HEINONLINE

Citation: 7 Bernard D. Reams Jr. Law of E-SIGN A Legislative
of the Electronic Signatures in Global and National
Act Public Law No. 106-229 2000 1 2002

Content downloaded/printed from
HeinOnline (http://heinonline.org)
Sun Apr 21 23:23:27 2013

-- Your use of this HeinOnline PDF indicates your acceptance
of HeinOnline's Terms and Conditions of the license
agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from
uncorrected OCR text.

United States General Accounting Office
Washington, DC 20548

November 8, 2000

The Honorable Alan Greenspan
Chairman
Board of Governors of the Federal Reserve System

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

Subject: Bank Regulators' Evaluation of Electronic Signature Systems

This letter presents the results of our review, conducted as part of our research and development work, of actions taken by the Federal Reserve System (Federal Reserve) and the Office of the Comptroller of the Currency (OCC) in connection with the operations of Identrus, LLC, New York, NY (Identrus).[1] Identrus is a global rulemaking and coordinating body for a network of financial institutions that will act as certification authorities and thereby provide services designed, in part, to verify or authenticate the identity of customers conducting financial and nonfinancial transactions over the Internet and other open electronic networks. To provide these services, Identrus and its network of participating financial institutions will utilize digital certificates and digital signatures in an electronic authentication system based on public key cryptography.

The use of electronic signature systems—which include digital signatures—in the financial services industry will likely increase in the future as a result of the implementation of the Electronic Signatures in Global and National Commerce (E-SIGN) Act.[2] Since the act promotes the legal validity of electronic signatures, a financial institution may begin to use electronic signatures as evidence of on-line transactions, such as the acceptance of the terms of a credit agreement by the customer. Further, consumers may begin to use electronic signatures to complete on-line transactions, such as opening bank accounts, obtaining credit, or establishing an insurance policy or brokerage account.

[1] See Federal Reserve Board Order of November 10, 1999, approving the application of Bayerische Hypo-und Vereinsbank AG, Munich, Germany; Deutsche Bank AG, Frankfurt, Germany; and Stichting Prioriteit ABN AMRO Holding, Stichting Administratiekantoor ABN AMRO Holding, ABN AMRO Holding N.V., and ABN AMRO Bank, N.V., all of Amsterdam, The Netherlands, each to retain up to 12.5 percent of the voting interests of Identrus, LLC, New York, NY, and to engage in acting as a certification authority in connection with financial and nonfinancial transactions and other related activities. See also Office of the Comptroller of the Currency Conditional Approval #339 letter dated November 16, 1999, to Bank of America and Citibank, NA, approving their application for Identrus to provide a system infrastructure within which the participants will provide certification authority services and concluding that the proposed activities of Identrus, LLC, are part of or incidental to the business of banking.

[2] See P.L. 106-229, which was enacted on June 30, 2000.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 1 2002

During November 1999, while we were monitoring technical developments pertinent to public key infrastructure (PKI) systems, we learned of the Federal Reserve's approval of banking institutions' investments in Identrus and of OCC's decision that Identrus' activities were permissible national bank activities. In monitoring these developments, we noted that Identrus intended to generate the public/private key pairs used by their customers for electronically signing transactions. Since any such practice would need to provide appropriate controls to link a given signature to a specific individual, we initiated this study to determine whether the Federal Reserve and OCC have taken, or plan to take, steps to evaluate the controls surrounding electronic signature systems, such as the Identrus PKI system.

Results in Brief

The Federal Reserve and OCC both issued decisions concluding that Identrus' certification authority services are part of or closely related to banking operations. Although the decisions outlined some of the business processes that may be used by an entity that performs certification authority services, these decisions did not, and were not intended to, provide the criteria that should be used by the financial institutions in setting up their PKI systems. Neither do they discuss criteria to be used by bank examiners to review PKI systems.

Officials from OCC and the Federal Reserve told us that they are currently in the process of developing an examination strategy for Identrus. OCC officials said that they plan to conduct a formal risk assessment and examination of Identrus at the beginning of next year. Federal Reserve officials told us that they have not yet determined the role they should play in assessing Identrus' operations, but stated that depository institutions should be taking the lead in assessing the risks posed by PKI systems.

OCC and the Federal Reserve have not yet developed a specific program to evaluate the risks associated with, and the controls surrounding, electronic signature systems, although they have issued guidance related to information technology assessments. Developing more specific regulatory guidance that includes criteria for evaluating electronic signature systems could assist the examiners and financial institutions in their information technology risk assessments and control evaluations. Such guidance could also assist the entities developing electronic signature systems in their requirements definition process. This letter includes a recommendation to develop this guidance. In developing the guidance, the banking regulators may want to consider the technology-neutral criteria that we have adopted that facilitates our assessment of whether an electronic signature system provides reasonable assurance that the signatures generated by the system were generated by the reported signer.

Background

Five federal regulators—the Federal Reserve, OCC, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of Thrift Supervision (OTS)—supervise and examine all federally insured depository institutions. The Federal Reserve and OCC are the primary federal regulators of the largest banks in the United States. In addition, the Federal Reserve supervises bank holding

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 2 2002

companies and is the umbrella regulator for financial holding companies.[3] The five federal regulators work together through the Federal Financial Institutions Examination Council (FFIEC), an interagency forum Congress created in 1979 to promote consistency in the examination and supervision of depository institutions.[4] The FFIEC issues interagency guidance on crosscutting supervisory and examination issues.

Under the National Bank Act, OCC supervises national banks. In exercising this responsibility, OCC approves applications by national banks to engage in certain activities directly or through ownership in a subsidiary. Generally, the activities of a national bank are limited to those that are part of or incidental to the business of banking. A national bank may also engage in these activities by means of an operating subsidiary.[5] Similarly, under the Bank Holding Company Act, a bank holding company may not acquire an interest in a nonbank affiliate unless the Federal Reserve Board (FRB) has concluded that the affiliate's activities are closely related to banking. OCC and the FRB have both found that certification authority services are part of or closely related to banking.

A certification authority performs a function similar to that of a notary in the paper-based environment. In paper-based systems, a notary provides a means to bind a signature to the stated signer. A certification authority performs a similar function in public-key-based electronic signature systems. The certification authority provides a means to link a given signature to a specific individual or entity. In the case of Identrus, the certification authorities provide the means to confirm the identities of parties sending and receiving electronic payments or other communications using a digital signature[6] and a PKI. A PKI is a system of computers, software, policies, and people that can be used to facilitate the protection of sensitive information and communications. A primary function of a PKI is to generate and manage the certificates that bind an individual or entity to a given public key. The resulting certificates are used for such items as verifying digital signatures (authentication and data integrity) and facilitating data encryption (confidentiality). For example, an entity that desires to validate a signature uses a properly designed and implemented PKI to ensure that the individual or entity associated with a given signature is still bound to that signature. This authentication service is commonly referred to as nonrepudiation.

Regulators Approved Certification Authority Activities

The Federal Reserve and OCC have both issued decisions stating that certification authority services are closely related to the business of banking. In the case of Identrus, the Federal Reserve, on November 10, 1999, approved several banking institutions' applications to each retain up to 12.5 percent of the voting interests of Identrus, and to act as a certification

[3] Under the recently enacted Gramm-Leach-Bliley Act , commercial banks, insurers, securities firms, merchant banks, and other financial entities are permitted to affiliate in a financial holding company structure, subject to the overall supervision of the Federal Reserve, with functional regulation of the component institutions.

[4] FFIEC is composed of the Comptroller of the Currency, one Federal Reserve Board governor, the OTS Director, the FDIC Chairman, and the Chairman of the NCUA Board.

[5] 12 C.F.R. §5.34.

[6] A digital signature is one form of electronic signature that recent law (P.L. 106-229) defines as an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 3 2002

authority in connection with financial and nonfinancial transactions and other related activities. Specifically, the Federal Reserve determined that Identrus' activities as a certification authority and, more generally, those connected with authenticating the identity of customers conducting financial and nonfinancial transactions, are activities that are closely related to banking within the meaning of section 4(c)(8) of the Bank Holding Company Act.[7] Additionally, on November 16, 1999, OCC found that the certification authority services proposed by the banking institutions with investments in Identrus are part of or incidental to the business of banking.[8]

Although the Federal Reserve and OCC decisions outlined some of the business processes that may be used by an entity that performs certification authority services, these decisions do not, and are not intended to, provide the criteria that should be used by the financial institutions in setting up their electronic signature systems. Nor do they discuss criteria used by examiners to review electronic signature systems. According to a Federal Reserve official, the Federal Reserve staff took steps to gather information concerning the business processes of Identrus and its PKI services during the application process in order to assist with the development of risk-focused supervisory strategies for the banking organizations supervised by the Federal Reserve that are participants in Identrus' activities, as well as with an appropriately risk-focused supervisory program for Identrus.

Following the passage of the Gramm-Leach-Bliley Act and the Federal Reserve's approval of the Identrus order, providing certification authority services is now a preapproved activity for both bank holding companies and financial holding companies. Accordingly, bank holding companies and financial holding companies must comply only with applicable notice requirements (not approval requirements) for future transactions involving certification authorities.

Lack of Guidance Hinders Evaluation of Electronic Signature Systems

Officials from OCC and the Federal Reserve told us they are currently in the process of developing an examination strategy for Identrus. OCC officials said that they plan to conduct a formal risk assessment and examination of Identrus at the beginning of next year.[9] Federal Reserve officials told us that they have not yet determined the role they should play in assessing Identrus' operations, but stated that depository institutions should be taking the lead in assessing the risks posed by electronic signature systems.

---

[7] In order to approve the application, the Federal Reserve also had to determine that the performance of the proposed activities "can reasonably be expected to produce benefits to the public . . . that outweigh possible adverse effects, such as undue concentration of resources, decreased or unfair competition, conflicts of interests, or unsound banking practices." See 12 U.S.C. §1843(c)(8). Also, see page 14 of the Federal Reserve Board's approval of Identrus' activities, November 10, 1999.

[8] See footnote 1.

[9] OCC's Conditional Approval Letter #339, November 16, 1999, stated: "The OCC has assigned to [Identrus] an examiner with special expertise in bank information systems to meet regularly with management to discuss their plans, monitor project management and observe trial implementations. OCC will conduct an onsite examination of [Identrus] and major non-bank service providers of [Identrus] . . ., as [Identrus] begins operations. . . . The scope of the review will be a thorough examination of the certification authority system, based on OCC's familiarity with the proposed activity" (pp. 11 and 12).

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 4 2002

OCC and the Federal Reserve have not yet developed a specific program to evaluate electronic signature systems. Specifically, the Federal Reserve has not developed any guidance with industry-specific criteria to evaluate electronic signature systems and the adequacy of internal controls over such operations, although it has issued supervisory guidance related to information technology assessment.[10] This guidance directs examiners to explicitly consider information technology when developing their risk assessments and supervisory plans. OCC has issued similar guidance on technology risk management.[11] It has also issued general guidance related to certification authorities that defines the elements of certification authority systems, describes the roles of banks in emerging systems, and identifies some of the risks of such systems using the OCC supervision-by-risk framework.[12] However, this general guidance does not apply to all electronic signature systems.

Although the Federal Reserve and OCC have not yet developed a specific program to evaluate electronic signature systems, including PKI systems, officials from the agencies have agreed to evaluate the need for guidance that includes criteria for evaluating such systems. The development and issuance of guidance by the banking regulators that includes criteria for the evaluation of electronic signature systems would help not only the information technology risk assessment and evaluation process of the financial institutions and regulators, but also the entities that are developing electronic signature systems, since this framework would assist the requirements definition process. Consequently, an entity developing an electronic signature system could reduce its information technology risks of developing a solution that, when evaluated by the financial institutions or the regulators, would be found lacking in critical internal controls. Additionally, because the use of electronic signatures will likely increase as a result of the implementation of the E-SIGN Act, all banking regulators are likely to be involved in overseeing electronic signature systems in the future. Therefore, it would be beneficial for the Federal Reserve and OCC to work through the FFIEC to develop guidance to evaluate such systems. By working through the FFIEC to develop guidance, the banking regulators could help ensure that they have a consistent methodology for evaluating electronic signature systems.

We have been asked by several federal agencies to review electronic signature systems—which may include digital signatures—used in financial management systems[13] and to discuss how such systems should be evaluated. Because of some of the unique risks associated with highly automated environments, traditional data integrity techniques used to authenticate an individual may not provide the same degree of assurance that the individual intended to be bound by a transaction as that provided by paper-based systems. For example, in a paper-based system, an individual's signature on the paper document is a

[10] See "Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations," SR 98-9 (SUP), Division of Banking Supervision and Regulation, Board of Governors of the Federal Reserve System, April 20, 1998.

[11] See "Technology Risk Management," OCC Bulletin 98-3, Office of the Comptroller of the Currency, February 4, 1998.

[12] See "Certification Authority Systems," OCC Bulletin 99-20, Office of the Comptroller of the Currency, May 4, 1999.

[13] Examples of GAO's work pertaining to electronic signatures include Corps of Engineers Electronic Signature System (GAO/AIMD-97-18R, Nov. 19, 1996); and State Electronic Signature System (GAO/AIMD-00-227R, July 10, 2000).

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 5 2002

time-tested method of showing that an individual intended to be bound by the terms and conditions contained in the paper document. However, in an electronic world, where adequate controls may not have been implemented, the similar approach of having an individual's name appended to a data record does not provide the same assurance because, for example, the terms and conditions can be changed without changing the individual's name.

When reviewing electronic signature systems, we evaluate whether a system generates electronic signatures that represent an individual's or entity's intent to be bound. To do this, we determine whether the electronic signature system provides reasonable assurance that the signature produced by the system is (1) unique to the signer; (2) under the signer's sole control; (3) capable of being verified; and (4) linked to the data in such a manner that, if the data are changed, the signature is invalidated upon verification. Adopting these criteria facilitates our evaluation of how well the electronic signature system addresses its threats and helps identify vulnerabilities that may be present in the system. We have also found these criteria useful since they are technology neutral and allow for a variety of implementation methods, depending on the degree of risk associated with a given application. When considering what their guidance should be, the banking regulators may want to consider including, as appropriate, elements of our criteria.

Recommendation for Executive Action

Given that the importance of electronic signature systems is likely to grow, banking regulators need a consistent methodology for assessing the risks and appropriateness of internal controls surrounding such systems. We recommend that the Chairman, Board of Governors of the Federal Reserve System, and the Comptroller of the Currency, OCC, work through the FFIEC to develop guidance that includes criteria for evaluating electronic signature systems in order to provide reasonable assurance that electronic signatures generated by the system are valid.

Agency Comments

We requested comments on a draft of this letter from the Comptroller of the Currency, OCC, and the Chairman, Board of Governors of the Federal Reserve System. OCC provided written comments that are included in enclosure I. An Associate Director, Division of Banking Supervision and Regulation, Board of Governors of the Federal Reserve System, provided comments electronically on a draft of this report.

OCC agreed to take our recommendation to the FFIEC. Additionally, as OCC exercises its oversight responsibilities in evaluating the safety and soundness of certification systems offered by national banks and their subsidiaries, it agreed to consider, as appropriate, the technology-neutral criteria that we have adopted in assessing whether an electronic signature system provides reasonable assurance that the signatures generated by the system were generated by the reported signer.

The Associate Director, Division of Banking Supervision and Regulation, Board of Governors of the Federal Reserve System, commented that our letter accurately reports that the FRB staff is currently in the process of deciding what role, if any, the Federal Reserve

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 6 2002

should play in assessing Identrus' operations. On behalf of the FRB staff, he agreed with the general thrust of our recommendation and stated that the need for guidelines for evaluating electronic signature systems through the bank supervision process should be discussed on an interagency basis under the auspices of the FFIEC. He also stated that FRB staff would work with their colleagues at the FFIEC to address our recommendation, and that an FFIEC subcommittee could review the current environment associated with digital certification authorities and PKI-related technology. He stated that this review could, for example, look into the steps that are being taken by the banking industry and other private sector firms providing certification authority services to establish safeguards for their services; the roles played by internal and external auditors in evaluating their clients' services; the adequacy of the due diligence processes and internal controls systems; and the responsibilities of banking organizations' boards of directors to oversee the contracts that their institutions are entering into for PKI and related services. After its assessment, the FRB official said the subcommittee could formulate recommendations to the banking agencies concerning whether any new bank examination-related guidance should be developed.

Scope and Methodology

We conducted our review from November 1999 to October 2000 in accordance with generally accepted government auditing standards. During this review, we examined the details of the Federal Reserve's Identrus Order and OCC's Conditional Approval #339. Our examination included an analysis of public key infrastructure issues presented in "Identrus Operating Rules," IL-OPRUL-00D (Aug. 3, 1999); OCC Conditional Approval #267, Re: Operating Subsidiary Application by Zions First National Bank, Salt Lake City, Utah, Application Control Number: 97-WO-08-0006 (January 1998); and "Certification Authority Systems," OCC Bulletin 99-20 (May 4, 1999).

We interviewed officials from the Federal Reserve System and OCC to determine how the Federal Reserve System and OCC evaluate risk associated with electronic signature systems and to further understand technical accuracy and coordination issues pertaining to the Federal Reserve's Identrus Order and OCC's Conditional Approval #339, and we compared their plans to criteria we use to review electronic signature systems.

We will send copies of this letter to interested congressional committees; the Honorable Lawrence H. Summers, Secretary of the Treasury; the Honorable Donna A. Tanoue, Chairman, Federal Deposit Insurance Corporation; the Honorable Ellen S. Seidman,

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 7 2002

Director, Office of Thrift Supervision; and the Honorable Norman E. D'Amours, Chairman, National Credit Union Administration. We will also make copies available to others on request. If you have questions concerning the report, please contact Richard J. Hillman on (202) 512-8678, who will serve as the focal point. Key contributors to this letter are listed in enclosure II.

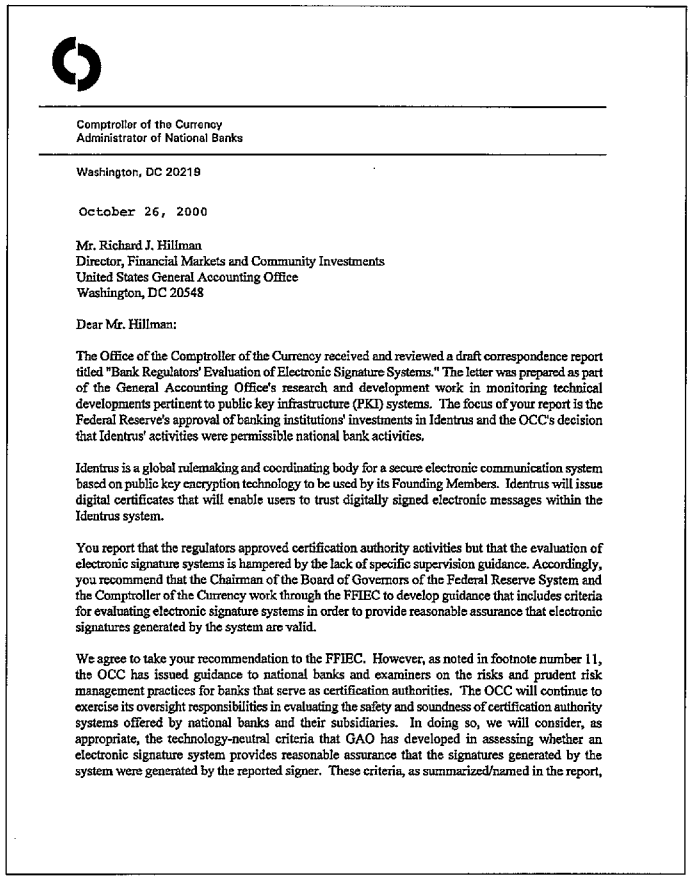
Richard J. Hillman
Director
Financial Markets and
Community Investment

Keith Rhodes
GAO Chief Technologist

Robert H. Hast
Managing Director
Office of Special Investigations

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 8 2002

Comments From OCC



Comptroller of the Currency
Administrator of National Banks

Washington, DC 20219

October 26, 2000

Mr. Richard J. Hillman
Director, Financial Markets and Community Investments
United States General Accounting Office
Washington, DC 20548

Dear Mr. Hillman:

The Office of the Comptroller of the Currency received and reviewed a draft correspondence report titled "Bank Regulators' Evaluation of Electronic Signature Systems." The letter was prepared as part of the General Accounting Office's research and development work in monitoring technical developments pertinent to public key infrastructure (PKI) systems. The focus of your report is the Federal Reserve's approval of banking institutions' investments in Identrus and the OCC's decision that Identrus' activities were permissible national bank activities.

Identrus is a global rulemaking and coordinating body for a secure electronic communication system based on public key encryption technology to be used by its Founding Members. Identrus will issue digital certificates that will enable users to trust digitally signed electronic messages within the Identrus system.

You report that the regulators approved certification authority activities but that the evaluation of electronic signature systems is hampered by the lack of specific supervision guidance. Accordingly, you recommend that the Chairman of the Board of Governors of the Federal Reserve System and the Comptroller of the Currency work through the FFIEC to develop guidance that includes criteria for evaluating electronic signature systems in order to provide reasonable assurance that electronic signatures generated by the system are valid.

We agree to take your recommendation to the FFIEC. However, as noted in footnote number 11, the OCC has issued guidance to national banks and examiners on the risks and prudent risk management practices for banks that serve as certification authorities. The OCC will continue to exercise its oversight responsibilities in evaluating the safety and soundness of certification authority systems offered by national banks and their subsidiaries. In doing so, we will consider, as appropriate, the technology-neutral criteria that GAO has developed in assessing whether an electronic signature system provides reasonable assurance that the signatures generated by the system were generated by the reported signer. These criteria, as summarized/named in the report,

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 9 2002

Enclosure I

are that the signature produced by the system is unique to the signer; under the signer's sole control; capable of being verified; and linked to the data in such a manner that, if the data are changed, the signature is invalidated upon verification. In applying these criteria and when developing further guidance, the OCC believes it is important to provide sufficient flexibility to allow the industry to benefit from the continued evolution of technology in this area.

Thank you for the opportunity to review and comment on the draft correspondence.

Sincerely,

John D. Hawke, Jr.
Comptroller of the Currency

2

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 10 2002

GAO Contacts and Staff Acknowledgments

GAO Contacts

Robert H. Hast, (202) 512-7455
Richard J. Hillman, (202) 512-8678
Keith Rhodes, (202) 512-6412

Acknowledgments

In addition to those named above, Rosemary Healy, M. Jane Hunt, John C. Martin, Kristi A. Peterson, and Harold J. Podell made key contributions to this report.

(600630)

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 11 2002

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 12 2002