

# COMPLIANCE

GUIDELINES WE FOLLOW

[theWEBcentric.com](http://theWEBcentric.com)



“You must keep in mind that “FFIEC compliance” does not necessarily constitute compliance with any of the 5 regulatory agencies (FDIC, NCUA, FRB, OCC, OTS) that make up the FFIEC.”

Janet Wilth, Senior Systems Auditor, CISA, CISM Certified

Janet has more than 25 years of information security experience in regulated industries, including 22 years in financial services. Prior to joining SPC, Janet was Vice President – Manager, Information Security at RBC Dain Rauscher, where she directed the development of policies, procedures and controls to ensure compliance with GLBA, SOX and IS17799 (now ISO 27002). Janet's experience also includes participation in Board of Governors audits while employed at the Federal Reserve Bank of Minneapolis. Janet's core areas of expertise include identifying and analyzing risk, and designing and implementing controls to mitigate risk.

# THE TRUTH AND FACTS ABOUT FFIEC COMPLIANCE

## FFIEC COMPLIANCE

How can an IT service provider achieve FFIEC compliance? I was recently asked this question and my initial response was “the FFIEC is not a regulatory body therefore there is no such thing as FFIEC compliance.” I was told there are companies marketing their products and services as FFIEC compliant so I decided to investigate the definition of FFIEC compliance.

Title 12 of the Code of Federal Regulations defines the FFIEC as:

§ 1101.2 Authority and functions.

(a) The Council was established by the Federal Financial Institutions Examination Council Act of 1978 (Act), 12 U.S.C. 3301–3308. It is composed of the Comptroller of the Currency; the Chairman of the Federal Deposit Insurance Corporation; a Governor of the Board of Governors of the Federal Reserve System; the Chairman of the Federal Home Loan Bank Board; and the Chairman of the National Credit Union Administration Board.

(b) The statutory functions of the Council are set out at 12 U.S.C. 3305. In summary, the mission of the Council is to promote consistency and progress in federal examination and supervision of financial institutions and their affiliates. The Council is empowered to prescribe uniform principles, standards, and reporting forms and systems; make recommendations in the interest of uniformity; and conduct examiner schools open to personnel of the agencies represented on the Council and employees of state financial institutions supervisory agencies.

The FFIEC.gov home page uses the following definition:

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS), and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the State Liaison Committee (SLC) was added to the Council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).

These definitions of the FFIEC seemed to support my initial statement so I investigated further and found most IT service providers who use the term FFIEC compliance are marketing authentication products and services. The following is the definition I found on Whatis.com:

FFIEC compliance is conformance to a set of standards for online banking issued in October 2005 by the Federal Financial Institutions Examination Council (FFIEC). The standards require multifactor authentication (MFA) because single-factor authentication (SFA) has proven inadequate against the tactics of increasingly sophisticated hackers, particularly on the Internet. In MFA, more than one form of authentication is implemented to verify the legitimacy of a transaction. In contrast, SFA involves only a user ID and password.

I also found several IT services providers marketing intrusion detection systems (IDS) or security log management (SLM) products as FFIEC compliant. These companies often reference the FFIEC IT examination handbooks as their source of compliance requirements.

The conclusion drawn, based on this research, is that there is not one commonly held definition of FFIEC compliance associated with IT services. The FFIEC IT Examination handbooks contain a total of 686 unique controls; true FFIEC compliance would be achieved by analyzing all 686 controls, and implementing and documenting those controls that apply to the IT services offered by the provider.

I recommend the consumer ask their IT service provider for their definition of FFIEC compliance to ensure a common understanding of the compliance issues addressed by the IT service provider's product. You must keep in mind that “FFIEC compliance” does not necessarily constitute compliance with any of the 5 regulatory agencies (FDIC, NCUA, FRB, OCC, OTS) that make up the FFIEC. Remember when outsourcing IT services, you can delegate authority, not responsibility. Your regulator will hold your institution responsible for compliance, not the IT service provider.



#### APPENDIX C: LAWS, REGULATIONS, AND GUIDANCE LAWS

12 USC 1867(c): Bank Service Company Act  
12 USC 1882: Bank Protection Act  
15 USC 1681w: Fair and Accurate Credit Transactions Act  
15 USC 6801 and 6805(b): Gramm–Leach–Bliley Act  
18 USC 1030: Fraud and Related Activity in Connection with Computers

#### FEDERAL RESERVE BOARD REGULATIONS

12 CFR 208.61: Minimum Security Devices and Procedures  
12 CFR 208.62: Reports of Suspicious Activities  
12 CFR 208.63: Procedures for Monitoring Bank Secrecy Act Compliance  
12 CFR 208, Appendix D-1: Interagency Guidelines Establishing Standards for Safety and Soundness  
12 CFR 208, Appendix D-2: Interagency Guidelines Establishing Information Security Standards (State Member Banks)  
12 CFR 211.5 (l): Interagency Guidelines Establishing Information Security Standards (Edge or agreement corporation)  
12 CFR 211.24 (i): Interagency Guidelines Establishing Information Security Standards (uninsured state-licensed branch or agency of a foreign bank)  
12 CFR 225 Appendix F: Interagency Guidelines Establishing Information Security Standards (bank holding companies and their non-bank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisors))

#### GUIDANCE

SR Letter 05-23 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (December 1, 2005)  
SR Letter 05-19 Interagency Guidance on Authentication in an Internet Banking Environment (October 13, 2005)  
FFIEC IT Examination Handbook Page C-1 Information Security Booklet – July 2006  
SR Letter 04-17 FFIEC Guidance on the use of Free and Open Source Software (December 6, 2004)  
SR Letter 04-14 FFIEC Brochure with Information on Internet "Phishing" (October 19, 2004)  
SR Letter 02-18: Section 312 of the USA Patriot Act—Due Diligence for Correspondent and Private Banking Accounts (July 23, 2002)  
SR Letter 02-6: Information Sharing Pursuant to Section 314(b) of the USA Patriot Act (March 14, 2002)  
SR Letter 01-15: Safeguarding Customer Information (May 31, 2001)  
SR Letter 01-11: Identity Theft and Pretext Calling (April 26, 2001)  
SR Letter 00-17: Guidance on the Risk Management of Outsourced Technology Services (November 30, 2000)  
SR Letter 00-04: Outsourcing of Information and Transaction Processing (February 29, 2000)  
SR Letter 99-08: Uniform Rating System for Information Technology (March 31, 1999)  
SR Letter 97-32: Sound Practices Guidance for Information Security for Networks (December 4, 1997)

#### FEDERAL DEPOSIT INSURANCE CORPORATION REGULATIONS

12 CFR 326, subpart A: Minimum Security Procedures  
12 CFR 326, subpart B: Procedures for Monitoring Bank Secrecy Act Compliance  
12 CFR 332: Privacy of Consumer Financial Information  
12 CFR 353: Suspicious Activity Reports  
12 CFR 364, appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness  
12 CFR 364, appendix B: Interagency Guidelines Establishing Information Security Standards

## GUIDANCE

FIL-103-2005: FFIEC Guidance Authentication in an Internet Banking Environment (October 12, 2005)  
FIL-66-2005: Spyware – Guidance on Mitigating Risks From Spyware (July 22, 2005)  
FIL-64-2005: “Pharming” – Guidance on How Financial Institutions can Protect against Pharming Attacks (July 18, 2005) FFIEC IT Examination Handbook Page C-2 Information Security Booklet – July 2006  
FIL-59-2005: Identity Theft Study Supplement on “Account Hijacking Identity Theft” (July 5, 2005)  
FIL-46-2005 Pre-Employment Background Screening: Guidance on Developing an Effective Pre-Employment Background Screening Process  
FIL-27-2005: Final Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (April 1, 2005)  
FIL-7-2005: Fair and Accurate Credit Transactions Act of 2003 Guidelines Requiring the Proper Disposal of Customer Information (February 2, 2005)  
FIL-132-2004: Identity Theft Study on “Account Hijacking” Identity Theft and Suggestions for Reducing Online Fraud (December 14, 2004)  
FIL-121-2004: Computer Software Due Diligence – Guidance on Developing an Effective Software Evaluation Program to Assure Quality and Regulatory Compliance  
FIL-114-2004: Risk Management of Free and Open Source Software FFIEC Guidance  
FIL-103-2004: Interagency Informational Brochure on Internet “Phishing” Scams (September 13, 2004)  
FIL-84-2004: Guidance on Instant Messaging (July 21, 2004)  
FIL-62-2004: Guidance on Developing and Effective Computer Virus Protection Program (June 7, 2004)  
FIL-27-2004: Guidance on Safeguarding Customers Against E-Mail and Internet Related Fraud Schemes (March 12, 2004)  
FIL-63-2003: Guidance on Identity Theft Response Programs (August 13, 2003)  
FIL-43-2003: Guidance on Developing an Effective Software Patch Management Program (May 29, 2003)  
FIL-8-2002: Wireless Networks And Customer Access (February 1, 2002)  
FIL-69-2001: Authentication in an Electronic Banking Environment (August 24, 2001)  
FIL-68-2001: 501(b) Examination Guidance (August 24, 2001)  
FIL-39-2001: Guidance on Identity Theft and Pretext Calling (May 9, 2001)  
FIL-22-2001: Security Standards for Customer Information (March 14, 2001)  
FIL-77-2000: Bank Technology Bulletin: Protecting Internet Domain Names (November 9, 2000)  
FIL-67-2000: Security Monitoring of Computer Networks (October 3, 2000)  
FIL-68-99: Risk Assessment Tools and Practices (July 7, 1999)  
FIL-98-98: Pretext Phone Calling (September 2, 1998)  
FIL-131-97: Security Risks Associated with the Internet (December 18, 1997)

FFIEC IT Examination Handbook Page C-3 Information Security Booklet – July 2006  
FIL-124-97 Suspicious Activity Reporting (December 5, 1997)  
FIL-82-96: Risks Involving Client/Server Computer Systems (October 8, 1996)  
FFIEC IT Examination Handbook Page C-4 Information Security Booklet – July 2006

## NATIONAL CREDIT UNION ADMINISTRATION REGULATIONS

12 CFR 721: Federal Credit Union Incidental Powers Activities  
12 CFR 748: Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance & Appendices  
12 CFR 716: Privacy of Consumer Financial Information & Appendix  
12 CFR 741: Requirements for Insurance

## GUIDANCE

NCUA Letter to Credit Unions 05-CU-20: Phishing Guidance for Credit Unions and Their Members  
NCUA Letter to Credit Unions 05-CU-18: Guidance on Authentication in Internet Banking Environment (November 2005)  
NCUA Letter to Credit Unions 04-CU-12: Phishing Guidance for Credit Union Members (September 2004)  
NCUA Letter to Credit Unions 04-CU-06: E-Mail and Internet Related Fraudulent Schemes Guidance (April 2004)  
NCUA Letter to Credit Unions 04-CU-05: Fraudulent E-Mail Schemes (April 2004)  
NCUA Letter to Credit Unions 03-CU-14: Computer Software Patch Management (September 2003)  
NCUA Letter to Credit Unions 03-CU-12: Fraudulent Newspaper Advertisements, and Websites by Entities Claiming to be Credit Unions (August 2003)  
NCUA Letter to Credit Unions 03-CU-08: Weblinking: Identifying Risks & Risk Management Techniques (April 2003)  
NCUA Letter to Credit Unions 03-CU-03: Wireless Technology (February 2003)  
NCUA Letter to Federal Credit Unions 02-FCU-11: Tips to Safely Conduct Financial Transactions over the Internet- An NCUA Brochure for Credit Union Members (July 2002)  
NCUA Letter to Credit Unions 02-CU-13: Vendor Information Systems & Technology Reviews—Summary Results (July 2002)  
NCUA Letter to Credit Unions 02-CU-08: Account Aggregation Services (April 2002)  
NCUA Letter to Federal Credit Unions 02-FCU-04: Weblinking Relationships (March 2002)  
FFIEC IT Examination Handbook Page C-5 Information Security Booklet – July 2006  
NCUA Letter to Credit Unions 01-CU-21: Disaster Recovery and Business Resumption Contingency Plans (December 2001)  
NCUA Letter to Credit Unions 01-CU-20: Due Diligence over Third-Party Service Providers (November 2001)  
NCUA Letter to Credit Unions 01-CU-12: E-Commerce Insurance Considerations (October 2001)  
NCUA Letter to Credit Unions 01-CU-09: Identity Theft and Pretext Calling (September 2001)  
NCUA Letter to Credit Unions 01-CU-11: Electronic Data Security Overview (August 2001)  
NCUA Letter to Credit Unions 01-CU-10: Authentication in an Electronic Banking Environment (August 2001)  
NCUA Letter to Credit Unions 01-CU-04: Integrating Financial Services and Emerging Technology (March 2001)  
NCUA Regulatory Alert 01-RA-03: Electronic Signatures in Global and National Commerce Act (E-Sign Act) (March 2001)  
NCUA Letter to Credit Unions 01-CU-02: Privacy of Consumer Financial Information (February 2001)  
NCUA Letter to Credit Unions 00-CU-11: Risk Management of Outsourced Technology Services (with Enclosure) (December 2000)  
NCUA Letter to Credit Unions 00-CU-07: NCUA's Information Systems & Technology Examination Program (October 2000)  
NCUA Letter to Credit Unions 00-CU-04: Suspicious Activity Reporting (see section on "Computer Intrusion") (July 2000)  
NCUA Letter to Credit Unions 00-CU-02: Identity Theft Prevention (May 2000)  
NCUA Regulatory Alert 99-RA-3: Pretext Phone Calling by Account Information Brokers (February 1999)  
NCUA Regulatory Alert 98-RA-4: Interagency Guidance on Electronic Financial Services and Consumer Compliance (July 1998)  
NCUA Letter to Credit Unions 97-CU-5: Interagency Statement on Retail On-Line PC Banking (April 1997)  
NCUA Letter to Credit Unions 97-CU-1: Automated Response System Controls (January 1997)  
NCUA Letter to Credit Unions 109: Information Processing Issues (September 1989)  
FFIEC IT Examination Handbook Page C-6 Information Security Booklet – July 2006

## OFFICE OF THE COMPTROLLER OF THE CURRENCY REGULATIONS

12 CFR 21, subpart A: Minimum Security Devices and Procedures  
12 CFR 21, subpart B: Reports of Suspicious Activities  
12 CFR 21, subpart C: Procedures for Monitoring Bank Secrecy Act Compliance  
12 CFR 30, appendix A: [Interagency] Guidelines Establishing Standards for Safety and Soundness  
12 CFR 30, appendix B: [Interagency] Guidelines Establishing Standards for Information Security

## GUIDANCE

OCC Bulletin 2005-35: Authentication in an Internet Banking Environment (October 2005)  
OCC Bulletin 2005-24: Threats from Fraudulent Bank Web Sites: Risk Mitigation and Response Guidance for Web Site Spoofing Incidents (July 2005)  
OCC Bulletin 2005-13: Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance (April 2005)  
OCC Bulletin 2005-1: Proper Disposal of Customer Information (January 2005)  
OCC Bulletin 2003-27: Suspicious Activity Report-Revised Form (June 2003)  
OCC Advisory 2003-10: Risk Management of Wireless Networks (December 2003)  
OCC Alert 2003-11: Customer Identity Theft: E-Mail-Related Fraud Threats (September 2003)  
OCC Bulletin 2001-47: Third-Party Relationships (November 2001)  
OCC Bulletin 2001-35: Examination Procedures for Guidelines to Safeguard Customer Information (July 2001)  
OCC Alert 2001-04: Network Security Vulnerabilities (April 2001)  
OCC Bulletin 2001-12: Bank-Provided Account Aggregation Services (February 2001)  
OCC Bulletin 2001-8: Guidelines Establishing Standards for Safeguarding Customer Information (February 2001)  
OCC Alert 2000-9: Protecting Internet Addresses of National Banks (July 2000)  
OCC Bulletin 2000-19: Suspicious Activity Report (June 2000)  
OCC Bulletin 2000-14: Infrastructure Threats—Intrusion Risks (May 2000)  
OCC Alert 2000-1: Internet Security: Distributed Denial of Service Attacks (February 2000)  
FFIEC IT Examination Handbook Page C-7 Information Security Booklet – July 2006  
OCC Bulletin 99-20: Certificate Authority Guidance (May 1999)  
OCC Bulletin 98-3: Technology Risk Management (February 1998)

## OFFICE OF THRIFT SUPERVISION REGULATIONS

12 CFR Part 555: Electronic Operations  
12 CFR 563.177: Procedures for Monitoring Bank Secrecy Act Compliance  
12 CFR 563.180: Suspicious Activity Reports and Other Reports and Statements  
12 CFR Part 568: Security Procedures Under the Bank Protection Act  
12 CFR Part 570, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness  
12 CFR Part 570, Appendix B: Interagency Guidelines Establishing Information Security Standards  
12 CFR Part 573: Privacy of Consumer Financial Information

## GUIDANCE

CEO Ltr 97: Policy Statement on Privacy and Accuracy of Customer Information and Interagency Pretext Phone Calling Memorandum (November 3, 1998)  
CEO Ltr 109: Transactional Web Sites (June 10, 1999)  
CEO Ltr 125: Privacy Rule (June 1, 2000) (transmits final rule for privacy of consumer financial information)  
CEO Ltr 139: Identity Theft and Pretext Calling (May 4, 2001)  
CEO Ltr 155: Interagency Guidance: Privacy of Consumer Financial Information. (February 11, 2002)  
CEO Ltr 193: 'Phishing' and E-mail Scams (March 8, 2004)  
CEO Ltr 214: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (March 30, 2005)  
CEO Ltr 228: Interagency Guidance on Authentication in an Internet Banking Environment (October 12, 2005)  
CEO Ltr 231: Compliance Guide- Interagency Guidelines Establishing Information Security Standards (December 14, 2005)  
CEO Ltr 237: Interagency Advisory on Influenza Pandemic Preparedness (March 15, 2006)  
Thrift Activities Handbook Section 341, Technology Risk Controls  
FFIEC IT Examination Handbook Page C-8



“I recommend the consumer ask their IT service provider for their definition of FFIEC compliance to ensure a common understanding of the compliance issues addressed by the IT service provider’s product.”

Janet Wilth, Senior Systems Auditor, CISA, CISM Certified

CONTACT JANET WILTH  
(800) 338-3096  
jwilt@securityproductscompany.com

CONTACT theWEBcentric  
(319) 266-9800 office  
success@theWEBcentric.com  
theWEBcentric.com