NCVHS Subcommittee on Privacy, Confidentiality, and Security

May 6, 2015 Hearing

NACHA – The Electronic Payments Association is pleased to submit this testimony to the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality, and Security as it reviews the evolution of the financial services sector since the passage of HIPAA in support of the health sector.

NACHA is the not-for-profit association responsible for the administration and enforcement of the operating rules for the ACH Network – the *NACHA Operating Rules*. These *Rules* support electronic payment services and standards in the areas of payroll, bill payment, business-to-business payments, and international payments. We bring together over 12,000 financial institutions[1] of all sizes and types throughout the United States, so they can consistently, efficiently, and safely initiate and receive ACH payments into millions of bank accounts. NACHA was identified as the standards body for the healthcare EFT standard transaction and the NACHA CCD+Addenda was identified as the format for the healthcare EFT claim payment standard.

While there are currently over 12,000 financial institutions in the United States today, it is important that the subcommittee recognize that there are most likely less than 20 financial institutions that receive and handle protected health information (PHI) for their health care clients, and that the PHI is transmitted through channels other than the ACH Network. Most financial institutions do not provide healthcare-specific services that would require the receipt of PHI, although it is likely that some would but for existing guidance on "meaningful use" that has been widely interpreted to prohibit health plans from sending electronic remittance advice (ERAs) with payment instructions to their financial institutions. Those financial institutions that actively support the healthcare industry and provide financial services that include the receipt of PHI are addressing the HIPAA Privacy and Security requirements, utilizing business associate agreements, or have established separate health care clearinghouses to handle the health care services and secure PHI.

While PHI is not currently carried through the ACH Network and most financial institutions do not handle PHI, financial institutions are well positioned to handle and protect PHI if it flowed through the ACH Network in the future. Financial institutions are subject to many legal and regulatory requirements designed to protect customer's sensitive information. The Federal Financial Institutions Examination Council (FFIEC) Information Technology Handbook (Handbook)[2] sets forth a broad set of risk-based

[1] The term "financial institution" is used herein to refer to the federally insured and regulated depository institutions (banks, savings associations and credit unions) that are eligible to participate in the ACH Network.
[2] FFIEC Information Technology Handbook, Information Security Booklet, July 2006, http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf

security standards that apply across the entire range of sensitive data that may come into the possession of an insured depository institution. The Handbook provides a listing of the 6 laws and 108 regulations on information security that financial institutions must comply with and states that "Information is one of a financial institution's most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institution and its customers, maintain compliance with the law, and protect the reputation of the institutions." [3]

To ensure compliance with, and identify vulnerabilities, in financial institution information security policies and procedures, the federal banking agencies conduct a full scope, on-site examination of each financial institution at least once every 12 to 18 months or more frequently as determined by the applicable federal regulator.[4] Additionally, third-party servicers that receive sensitive customer data are required to adhere to the same requirements and standards as if they were financial institution, and are subject to examination by federal regulators for compliance with such requirements.[5]

NACHA Operating Rules

In addition to the legal and regulatory framework for the security of financial information flowing through the ACH Network, the *NACHA Operating Rules* also provide another layer of protection for payments and remittance data entering the ACH Network. The *Rules* require ACH participants, including financial institutions and corporate users, to protect the security and integrity of ACH data throughout its lifecycle. All corporate users, financial institutions, third-party service providers and third-party senders must establish, implement and, as appropriate, update security policies, procedures, and systems related to the initiation, processing and storage of entries and resulting protected information. The transmission of information in connection with ACH payments is secure, either through closed telecommunications networks, such as leased line, or if transmission is not through a closed network, the *Rules* require that such information transmitted via an "Unsecured Electronic Network" must at all times from the point of data entry and through transmission be either encrypted or transmitted via a security session using commercially reasonable technology. The ACH Network itself, as a system used to transfer trillions of dollars each year, is very secure. Financial institutions transfer payment instructions to the ACH Operator (either the Federal Reserve or EPN) using one of three methods. Each method of transmission to the ACH Operator uses standard encryption methodology for all files. In addition, the system is closely audited for security and integrity by federal financial regulator agencies. NACHA also provides guidance with respect to security requirements under the *Rule*s from time to time to address changes in the legal, regulatory and/or commercial environment. As an example, as concerns about data security have evolved, NACHA adopted Board Policy Statements on Data Security and on the Data Breach Notification Requirements providing additional guidance to participants in compliance with the *Rules* and has recommended practices to protect the security of data in the ACH Network.

---

[3] *Id*. At 1.

[4] 12 C.F.R. § 4.6 (Office of the Comptroller of the Currency); 12 C.F.R. § 208.64 (Board of Governors of the Federal Reserve System); 12 C.F.R. § 563.171 (Federal Deposit Insurance Corporation); !2 C.F.R. § 337.12 (Office of Thrift Supervision). Certain small institutions that meet defined regulatory criteria may be examined every 18 months.

[5] *See* FFIEC Information Technology Handbook, Supervision of Technology Service Providers booklet, March 2003, http://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers.aspx.

Questions: The subcommittee is interested in understanding -

1. **The types of services financial sector companies are providing to HIPAA covered entities.**

   All financial institutions that participate in the ACH Network are required by the *NACHA Operating Rules* to receive healthcare EFT standard transactions on behalf of providers that are their customers. These standard transactions do not contain PHI.

   Department of Health and Human Services (HHS) identified the NACHA CCD+Addenda as the healthcare EFT standard and NACHA as the standard organization for the healthcare EFT standard in January 2012 with the regulation effective January 1, 2014. In September 2013, changes were implemented to the *NACHA Operating Rules* to ensure that all financial institutions understood and were ready to support payers and providers with the new healthcare EFT standard. The changes incorporated requirements of the federal healthcare EFT standard into the *NACHA Operating Rules* and also added an indicator that allows identification of the healthcare EFT transactions that flow through the ACH Network. With these changes, the ACH Operators were able to count the healthcare EFT standard transactions processed through the Network and in 2014 a total of 149,300,700 claims reimbursement payments using the HIPAA healthcare EFT standard transaction valued at $876,601,291,535 were identified. The monthly healthcare EFT volumes increased 104% from 8.1 million entries in January to 16.7 million entries in December 2014.

2. **What protected health information they receive and how they use it.**

   The healthcare EFT standard as defined in 45 CFR Parts 106 and 162, Administrative Simplification: Adoption of Standards for Health Care Electronic Funds Transfers (EFTs) and Remittance Advice, states that HIPAA Privacy and Security rules do not apply to the transmission of the healthcare EFT standards adopted in the regulation as the ACH transactions includes no individually identifiable health information. [6]

3. **What regulations apply to that information, including self-regulatory codes, if any.**

   The financial services industry is subject to an extensive set of laws and regulatory and supervisory framework designed to protect the sensitive information that flows through the financial services industry and the ACH Network. The FFIEC Handbook outlines 6 laws and 108 regulations on information security that financial institutions must comply with in addition to the security requirements included in the *NACHA Operating Rules*. A list of the specific laws and regulatory and supervisory frameworks is included in Attachment A.

[6] Federal Register/Vol. 77, No.6, January 10, 2012 page 1568.

4. **Whether your members operate under business associate agreements**;

Business Associate Agreements are not required between the financial institutions and their customers to process and deliver the healthcare EFT standard and addenda information. Banks are exempt under 1179 for payment processing, which includes funds transfer and remittance. The healthcare EFT standard does not carry PHI, so the question regarding BAAs is not applicable. The small number of banks that handle PHI outside of the ACH Network do so under Business Associate Agreements.

5. What technical assistance, guidance, or other resources the Department could provide that would be helpful.

The Department could assist in achieving greater administrative simplification by giving clear effect to the Section 1179 exemption for financial institutions for payment processing. The current "minimum necessary" guidance precludes financial institutions and their healthcare customer from transmitting dollars and data together; instead, the dollars and data are kept separate and must be reassociated by providers.

NACHA met twice with representatives from the Office of Civil Rights (OCR) in July 2003 and May 2011 requesting updated guidance to the narrow view of what "minimum necessary information" is allowed to be sent to financial institutions for payment processing with respect to the explicit 1179 exemption. Unfortunately, OCR never responded to either request. It will be beneficial to both the financial services and healthcare industry to receive clarification that gives effect to the explicit, statutory exemption for financial institutions services.

Although financial institutions are clearly and expressly exempt from HIPAA when they engage in traditional, routine banking functions, and covered entities may disclose PHI without permission from the subject of the data for a number of specific purposes, including for "payment "and "health care operations", as defined by 45 C.F.R. 164.502 (a)1(ii) with the existing "minimum necessary guidance" from OCR, covered entities feel it is a violation of HIPAA Privacy if the ERA is sent with the EFT through the ACH Network in a CTX format. The "minimum necessary" provision states in 45 C.F. R 164.502 (b)when making a disclosure for these purposes, however, a covered entity must make reasonable efforts to limit the disclosure to the "minimum necessary" information to accomplish the intended purpose. The preamble to the 2000 HIPAA Privacy Rules states that the information contained in a remittance advice is not necessary to conduct a funds transfer (64 Fed. Reg. 82462 at 82496 and 82616 (Dec. 28, 2000). OCR's narrow interpretation of payment processing to include only EFT has led to the adoption of the less than fully efficient system for transmitting payment from plans to providers, under which the EFT instruction is artificially segregated and transmitted separately from the remittance advice, and then re-associated.

While ERA is not, as a technical matter, needed for a financial institution to execute a funds transfer, *payment processing is broader than executing an EFT.* Financial institutions facilitate efficient payment processing by providing the additional payment-related information (invoices numbers and details) so that the funds are applied correctly as a normal part of the payment process. Disclosure

of ERA does not lose its "payment" status in the health care context simply because the information is transmitted through a financial institution on behalf of a plan or provider. The definition of "payment" under HIPAA encompasses related data processing, 45 C.F.R. 164.501 explicitly states this with respect to provider billing and collection activities – "The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and included, but are not limited to …. (iii) Billing, claims management, collection activities…, and related health care data processing [.]" When the EFT and ERA are transferred together, the need for re-association of the EFT and related remittance information is eliminated, and even greater levels of administrative simplification can be achieved. Administrative simplification cost savings will be maximized for many entities when the EFT and ERA can flow together, seamlessly, to provide what is called "straight-through-processing".

NACHA previously has requested that OCR remove this hurdle to administrative simplification that entities currently perceive under existing minimum necessary guidance, by clarifying that the disclosure and electronic transmission of ERA over the ACH Network together with EFT by a health plan to a health care provider is permitted under HIPAA and that ODFIs and RDFIs are not required to enter into business associate agreements with their respective health plan and health care provider customers when performing this function.

Section 1179 of the SSA, 42 U.S.C 1320d-8, *Processing Payment Transactions by Financial Institutions* states, "To the extent an entity is engaged in activities of a financial institutions (as defined in section 1101 of the Right to Financial Privacy Act of 1978), or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for a financial institutions, this part and any standard adopted under this part, shall not apply to the entity with respect to such activities, including…[t]he use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit , or other payment card, an account, check or electronic funds transfer."

Because of the Section 1179 exemption for financial institutions engaging in traditional banking functions, payment processing is not a business associate function and does not render a financial institution a business associate of a covered entity.

Attachment A

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 ()
• USA Patriot Act ()

Federal Reserve Board

• 12 CFR 208.61: Minimum Security Devices and Procedures (N/A)
• 12 CFR 208.62: Reports of Suspicious Activities (N/A)
• 12 CFR 208.63: Procedures for Monitoring Bank Secrecy Act Compliance (N/A)
• 12 CFR 208, Appendix D-1: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
• 12 CFR 208, Appendix D-2: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
• 12 CFR 211.5 (1): Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Edge or agreement corporation) (N/A)
• 12 CFR 211.24 (i): Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
• 12 CFR 225 Appendix F: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
• SR Letter 11-9 Interagency Supplement to Authentication in an Internet Banking Environment (June 28, 2011)
• 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)
• 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

• 12 CFR 326, subpart A: Minimum Security Procedures (N/A)
• 12 CFR 326, subpart B: Procedures for Monitoring Bank Secrecy Act Compliance (N/A)
• 12 CFR 332: Privacy of Consumer Financial Information (N/A)
• 12 CFR 353: Suspicious Activity Reports (N/A)
• 12 CFR 364, appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
• 12 CFR 364, appendix B: Interagency Guidelines Establishing Standards for Safeguarding Customer Information (N/A)
• FIL-50-2011 FFIEC Supplement to Authentication in an Internet Banking Environment (June 29, 2011)
• 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)
• 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 (June 1, 2005)
• 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 (November 16, 2004)
• FIL-114-2004: Risk Management of Free and Open Source Software FFIEC Guidance (October 21, 2004)
• 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, FIL-63-2003 (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)
• Risk Assessment Tools and Practices, FIL-68-99 (July 1999)
• FIL-98-98: Pretext Phone Calling (September 2, 1998)
• FIL-131-97: Security Risks Associated with the Internet (December 18, 1997)
• FIL-124-97: Suspicious Activity Reporting (December 5, 1997)
• FIL-48-2000: Suspicious Activity Reports (July 14, 2000)
• FIL-82-96: Risks Involving Client/Server Computer Systems (October 8, 1996)

National Credit Union Administration

• 12 CFR 721: Federal Credit Union Incidental Powers Activities (N/A)
• 12 CFR 748: Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance and Appendix (N/A)
• 12 CFR 716: Privacy of Consumer Financial Information, and Appendix (N/A)
• 12 CFR 741: Requirements for Insurance (N/A)
• NCUA Letter to Credit Unions 11-CU-09 Supplement to Authentication in an Internet Banking Environment (June 28, 2012)
• NCUA Letter to Credit Unions 05-CU-20: Phishing Guidance for Credit Unions and Their Members (December 2005)
• 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 (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)
• 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, NCUA Letter to Credit Unions 01-CU-04 (March 2001)
• NCUA Regulatory Alert 01-RA-03: Electronic Signatures in Global and National Commerce 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 (December 2000)
• NCUA Letter to Credit Unions 00-CU-11: NCUA's Information Systems & Technology Examination Program (October 2000)
• NCUA Letter to Credit Unions 00-CU-04: Suspicious Activity Reporting (July 2000)
• NCUA Letter to Credit Unions 00-CU02: Identity Theft Prevention, NCUA Letter to Credit Unions 00-CU-02 (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)
• Automated Response System Controls (January 1997)
• NCUA Letter to Credit Unions 109: Information Processing Issues (September 1989)

Office of the Comptroller of the Currency

• 12 CFR, 21, Subpart A: Minimum Security Devices and Procedures (N/A)
• 12 CFR, 21, Subpart B: Reports of Suspicious Activities (N/A)
• 12 CFR, 21, Subpart C: Procedures for Monitoring Bank Secrecy Act Compliance (N/A)
• 12 CFR, 30, Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
• 12 CFR, 30, Appendix B: Interagency Guidelines Establishing Information Security (N/A)
• OCC Bulletin 2011-26: Authentication in an Internet Environment - Supplement (June 28, 2011)
• OCC Bulletin 2005-35; Authentication in an Internet Banking Environment (October 12, 2005)

• OCC Bulletin 2005-24: Threats from Fraudulent Bank Web Sites (July 1, 2005)
• OCC Bulletin 2005-13: Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance (April 14, 2005)
• OCC Bulletin 2005-1: Proper Disposal of Consumer Information (January 12, 2005)
• OCC Bulletin 2003-27: Suspicious Activity Report (June 24, 2003)
• OCC Advisory 2003-10: Risk Management of Wireless Networks (December 9, 2003)
• OCC Alert 2003-11: Customer Identity Theft: E-Mail-Related Fraud Threats (September 12, 2003)
• OCC Bulletin 2001-47: Third Party Relationships (November 1, 2001)
• OCC Bulletin 2001-35: Examination Procedures for Guidelines to Safeguard Customer Information (July 18, 2001)
• OCC Alert 2001-04: Network Security Vulnerabilities (April 24, 2001)
• OCC Bulletin 2001-12: Bank Provided Account Aggregation Services (February 28, 2001)
• OCC Bulletin 99-20: Certificate Authority Guidance (May , 1999)
• OCC Bulletin 2001-8: Guidelines Establishing Standards for Safeguarding Customer Information (February 15, 2001)
• OCC Alert 2000-9: Protecting Internet Addresses of National Banks (July 19, 2000)
• OCC Bulletin 2000-19: Suspicious Activity Report (June19, 2000)
• OCC Bulletin 2000-14: Infrastructure Threats-Intrusion Risks (May 15, 2000)
• OCC Alert 2000-1: Internet Security: Distributed Denial of Service Attacks (February 11, 2000)
• OCC Advisory Letter 2000-12: Risk Management of Outsourcing Technology Services (November 28, 2000)
• OCC Bulletin 98-3: Technology Risk Management (February 4, 1998)
• OCC Bulletin 98:38 Technology Risk Management: PC Banking (August 24, 1998)
• Authentication in an Internet Environment Supplement (June 28, 2011)

Office of Thrift Supervision

• 12 CFR Part 555: Electronic Operations (N/A)
• 12 CFR 563.177: Procedures for Monitoring Bank Secrecy Act Compliance (N/A)
• 12 CFR 563.180: Suspicious Activity Reports and Other Reports and Statements (N/A)
• 12 CFR 568: Security Procedures Under the Bank Protection Act (N/A)
• 12 CFR 570 Appendix A: Interagency Guidelines Establishing Standards for Safety and Soundness (N/A)
• 12 CFR 570 Appendix B: Interagency Guidelines Establishing Information Security Standards (N/A)
• 12 CFR 573: Privacy of Consumer Financial Information (N/A)
• 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 (Transmits final rule for Privacy of Consumer Financial Information) (June 1, 2000)
• 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 (January 2002)

External Resources

• Control Objectives for Information Technology Website at www.isaca.org (The Information Systems Audit and Control Association & Foundation) (N/A)
• Code of Practice for Information Security Management (ISO /IEC 17799) (available at The International Organization for Standards (ISO) Information Technology Website, www.iso.org/iso/en/CatalogueListPage.CatalogueList) (September 2001)
• Information Security -- Security Techniques-Evaluation Criteria for IT Security (ISO / IEC 15408) (available at The International Organization for Standards (ISO) Information Technology Website, www.iso.org/iso/en/ CatalogueListPage.CatalogueList.) (December 1999)
• Guidelines on Firewalls and Firewall Policy, Special Publication 800-41 (January 2002)
• Risk Management Guide for Information Technology Systems, Special Publication 800-30 (October 2001)
• The National Institute of Standards and Technology (NIST) Website at www.nist.gov (N/A)