



OCC ADVISORY LETTER

Comptroller of the Currency
Administrator of National Banks

Subject: Electronic Record Keeping

TO: Chief Executive Officers of All National Banks, Federal Branches and Agencies, Service Providers and Software Vendors, Department and Division Heads, and All Examining Personnel.

PURPOSE

This advisory letter highlights issues regarding bank electronic record systems in light of the E-SIGN Act. 15 USC 7001, et seq. The letter provides a basic framework that bank management can use to assess and address key issues posed by electronic record keeping systems.

BACKGROUND

Federal legislation changed the legal framework for electronic records and will likely result in more banks adopting electronic record retention systems. Banks can implement electronic record retention systems in many ways to support different business processes. Some examples of possible electronic record retention systems are loan file imaging, retention of paperless applications and online agreements, and the use of electronic payment systems.

Under the E-SIGN Act (the “Act”), which became effective March 1, 2001, an electronic record¹ can satisfy most legal record retention requirements for contracts or other records² (including requirements that a record must be retained in its original form) provided that the electronic record is

- retained in a form that accurately reflects the information in the contract or other record,
- accessible to all persons who are entitled to access the information for the period of time required by law, and

¹ Under the Act, an “electronic record” is a contract or other record created, generated, communicated, or stored by electronic means.

² Checks and other negotiable instruments governed by the Uniform Commercial Code are specifically excluded from the Act. For background on the legal status of and requirements for electronic images of checks, see Check 21 Act, Pub. L. No. 108-100, 117 Stat. 1177 (codified at 12 USC 5001-5018).

- in a form that allows it to be accurately reproduced for later reference by transmission, printing or otherwise.

An electronic record that meets all of the above general standards will satisfy a legal requirement that a contract or other record (such as a consumer disclosure) must be retained in writing. 15 USC 7001(d).

However, as discussed below, the general standards under the Act need further development and interpretation before they can be applied with assurance. Moreover, the Act does not resolve all legal or practical issues relating to electronic records to ensure that the records can fulfill their intended purposes and will comply with applicable regulatory requirements other than retention. For example, the Act does not ensure admissibility of electronic records in litigation. This is important because the practical effect of having electronic records that are not admissible into evidence in judicial proceedings may be to render the electronic contract or record effectively unenforceable.³

While banks are permitted under E-SIGN to satisfy record retention requirements with electronic record retention systems⁴ that comply with the Act, banks will need to carefully plan their implementation and operation of these electronic record retention systems to ensure they meet functional and regulatory requirements.

FUNCTIONAL AND REGULATORY CONSIDERATIONS

The Act does not provide specific definitions for its general, minimum standards of accuracy, integrity,⁵ or accessibility.⁶ Nevertheless, banks adopting electronic record retention systems should understand and consider the risks resulting from inadequate record retention practices and systems.

The failure of banks to maintain adequate record retention systems can create significant reputation, transaction, credit, and compliance risks. Also, the risks and necessary controls associated with different types of electronic record retention systems will vary according to the

³ The Act does not automatically render contracts “non-enforceable” merely because they are retained in a form that fails to comply with the retention standards of 15 USC 7001(d). However, under the Act, a contract or record that is required by law to be in writing may be denied legal effect unless it is in a “form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.” 15 USC 7001(e). This 7001(e) requirement (and its sanction of denial of enforceability) relates to the form in which the record is *made available* to other parties, i.e., whether the record was provided in a proper form; it does not relate to whether the record was properly retained by the bank under 7001(d).

⁴ “Electronic record retention system” in this advisory letter will refer to an information technology system that stores and retains records in electronic form.

⁵ The “integrity” of a records system is its ability to prevent unauthorized modifications or changes to stored records.

⁶ While federal agencies (including the banking agencies) are empowered by E-SIGN to specify performance standards to ensure accuracy, record integrity, and accessibility, the Office of the Comptroller of the Currency (OCC) and the other banking agencies have not yet exercised this authority. Given the continuing developments in technology, it would be premature to adopt such regulations at this time.

specific records that are in a particular system and the sensitivity and criticality of those records to the bank or its customers.

Despite the absence of specificity in the Act's standards, an electronic record system of a national bank must have sufficient accuracy, accessibility, and integrity to achieve and accomplish all essential functions and purposes that pertain to the *specific* records that are contained within that particular system. Likewise, the system must have the accuracy, accessibility, integrity, and other attributes needed to comply with regulatory requirements applicable to those specific records. Until more specific standards are developed, banks should design, implement, and operate their electronic records systems so that they are adequate to serve the following purposes and functions according to the nature of the retained records:

- Potential use in litigation support,
- Internal and external audits and controls,
- Bank supervision, and
- Compliance with regulatory requirements.

Each is discussed in greater detail below.

Records needed for litigation

Records that the bank may need to produce or to introduce into evidence in litigation should receive special attention. Without adequate and admissible records, the bank will be unable to enforce its rights and to protect itself against claims in litigation. Thus, if records that support loan or investment transactions are inadmissible, the bank may face credit, transaction, and market risk. Under the "Interagency Guidelines and Standards for Safety and Soundness," Appendix A of 12 CFR Part 30, it is an unsafe and unsound practice if the bank fails to maintain loan documentation that, among other things, ensures that the bank's claims against its borrowers are legally enforceable. *See* 12 CFR Part 30, Appendix A, II, C. 3.

Bank management should consult with legal counsel to ensure that electronic record retention systems containing records that the bank may need in litigation are sufficient to ensure admissibility in relevant courts. If an electronic record cannot be admitted into evidence, it is useless in litigation even though it formally satisfies federal record retention requirements.

The Act does not provide any assured standards for admissibility of electronic records. The courts continue to develop precedent on the admissibility of electronic records. However, each new record-retention technology raises issues that must be addressed before the legal uncertainties of record retention systems based on the technology are resolved. Moreover, the standards for admissibility of electronic records can vary from state to state.⁷ The standards developed in one state are not binding in another. This lack of uniformity can pose a significant

⁷ On the admissibility of electronic records, bank counsel can refer generally to the Federal Rules of Evidence (particularly Fed. R. Evid. 1001(3)) and to sections 12 and 13 of the Uniform Electronic Transactions Act (a state law counterpart to E-SIGN that has been adopted in many states).

challenge to a bank that wants to establish a single electronic record retention system and is doing business in more than one state.

Electronic documents with electronic signatures may pose special retention challenges to ensure their admissibility. National banks should also understand that digital copies of physical documents signed with original manual signatures may face challenges as to authenticity and admissibility if the actual original signature is no longer available.

Records needed for internal and external audits and controls

Adequate electronic record systems with sufficient accuracy, integrity, and accessibility are also necessary to support controls like internal and external audits. Bank management should consult with internal and external auditors to ensure that electronic record retention systems containing records that the bank may need for such audits are sufficient to support the auditing and control functions. For example, an electronic record retention system with poor integrity due to weak access controls could be subject to falsification and manipulation by insiders seeking to prevent detection of their malfeasance. For this reason, the “Guidelines and Interagency Standards for Safety and Soundness” implicitly require that there be a record retention system (whether paper or electronic) that is adequate to support an appropriate internal auditing system. *See* 12 CFR Part 30, Appendix A, II, B.

Records needed for bank supervision

The ability of the OCC to supervise national banks is dependent upon access to adequate and accurate records. Thus, a national bank that has digitized its records must maintain electronic records that provide OCC staff with prompt and sufficient access to reliable information to permit adequate examination and supervision. 12 USC 481. Moreover, a national bank with electronic record retention systems should maintain records sufficiently complete and accurate to enable the OCC to determine its financial condition and the substance and purpose of transactions that may have a material effect on its financial condition. 12 USC 1818(c)(3). National banks should ensure that any bank electronic record retention system they adopt permits access to electronic records by all persons entitled to access by law. Among other things, the bank should maintain the necessary equipment and software to enable timely OCC access to bank records.

Records needed to comply with laws and regulations

Inadequate record retention systems may result in compliance violations. Federal rules contain many record retention requirements pertaining to consumer protection (for example, Regulations B, Z, DD), securities activities (for example, 12 CFR 12.3 and 12.4), and Bank Secrecy Act (BSA) compliance (for example, 31 CFR 103.29 and 103.32). Most of these retention laws and regulations do not provide clear instructions on the use of electronic technology or records.

If a bank adopts an electronic record retention system to contain records subject to these consumer protection and BSA laws, bank management should ensure that the system is designed and operated so that electronic records will comply with the specific requirements of the

applicable laws.⁸ For example, electronic record retention systems with unreliable scanning or image capture technology could result in inferior or missing records that would not comply with retention requirements and may subject the bank to regulatory enforcement actions. Moreover, the system must also enable the bank to retrieve and produce records within required timeframes. *See*, for example, 31 USC 5318(k)(2)(which provides that a bank has 120 hours to produce records concerning accounts opened, maintained, administered, or managed in the United States.

IMPLEMENTATION CONSIDERATIONS

National banks should conduct proper planning and due diligence before acquiring or developing an electronic record retention system. An effective planning process will include representation from all affected areas in the bank, including management and personnel from the relevant business lines, information technology, operations, audit, legal, and compliance. The electronic record retention system should be fully consistent with the bank's general corporate records management program. Management should assess the risks and objectives associated with the new electronic system and consider the potential effect on current business processes and internal controls.

As part of this risk assessment, national banks should consult with knowledgeable legal counsel before undertaking any systematic digitalization of their records. This will help ensure that the electronic records comply with the requirements of the E-SIGN Act and, when appropriate, will satisfy applicable standards for admissibility into evidence. National banks should be especially careful regarding digitization of records that are likely subjects of litigation, such as consumer compliance, asset management, and loan records. Bank management should also consider consulting with their audit and compliance personnel when planning and developing a new electronic record retention system.

After assessing the risks of an electronic records system, bank management will need to establish the necessary business and control requirements and conduct due diligence to compare the various options against those requirements. As part of the planning and due diligence process, OCC encourages national banks to consider the general points described below:

Security

The failure to properly secure and protect bank electronic record retention systems that contain confidential customer information will violate the minimum security standards imposed under section 501(b) of the Gramm-Leach-Bliley Act. *See* 12 CFR Part 30, Appendix B. However, the security device utilized must not prevent accessibility of the record to those legally entitled to it, including OCC examiners. Bank management should confirm that its record systems are properly secure from unauthorized access and data alteration, and this aspect of the systems should be adequately tested. The record systems architecture should be fully documented, and the systems adequately indexed.

⁸ Management may want to involve the bank's compliance and legal staffs in the design and implementation of a system that will contain records subject to these requirements.

Internal controls

When appropriate because of the nature of the records stored in the system, national banks should implement effective internal controls to protect electronic record retention systems from unauthorized access and alteration, including associated business and information management practices. Internal controls include methods such as segregation of duties, physical and logical access controls, retention requirements, documentation of changes to records, elimination of write-access to records after capture, encryption for transmission and storage, software integrity checks, and equipment and record media disposal procedures.⁹ The effectiveness of these controls should be subject to audit review.

Back-up and recovery

A national bank with an electronic records retention system with inadequate back-up and recovery processes may find that its records are inaccessible following an emergency. Thus, national banks should ensure that their electronic records are sufficiently backed up so that recovered records will meet the same accuracy and integrity standards as the primary electronic versions. National banks should assess whether they have a consistent process for periodic record back-up that stores the records in a secure off-site location with proper access controls, and for periodically testing their ability to recover the records.

Record destruction and disposal

Record destruction and disposal should generally occur only in accordance with a systematic and well-documented procedure and an approved records retention and disposition schedule. Among other things, the bank's procedures for disposal of electronic records should contain provisions for suspending records destruction if warranted by litigation or regulatory requests. This procedure should also comply with the guidelines and rules on safeguarding customer information previously issued to implement section 501(b) of the Gramm-Leach-Bliley Act. 12 CFR Part 30, Appendix B.¹⁰ Additionally, the procedure must conform to OCC's requirements issued under Section 216 of the Fair and Accurate Credit Transactions (FACT) Act, Pub. L. No. 108-159, requiring "any person that maintains or otherwise possesses consumer information ... derived from consumer reports ... to properly dispose of any such information or compilation." The OCC and the other federal banking agencies will implement section 216 of the FACT Act by amending the existing 501(b) guidelines.

⁹ See *FFIEC IT Examination Handbook*, "Information Security Booklet" (December 2002) http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

¹⁰ The "customer information systems" subject to the requirements of section 501(b) are "any methods used to access, collect, store, use, transmit, protect, or dispose of customer information." 12 CFR Part 30, Appendix B, I.C.2.d.. (Emphasis added.)

Retention periods and content

Electronic record retention systems of national banks should also comply with all requirements imposed by statute or regulation for the mandated retained records. Thus, management should seek to establish a period of retention appropriate to the specific record and consistent with applicable legal, regulatory, fiscal, and administrative requirements.

As part of its evaluation of an electronic records retention system, bank management should determine which electronic messages and communications to retain.¹¹ This determination will depend on whether a particular e-mail or electronic message is a “record” for purposes of the particular record retention requirement or whether the bank may need it later for business or litigation purposes. Thus, banks should look to the content of particular messages rather than their format or technology. If the e-mail were considered a “record” or would be retained for business purposes because of its content if it had been received or sent in paper, then it should also be retained as a “record” even though it is in electronic form. This is consistent with the general approach in developing law to impose “record” requirements that are technology neutral. See, for example, the E-SIGN Act and Sarbanes-Oxley Act of 2002, Pub. L. 107-204 (especially section 802 on retention of auditor work papers). The process should ensure that both the content of the message and sufficient information about its attributes, such as the source, destination, date, and time, are retained for authenticity purposes.

Change management

A national bank’s plan for its electronic records systems should provide for continuing accessibility despite future changes in technology that will require that record systems be updated and that records be migrated to the updated systems.

National banks should assess and test the impact on the integrity and accessibility of their electronic records that may be caused by any changes in their systems or those of their service provider. Banks should consider change management controls that address risks to electronic record systems before, during, and following a change.

¹¹ One challenge facing banks is that new forms of electronic communications are developing beyond the established forms such as e-mail. One example is Instant Messages (IMs); however, this advisory letter will not specifically discuss retention of IMs because their legal status as records is uncertain. However, the National Association of Securities Dealers (NASD) recently instructed securities brokers and dealers to save all IMs sent to clients and employees for three years. See <http://www.nasdr.com/pdf-text/0333ntm.pdf>.

RESPONSIBLE OFFICE

Questions regarding this advisory letter can be directed to Aida Plaza Carter, Director, Bank Information Technology at (202) 874-4740 or to James Gillespie, Assistant Chief Counsel, at (202) 874-5200.

Mark O'Dell
Deputy Comptroller, Operational Risk