems are used to detect unauthorized access to, or misuse of, a computer network. Software can analyze incoming or outgoing traffic for known attack signatures.

OCC Bulletin 2000-14: Infrastructure Threats -- Intrusion Risks

Intrusion Response

- Prioritize the sequence of actions for intrusion response
  - Contain the activity and eliminate the vulnerability.
  - Determine if systems will remain operational or if they must be shut down.
- Gather and maintain evidence.
- Communicate employee responsibilities and escalation procedures for senior management notification.
- Identify steps to restore and test systems.
- Notify affected customers, regulators, information sharing organizations, and law enforcement agencies -- including completion of a Suspicious Activity Report.

Do serviced banks need a response plan? ***YES***

Why notify customers if no money is lost? ***Reputation risk and legal liability***

Security Audits

Internal or external audits/tests of security controls consistent with your risks.

- Physical security of customer information and information systems
- Funds transfer security
- Internet banking application security
- Network security including remote system access and Internet access

Vulnerability Assessment

A review of the bank's systems to identify known weaknesses that could be exploited.

- Network- or host-based
- Conducted periodically
- Qualified personnel using appropriate tools
  - ⇨Bank personnel or third party
  - ⇨Commercially available software tools
- Verifies and tests your patch process and configuration management
- Prompt follow up and corrective action

Penetration Testing

System is subjected to real-world attacks selected by the testing personnel.

- Performed with or without inside knowledge.
- Often starts by using vulnerability assessment tools to gain intelligence about the target's systems and determine potential weaknesses.
- Tests actual effectiveness of security controls including your intrusion detection and response controls.
- Select reputable third parties, define the scope, obtain a non-disclosure agreement, and obtain assurance that all test-related information will be destroyed or returned to the bank.

Polling Question #3

Has your bank or service provider experienced a security incident that resulted in a potential privacy breach?

① Yes
② No
③ Don't know
④ Not applicable

What about my service providers?

Regulatory Requirements Related to Service Providers [1]

Oversee service providers by:

- Addressing them in their **risk assessment.**
- Performing **due diligence** in selecting them.
- Requiring them by **contract** to implement appropriate measures designed to meet the objectives of the Guidelines for Safeguarding Customer Information (due in all contracts after March 5, 2001).
- **Monitoring** them to confirm that they have met their obligations. Monitoring may include reviewing audits, test result summaries, and periodic reports.

[1]See OCC Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information" and OCC Advisory Letter 2000-12, "Risk Management of Outsourced Technology Services".

Typical Service Provider Reports

- SAS 70 Audit Reports
  - ⇨ Identify specified control objectives
    - Customer involvement
    - Include network security, security oversight, and telecommunications
  - ⇨ Type 2 - Includes actual testing of controls
  - ⇨ Timing (annual, biannual)
    - Gaps in reporting periods
    - Pace-of-change in control environment
    - Delays in report availability
- Security assessment, penetration test, and security incident reports

  Document your analysis of these reports and periodically discuss with the board.

Questions to Consider When Selecting a Service Provider

- Who are their other bank clients, and what do banks with similar operations and systems say about the services?
- Have they conducted a security risk assessment?
- Do they have a written information security program consistent with the 501(b) Guidelines?
- Does a data center tour reveal a strong commitment to security?
- Does the application have adequate security capabilities?
- Will they define clearly their security responsibilities in the contract?
- Do they audit or test their security controls regularly?
- Will they provide the results of their audits or tests?
- Do they have a clear security incident handling plan that includes communication with bankers?
- Do they have personnel dedicated to security oversight?
- Do they have a privacy policy consistent with your bank's policy?

Service Providers

Case 4 - Small Service Provider

- A customer bank identifies fraudulent Internet banking activity on one of their customer's accounts.
- An investigation shows that proper user IDs and passwords were used, but the customer insists they did not initiate the transactions.
- The service provider investigates and determines that their firewall was breached.
- Hacker obtained access to user IDs and passwords.

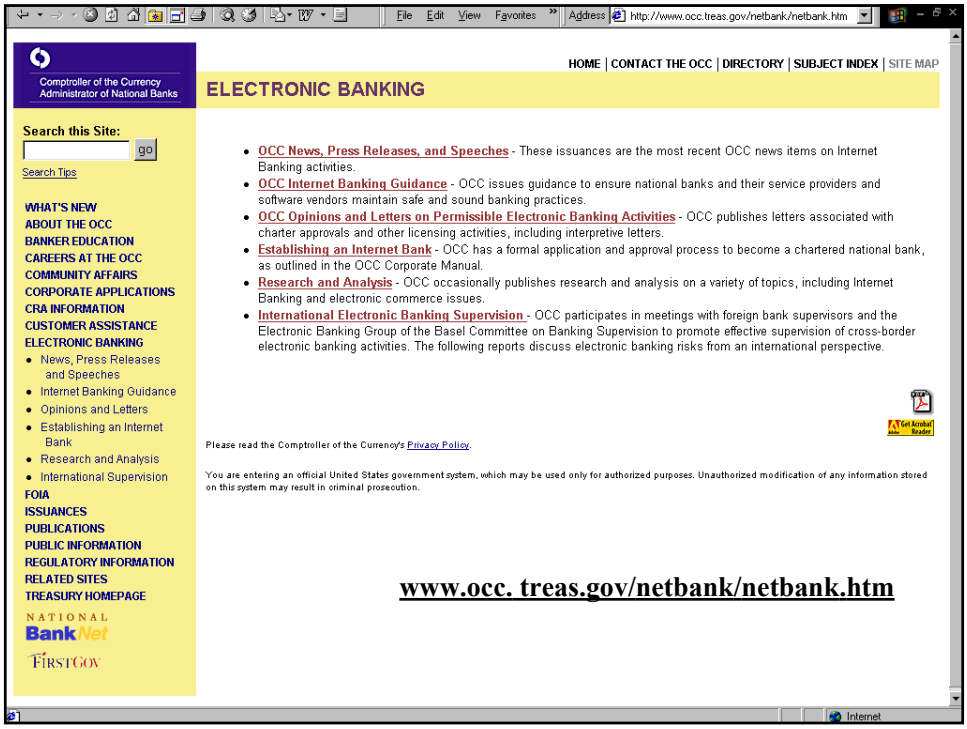
Case 4 - Lessons Learned

- You cannot outsource your security responsibilities.
- You should ensure that your providers firewall and security controls are independently tested and evaluate the adequacy of the tests.
- You may need to establish more conservative password composition standards.
- You need to talk to your service provider about their intrusion response plan before an intrusion.

Conclusion

OCC Security-Related Issuances

- Basle Committee's Risk Management Principles for Electronic Banking
- AL 2001-4 Identity Theft and Pretext Calling - 4/30/2001
- ALERT 2001-4 Network Security Vulnerabilities - 4/24/2001
- OCC 2001-12 Bank Provided Account Aggregation - 2/28/2001
- OCC 2001-8 Safeguarding Customer Information - 2/15/2001
- AL 2001-3 Internet-Initiated ACH - 1/29/2001
- AL 2000-12 Risk Management of Outsourcing - 11/28/2000
- OCC 2000-19 Suspicious Activity Reports - 6/19/2000
- OCC 2000-14 Intrusion Risk - 5/15/2000
- OCC 98-38 PC Banking - 8/24/1998
- OCC 98-3 Technology Risk Management - 2/4/1998
- BC 229 - Information Security - 5/31/1988



Websites with Security Resources

- www.occ. treas.gov/netbank/netbank.htm
- www.sans.org
- www.cert.org
- www.nipc.gov
- www.cerias.purdue.edu/
- www.cve.mitre.org

Conclusion

The future of Internet banking depends on all banks making information security a priority.

Bank Motivators

- Customer acceptance
- Computer crime
- Legal liability
- Insurance requirements
- Bank Reputation
- Regulatory expectations

Bank Action Items

- Complete a risk assessment
- Implement effective security program
  - ⇨Board involvement
  - ⇨Controls
  - ⇨Monitoring
  - ⇨Third-party oversight

Appendix

Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness

This document contains revisions to 12 CRF 30 to incorporate Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

The full text of the notice published in the Federal Register can be found on the OCC's public website as News Release 2004-1.

Office of the Comptroller of the Currency

12 CFR Chapter I

Authority and Issuance
For the reasons set forth in the joint preamble, part 30 of the chapter I of title 12 of the Code of Federal Regulations is amended as follows:

Part 30 -- SAFETY AND SOUNDNESS STANDARDS

1. The authority citation for part 30 is revised to read as follows:
Authority: 12 U.S.C. 93a, 1818, 1831-p, 3102(b); 15 U.S.C. 6801, 6805(b)(1).

2. Revise § 30.1 to read as follows:.

§ 30.1 Scope.

(a) This rule and the standards set forth in appendices A and B to this part apply to national banks and federal branches of foreign banks, that are subject to the provisions of section 39 of the Federal Deposit Insurance Act (section 39)(12 U.S.C. 1831p-1).
(b) The standards set forth in appendix B to this part also apply to uninsured national banks, federal branches and federal agencies of foreign banks, and the subsidiaries of any national bank, federal branch or federal agency of a foreign bank (except brokers, dealers, persons providing insurance, investment companies and investment advisers). Violation of these standards may be an unsafe and unsound practice within the meaning of 12 U.S.C. 1818.

3. In § 30.2, revise the last sentence to read as follows:

§ 30.2 Purpose.
* * * The Interagency Guidelines Establishing Standards for Safety and Soundness are set forth in appendix A to this part, and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information are set forth in appendix B to this part.

4. In § 30.3, revise paragraph (a) to read as follows:

§ 30.3 Determination and notification of failure to meet safety and soundness standard.
(a) *Determinatio*n. The OCC may, based upon an examination, inspection, or any other. information that becomes available to the OCC, determine that a bank has failed to satisfy the safety and soundness standards contained in the Interagency Guidelines Establishing Standards for Safety and Soundness set forth in appendix A to this part, and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information set forth in appendix B to this part.
* * * * *

5. Revise appendix B to part 30 to read as follows:

Appendix B to Part 30 -- Interagency Guidelines Establishing Standards For Safeguarding Customer Information

Table of Contents

I. Introduction

The Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) set forth standards pursuant to section 39 of the Federal Deposit Insurance Act (section 39, codified at 12 U.S.C. 1831p-1), and sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

A. Scope. The Guidelines apply to customer information maintained by or on behalf of entities over which the OCC has authority. Such entities, referred to as "the bank," are national banks, federal branches and federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

B. Preservation of Existing Authority. Neither section 39 nor these Guidelines in any way limit the authority of the OCC to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. The OCC may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to the OCC..76

C. Definitions.

1. Except as modified in the Guidelines, or unless the context otherwise requires, the terms used in these Guidelines have the same meanings as set forth in sections 3 and 39 of the Federal Deposit Insurance Act (12 U.S.C. 1813 and 1831p-1).

2. For purposes of the Guidelines, the following definitions apply:

a. Board of directors, in the case of a branch or agency of a foreign bank, means the managing official in charge of the branch or agency.

b. Customer means any customer of the bank as defined in § 40.3(h) of this chapter.

c. Customer information means any record containing nonpublic personal information, as defined in § 40.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the bank.

d. Customer information systems means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

e. Service provider means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank.

II. Standards for Safeguarding Customer Information

A. Information Security Program. Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

B. Objectives. A bank's information security program shall be designed to:.

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

II. Development and Implementation of Information Security Program

A. Involve the Board of Director*s.* The board of directors or an appropriate committee of the board of each bank shall:

1. Approve the bank's written information security program; and

2. Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. Assess Risk. Each bank shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

C. Manage and Control Risk. Each bank shall:

1. Design its information security program to control the identified risks, commensurate. with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

d. Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;

e. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

g. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

h. Measures to protect against destruction, loss, or damage of customer information due. to potential environmental hazards, such as fire and water damage or technological failures.

2. Train staff to implement the bank's information security program.

3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

D. Oversee Service Provider Arrangements. Each bank shall:

1. Exercise appropriate due diligence in selecting its service providers;

2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and

3. Where indicated by the bank's risk assessment, monitor its service providers to

confirm that they have satisfied their obligations as required by section D.2. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. Adjust the Program. Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. Report to the Board. Each bank shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank's compliance with these Guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

G. Implement the Standards.

1. Effective date. Each bank must implement an information security program pursuant to these Guidelines by July 1, 2001.

2. Two-year grandfathering of agreements with service providers. Until July 1, 2003, a contract that a bank has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of section III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of customer information, as long as the bank entered into the contract on or before [Insert date thirty days after date of publication in the Federal Register].

6. Appendix C to part 30 is removed.

[THIS SIGNATURE PAGE PERTAINS TO THE OCC'S PORTION OF THE. "INTERAGENCY GUIDELINES ESTABLISHING STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION AND RESCISSION OF YEAR 2000 STANDARDS FOR SAFETY AND SOUNDNESS"]

Dated: _____

_____

John D. Hawke, Jr.,
Comptroller of the Currency.