UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 4 | Issue 1 Article 16

2000

Now That the Floodgates Have Been Opened, Why Haven't Banks Rushed into the Certification Authority Business

Tara C. Hogan

Now That the Floodgates Have Been Opened, Why Haven't Banks Rushed Into the Certification Authority Business?

I. INTRODUCTION

Gone are the days in which one could only transact business in buildings made of bricks and mortar. Parties that used to do business face-to-face with an ink signature, a handshake, and a look in the eyes may now be many miles apart and may never meet in person. How is that transaction possible? It is possible with the Internet. The Internet has created countless new possibilities, especially with the expansion of electronic commerce ("e-commerce"),[1] which has quickly become the preferred method of transaction for many businesses.[2]

When business transactions like e-commerce are carried out over the Internet, one simple fact may thwart the growth of e-commerce: the Internet is not secure.[3] It is well-settled that in or-

---

1. E-commerce is the "all electronic performance of business activities." THOMAS J. SMEDINGHOFF, ONLINE LAW: THE SPA'S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET, 512 (1996). E- commerce not only includes electronic data interchange (EDI), but also the use of electronic mail, electronic transfer of digital content, and electronic purchasing and payments. *See id.*

2. According to Forrester Research, it is estimated that in the U.S. alone, business-to-business Internet trade is projected to soar to $1.3 trillion by 2003. *See Identity Uncertainty Still Dogs E-Commerce*, ELECTRONIC COM. NEWS (Phillips Bus. Info., Potomac, MD), Dec. 6, 1999, *available in* LEXIS, Banking Library, PHILPS File. This is remarkable considering that the Internet only generated $48 billion in 1999. *See* Forrester Findings, *Internet Commerce* (visited Feb. 28, 2000) <http://www.forrester.com/ER/Press/ForrFind/0,1768,0,FF.html>.

3. *See* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 49 (1996). As an open network, the Internet is accessible to anyone who wants to take advantage of the fact that it is possible to access other systems connected to the network. *See* Thomas J. Smedinghoff, *The Key to Secure Internet Commerce*, OIL GLASS-CLE 201, at ¶ 2 (1998). Because the Internet "lacks rigorous access and usage controls," it is also possible to monitor and interfere with communications transmitted over the Internet. *See id.* Before the recent expansion of the Internet, electronic commerce was conducted primarily over

der for e-commerce to prosper, an elevated level of security is needed.[4] Instead of making the security of the Internet the method by which to provide security,[5] many are supporting a heightened level of authentication and certification of electronic documents "to assure the reliability and enforceability of underlying acts." In other words, because the Internet is not secure, parties must protect the messages they transmit via the Internet, not the Internet itself.

Conducting business over the Internet not only presents security challenges but also trust issues. Trust is a part of all commercial transactions, whether the transaction originates in the paper-based world or on the Internet.[6] Traditionally, trust is built over time, upon experience, and after parties interact with each other repeatedly.[7] But the very nature of e-commerce presents serious obstacles in building this traditional type of trust. E-commerce often involves one-time exchanges transacted in real time between parties who are strangers.[8] The lack of traditional paper-based methods of evidencing trust, the immediacy of electronic commerce, and the uncontrolled access to the Internet raises many practical and legal problems in e-commerce.[9] Thus,

---

closed networks. *See* Jane Kaufman Winn, *Couriers Without Luggage: Negotiable Instruments and Digital Signatures*, 49 S.C. L. REV. 739, 742 (1998). Closed networks, which were proprietary are being threatened by the open networks like the Internet, which distribute client-server computer systems. *See id.*

4. Brian Smith and Paul Tufaro, *To Certify or Not to Certify? The OCC Opens the Door to Digital Signature Certification*, 24 OHIO N.U.L. REV. 813, 814 (1998). In the commercial realm, differences in the law and the difficulty of building "trust relationships" between parties which have had no prior dealings make reliability and enforceability particularly important. *See id.*

5. *See* Digital Signature Trust Company for the American Bankers Association, *Digital Signatures: the Key to Information Technology Security* (visited Feb. 28, 2000) <http://www.se-com.com/secom/wp/aba.html> [hereinafter DST for ABA].

6. *See* Thomas J. Smedinghoff & Ruth Hill Bro, *Moving With Change: Electronic Signature Legislation As a Vehicle for Advancing E-Commerce*, 17 J. MARSHALL J. COMPUTER & INFO. L. 723, 745 (1999). Authentication, integrity, and non-repudiation are all legal issues one must consider when placing trust in a message. *See id.*

7. *See Prepared Testimony of Professor Andrew B. Whinston, Director, Center for Research in Electronic Commerce, University of Texas at Austin, Before the House Small Business Committee*, FED. NEWS SERVICE, May 26, 1999, at ¶ 2, *available in* LEXIS, News Library, FEDNEW File.

8. Real time means the parties do not have the chance to "size each other up." *See* Smedinghoff, *supra* note 3, at ¶ 2.

9. *See id.*

the anticipated growth of electronic commerce will not become a realization until parties can place trust in the security of the messages they send via the Internet.

When the Office of the Comptroller of the Currency ("OCC")[10] granted authorization to Zions First National Bank of Utah ("Zions") to establish a subsidiary to operate as a certification authority, [11] many believed the OCC "opened the floodgates" to a profitable business for banks.[12] A certification authority ("CA") is a trusted third person or entity that ascertains the identity of a person and then issues a digital certificate that attests to the association between the person's identification and the public key of a public/private key pair.[13] The key pair is used to create a digital signature.[14] Many commentators have stated that banks were the "best positioned players"[15] and ideally situated to provide CA services. [16] Since the Zions approval,

---

10. The OCC charters, regulates and supervises more than 2,600 national banks and 66 federal branches and agencies of foreign banks in the United States, accounting for 56% of the nation's banking assets. Its mission is to ensure a safe, sound and competitive national banking system that supports the citizens, communities and economy of the United States. *See* Office of the Comptroller of the Currency Home Page (visited Feb. 28, 2000)
<http:// www.occ.treas.gov/AboutOCC.htm>.

11. *See* OCC Conditional Approval Letter 267 (Jan. 12, 1998) [hereinafter Zions letter].

12. *See* Smith & Tufaro, *supra* note 4, at 813. Banks stand to make a huge profit from this new business because CAs allow commercial parties to verify and authenticate electronic signatures. *See id.*

13. *See* Thomas J. Smedinghoff, *Electronic Contracts & Digital Signatures: An Overview of the Law and Legislation*, 564 PRACTICING L. INST. 125, 149-150 (1999) [hereinafter Smedinghoff (PLI)]. Because CAs verify a signer's identity, some analogize them to notary publics and refer to them as "online notaries." *See* OCC Bulletin 99-20, *Certification Authority Systems, Guidance for Bankers and Examiners*, 1,1 (May 4, 1999) [hereinafter OCC Guidance]; *but see* John C. Anderson & Michael L. Closen, *Document Authentication in Electronic Commerce: The Misleading Notary Public Analog for the Digital Signature Certification Authority*, 17 J. MARSHALL J. COMPUTER & INFO. L. 833, 839 (1999) (contending that the notary analogy is misplaced and certification authorities deserve a "distinct, vital, and respected position, with a heightened duty of care owed to subscribers to adequately ensure the continued growth of secure electronic commerce.").

14. *See* Smedinghoff, *supra* note 13, at 149.

15. *See* David Hallerman, *Will Banks Become E-commerce Authorities?* 12 BANK TECH. NEWS, June 1, 1999, *available in* LEXIS, Busfin Library, BIS File.

16. *See* Smith & Tufaro, *supra* note 4, at 820.

however, banks have failed to jump onto the CA bandwagon.[17] Though the floodgates have been opened, U.S. banks have not rushed in. [18]

This paper begins with an explanation of the technology used by CAs (Part II)[19] and explores why banks are in an ideal position to operate as CAs (Part III).[20] Although the issues facing the CA industry are complex and have yet to be fully framed, this paper attempts to identify the reasons why banks have not become CAs (Part IV).[21] The article concludes that despite current obstacles, U.S. banks should become certification authorities and continue to evolve these services with the evolution in technology.

II. THE TECHNOLOGY USED BY CERTIFICATION AUTHORITIES

A. *Public Key Infrastructure ("PKI")*

Public key infrastructure ("PKI") is the umbrella under which certification authorities, digital certificates, digital signatures, and the implementing hardware and software operate.[22] A PKI is a "group of people who provide the necessary services to allow public key technology users to establish the authenticity of the public keys of the people with whom they are transacting business."[23] PKI has become the "accepted model" by which to

---

17. *See id.* Other U.S. banks are now operating as CAs but as a part of the worldwide company, Identrus, LLC. *See* OCC Conditional Approval Letter 339 (Nov. 16, 1999). The members of Identrus, LLC include Bank of America, Citibank, ABN AMRO, Bankers Trust Company, Barclays Bank PLC, Bayerische Hypo- und Vereinsbank AG, The Chase Manhattan Bank, Deutsche Bank, National Westminster Bank PLC, Canadian Imperial Bank of Commerce, and Sanwa Bank. *See id.* at 1. The OCC conditionally approved Indentrus to "expand activities . . . to establish and issue digital certificates." *Id.*

18. This paper limits its scope to American banks operating CAs in the United States only.

19. *See infra* notes 23- 71 and accompanying text.

20. *See infra* notes 72- 94 and accompanying text.

21. *See infra* notes 95- 162 and accompanying text.

22. For a detailed discussion on PKIs, *see generally* Michael S. Baum & Warwick Ford, *Public Key Infrastructure Interoperation*, 38 JURIMETRICS J. 359-384 (1998).

23. *See* Michael J. Osty & Michael J. Pulcanio, *The Liability of Certification Authorities to Relying Third Parties*, 17 J. MARSHALL J. COMPUTER & INFO. L. 961, 965

deliver and secure electronic communications via the Internet.[24] CAs are a vital part of the PKI because they create an environment of trust in which parties may conduct their electronic transactions using digital signatures.[25] Conversely, without the support and infrastructure of the PKI, CAs would not be able to manage and distribute certificates.

B. *Digital Signatures and Public Key Cryptography*

Signatures are a "vital element in commerce."[26] In the paper-based world, handwritten signatures legally bind parties and signify authentication.[27] Handwritten signatures, however, cannot be made online.[28] Consequently, their equivalent function had to be developed for the Internet.[29] Digital and electronic signatures now fill the role in Cyberspace that handwritten signatures fill in the paper-based world.[30] These two types of signature are different, however, and it is important to distinguish them. 'Digital signature' is a term for a technology-specific type of electronic signature, known as public key cryptography.[31]

(1999) (*citing* Information Security Committee, Section of Science and Technology, American Bar Association, *Tutorial*, 38 JURIMETRICS J. 243, 248 (1998)).

24. *See Banks Rush to Become CAs*, ELEC. PAYMENTS INT'L (Lafferty Publications, Sidcup, Eng.), May 1998, at 9, *available in* LEXIS, Banking Library, LAFNLT File.

25. *See* Osty & Pulcanio, *supra* note 23, at 965.

26. Edward Kania, *The ABA's Digital Signature Guidelines: An Imperfect Solution to Digital Signatures on the Internet*, 7 COMMLAW CONSPECTUS 297, 300 (1999). Signatures serve four basic functions. *See* Kalama M. Lui-Kwan, *Recent Developments in Digital Signature Legislation and Electronic Commerce*, 14 BERKELEY TECH. L.J. 463, 469 (1999). First, signatures authenticate the relationship between a signer and an agreement; second, a signature attests to the originality and authenticity of a document; third, a signature represents the affirmative act of signers; and finally, signatures provide a certain level of efficiency. *See id.*

27. *See* Internet Law &Policy Forum, *Description of Digital Signatures* (visited Feb. 28, 2000) <http://www.ilpf.org/work/ca/app6.htm> [hereinafter ILPF]. Handwritten signatures also represent authorship, acknowledgment, and assent. *See id.*

28. Documents on the Internet are typed not handwritten, and are not subject to the traditional notions of "signatures." *See* Kania, *supra* note 26, at 300. By merely attaching one's name at the end of an electronic document does not meet the requirement of authentication. *See id.*

29. *See id.* at 298.

30. *See* Simone van der Hof, *Documentation in the Digital Age; Laws on Digital Signatures*, SECURITY MGMT., April 1998, *available in* LEXIS, Busfin Library, ABI File.

31. *See* Smith & Tufaro, *supra* note 4, at 815. Contrary to popular belief, the

'Electronic signature' is a broader, generic, technology-neutral term that refers to the universe of various methods by which one evidences an intent to be bound by or to authenticate an electronic record, including digital signatures.[32] As between the different types of signatures, digital signatures are considered superior because they are more secure,[33] and with this security comes higher comfort in doing business online.[34]

The superiority of digital signature technology has made it the most popular technology for establishing trust during secure communications and e-commerce.[35] The technological combination of digital signatures and certificates is considered so strong that "all the leading Internet security protocols have adopted this mechanism as the vehicle of choice for authentication, privacy, and non-repudiation."[36] The digital system process accomplishes the necessary requirements for legally-binding signatures[37] and provides assurance as to the integrity and source of

---

digital signature is not a digitized image of a handwritten signature.

32. *See id.* Examples of electronic signatures include a name typed at the end of an email message by the sender, a digitized image of a handwritten signature attached to an electronic document, and a unique biometrics-based identifier, such as a fingerprint or retinal scan. *See* Smedinghoff & Bro, *supra* note 6, at 730.

33. Digital signatures are more secure because the receiver of a digitally signed communication can determine if the communication was changed after it was digitally signed. *See* ILPF, *supra* note 27, at ¶ 1.

34. *See* Lui-Kwan, *supra* note 26, at 469. "The introduction of digital signatures would make companies feel comfortable with doing business online because they would be less concerned that people were using, for example, false credit card and checking account numbers or mailing addresses. Similarly consumers may feel more comfortable doing business online because, in addition to the relative ease with which they may conduct transactions, they would be able to rest assured that the company they are dealing with is, in fact, the company it represents itself to be. For both parties, enforcing contracts using digital signatures would be simpler in the digital environment, provided that state and federal law recognizes digital signatures as representations that are enforceable as handwritten signatures." *Id.* at 469-470.

35. *Prepared Statement of Stratton D. Sclavos, President & CEO, Verisign, Inc. Before the House Committee Telecommunication, Trade and Consumer Protection Subcommittee*, FED. NEWS SERVICE, May 21, 1998, *available in* LEXIS, News Library, FEDNEW File.

36. *See id.*

37. Kania, *supra* note 26, at 301 (*citing* Gary W. Fresen, *What Lawyers Should Know about Digital Signatures*, 85 ILL. B J. 170 (1997)). To be legally binding, electronic documents must satisfy the following requirements: authenticity, integrity, and non-repudiation. *See* Smedinghoff (PLI), *supra* note 13, at 139-142. Contract law also requires that a writing and signature be included. *See id.*

the communication.[38]

So how do digital signatures work? The ability to digitally sign a document is dependent upon Public key cryptography.[39] Although the technology is not new, it is relatively new to the banking industry.[40] Public key cryptography employs an algorithm[41] using two different keys: a public key and a private key.[42] The private key, which only the signer holds, creates a digital signature, which in essence changes the communication into a seemingly unintelligible form.[43] The public key is widely known and can be used by the receiver to either verify a digital signature or return the message to its original form.[44] Although the keys are mathematically related, it is impossible to determine what the private key is from the public key.[45] Although, many may know the public key of a given signer and use it to verify that signer's signature, they cannot use the public key to discover a signer's private key and use it to forge signatures.[46]

---

38. *See* ILPF, *supra* note 27, at ¶ 1.

39. Cryptography is the branch of applied mathematics that deals with changing messages into "seemingly unintelligible forms and back again." *See Digital Signature Guidelines, Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* 1996 A.B.A. SEC. SCI. & TECH. [hereinafter Digital Signature Guidelines] (also *available in* (visited Mar. 7, 2000) <http://www.abanet.org/scitech/ec/isc/dsgfree.html>). Public key cryptography gets its name from the fact that one key will be published by the user but the other will remain a secret. *See* Froomkin, *supra* note 3, at 51.

40. *See* OCC Guidance, *supra* note 13, at 25. Before public key cryptography, the financial industry ensure confidentiality by using symmetric cryptography. Symmetric cryptography is often called "shared secret" or "secret key" cryptography and, unlike public key cryptography which requires two keys, uses one mathematical function or algorithm to encrypt and decrypt a message. *See id.* Public key cryptography adds a layer of security by requiring two keys. *See id.*

41. An algorithm is a set of rules for solving a problem in a finite number of steps, as for finding the greatest common divisor. RANDOM HOUSE WEBSTER'S UNABRIDGED DICTIONARY (2nd ed. 1998).

42. *See* Digital Signature Guidelines, Tutorial, *supra* note 39, at 9. Asymmetric cryptosystem collectively describes the computer equipment and software using two keys. *See id.* The use of two keys makes this system strong because mere possession of one key does not provide useful information about the other key. *See* Froomkin, *supra* note 3, at 51.

43. *See* Digital Signature Guidelines, Tutorial, *supra* note 39, at 9.

44. *See id.*

45. *See id.*; *see also* Lui-Kwan, *supra* note 26, at 457.

46. *See* Digital Signature Guidelines, Tutorial, *supra* note 40, at 10.

It is helpful to illustrate the process used to digitally sign a document or any other electronic information[47] by using a transaction between A and B. The sender, A, precisely designates the borders of the data to be signed. This is known as the message.[48] Using a hash function,[49] the software on A's computer computes a hash result unique to his message. Using A's private key, the software then changes the hash result into a digital signature.[50] The digital signature is the end result and is unique to both the message and the private key used to create it.[51] It is attached to the message and stored or transmitted along with the message.[52]

How does the recipient, B, verify that the message is really from A? B uses the same hash function that A used to create the digital signature to compute a new hash result.[53] Then using the public key and the new hash result, B determines if the digital signature was created using the corresponding private key and whether the newly computed hash result matches the original hash result, which was transformed into the digital signature during the signing process.[54] The most attractive feature of this technology is that a message decrypted with the public key by B could only have been encrypted with A's private key. Therefore, if A signs a document with his private key, B can use A's public

---

47. The utility of digital signatures is varied. Any information in e-commerce a sender wanted to send securely over the Internet could be sent using digital signatures. For example, contracts, images, letters, blueprints, purchase orders could all be sent via the Internet without fear of compromising the information's legally-binding status. *See* Telephone Interview with Tom Greco, Vice President of Legal and Policy at Digital Signature Trust Company (Nov. 11, 1999) [hereinafter Greco Interview]. Others envision digital signatures being used in moving real estate documents "from title companies to mortgage companies to county recorders' offices, or to transmit signed medical records from physicians to insurance companies and pharmacies." Sheila R. McCann, *Utah Stands Out As a Trailblazer for Digital Signatures*, SALT LAKE TRIB. Aug. 29, 1999, at E1.

48. *See* Digital Signature Guidelines, Tutorial, *supra* note 39, at 12.

49. The hash function is an "algorithm which creates a digital representation or 'fingerprint' in the form of a hash value or hash result." Digital Signature Guidelines, Tutorial, *supra* note 39, at 11.

50. *See id.* at 12.

51. *See id.*

52. *See id.*

53. *See id.*

54. *See id.* at 13.

key and digital signature to confirm the authenticity of the document.[55] Although this process sounds complex, A performs the signing process and B performs the verification process with little or no intervention.[56]

C. *Digital Certificates and the Role of Certification Authorities*

Although it is predicted that digital signature technology could be the most promising method for achieving security in e-commerce, its utility is limited by the ability of B to ensure the authenticity of the public key used to verify the signature.[57] Returning to the transaction between A and B, without an independent confirmation that A's message is actually from A, B does not know if he can trust that A's public key really belongs to A. C, an impostor, could have sent B his public key, purporting that it belongs to A. This transaction needs a reliable third party to not only register the public keys of the parties but to also guarantee the accuracy of the identification of the parties. The CA is this reliable third party.

The CA fills this need by issuing digital certificates that attest to some fact about the subscriber, the subject of the certificate.[58] The digital certificate is a computer-based record that contains information valuable in a commercial transaction between strangers. Information such as the identity of the issuing CA, the name, identity and some attribute of the subscriber, the

---

55. *See* Lui-Kwan, *supra* note 26, at 467; *see* Winn, *supra* note 3, at 764.

56. Digital signature software can be purchased or downloaded onto the sender's computer. *See* DST for ABA, *supra* note 5. To sign an electronic document, the user simply clicks "sign" on the computer toolbar. *See id.* The software retrieves his private key from wherever it is stored (the computer hard drive or floppy disk) and the document is signed. *See id.* The recipient clicks "verify" on his computer toolbar and the appropriate public key is retrieved from wherever it is stored (on the recipient's hard drive or an online public key repository). One bank employee noted that the technology is essentially invisible to the user. "It has become routine for us already," she notes. Hallerman, *supra* note 15; *see* McCann, *supra* note 47, at E1 (*quoting* First Security Bank employee).

57. *See* Froomkin, *supra* note 3, at 54.

58. *See* Smith & Tufaro, *supra* note 4, at 817. This is necessary because the public key and private key pair is merely a pair of numbers and has no intrinsic relationship with any one particular person. *See id.*

subscriber's public key, and the digital signature of the CA, are included in digital certificates.[59] The primary function of the certificate is to bind a key with a particular subscriber.[60]

The subscriber must provide the CA with evidence of identity, such as a driver's license, passport, or any other proof required by the CA.[61] The subscriber must then demonstrate that he holds the private key corresponding to the public key (without disclosing the private key).[62] These steps may differ from CA to CA, depending on a number of factors, including the type or level of certificate being offered by the CA.[63] Once the CA has verified the association between an identified person or entity and the public key, it issues a digital certificate.[64]

The CA digitally signs the certificate to assure both the message and identity authenticity of the certificate.[65] The subscriber may publish a certificate in an online, publicly accessible repository[66] to make it available to third parties that might want to communicate with the subscriber.[67] Repositories also house helpful information concerning certificates that have been re-

---

59. *See* Froomkin, *supra* note 3, at 58.

60. *See* DST for ABA, *supra* note 5. A subscriber is defined as the subject of a certificate that holds the private key that corresponds to the public key listed in the certificate. *See* Digital Signature Guidelines, *supra* note 39, at 63. *See also* Froomkin, *supra* note 3, at 57-64 (identifying different types of certificates and their purpose in identification).

61. *See* Smedinhoff (PLI), *supra* note 13, at 149.

62. *See id.*

63. *See id.*

64. *See id.* at 150.

65. But how does the relying party know the CA that signed the certificate is a valid CA? The CA's digital signature can be verified using the public key of the CA listed in another certificate by another CA. *See* Froomkin, *supra* note 3, at 56. This creates a hierarchy of CAs called a "certificate chain." *See id.* At the root of the hierarchy is the root certificate. *See id.* But how does one know the root CA is valid? One solution to this problem contemplates a governmental role in the certifying the keys of CAs. *See id.* The root CA would belong to a state or federal agency, and the few CAs that meet state licensing requirements would be rewarded with governmental certification of their root keys. *See id.* These CAs would then certify the root keys of organizations that wished to manage their own certificates. *See id.*

66. A repository is a "database of active digital certificates for a CA system" OCC Guidance, *supra* note 13, at 8.

67. *See* Digital Signature Guidelines, Tutorial, *supra* note 39, at 19; *see* DST for ABA, *supra* note 5.

voked or suspended due to lost or expired private keys.[68] Public access to the status of digital certificates informs relying parties so they may determine whether or not they should rely on communications digitally signed with a certain key.[69]

Digital certificates provide the necessary security for electronic transactions, but they "do not by themselves, establish a reason that they should be relied upon . . . The trust that is placed in a certificate is, in the end, a function of who has issued the certificate and that issuer's willingness to stand behind it."[70] It is at this point that bank involvement becomes important.

III. WHY BANKS AS CAS?

A. *The Attributes of Banks That Make Them Ideal CAs*

Many argue that the certification authority role should be filled by banks. The strongest argument for bank involvement in the CA business is the fact that banks are trusted entities. They are already known as providers of trust in commercial transactions because they have "long played the role as trusted intermediaries".[71] Banks have "distinctive risk-reducing features" including high capital assets, sophisticated networks, and state-of-the-art technology implementations, which collectively endow banks with a higher level of trust.[72] Banks also have the financial strength to enter into a new industry.[73]

Many larger banks have the "technical expertise" needed

---

68. *See* DST for ABA, *supra* note 5.

69. *See* Thomas J. Smedinghoff, *Certification Authority Liability Analysis*, AM. BANKERS ASS'N, (1998) [hereinafter ABA Liability Analysis].

70. Hallerman, *supra* note 15 (quoting ABAecom, a subsidiary of the American Bankers Association).

71. OCC News Release 98-4, *OCC Approves a National Bank to Certify Digital Signatures* (Jan. 13, 1998) (quoting Eugene Ludwig, former Comptroller of the Currency).

72. Smith & Tufaro, *supra* note 4, at 820. Some believe that banks are in a better position than technology companies to provide CA service because banks are more responsible. *See* Hallerman, *supra* note 15.

73. *See* Paul Corwin, *The Virtual Dotted Line: Understanding Digital Signatures*, 16 NO. 4 BANKING POL'Y REP. 1, 16 (1997).

to operate a CA due to the sudden growth of e-commerce enterprises.[74] These experiences with e-commerce would make the transition into the CA business an easy one.[75] Those banks that employ a significant amount of technology may have the necessary infrastructure to manage and oversee the risks accompanying CA business.[76] Furthermore, to fill their obligation to "know their customers", banks have implemented "stringent internal control policies, requiring them to obtain records containing information concerning the true identity of persons conducting financial transactions".[77]

Operating a certification business could confer great benefits and profits for banks and provide a new service to their customers.[78] Not only does a CA system provide potentially profitable opportunities for banks to expand their relationships with business customers,[79] but banks can shift their dominance in the physical payment infrastructure over to the Internet.[80] In addition, with the evolution of the electronic payment systems, the ability to act as a CA for digital signature technology is expected to be vital to their role in electronic payments.[81] As the digital signature infrastructure grows, financial institutions will not only benefit from the growth of electronic commerce but also from the

---

74. *See* Smith & Tufaro, *supra* note 4, at 820.

75. *See id.* at 814. Banks are familiar with and are experts in "cryptography and electronic data exchange, recordkeeping, data security, customer privacy, and the duties as a fiduciary." Corwin, *supra* note 74, at 16.

76. *See* Smith & Tufaro, *supra* note 4, at 820.

77. *Id.* at 820.

78. *See* Zions letter, *supra* note 11, at 35. The OCC notes that a businesses involving PC Banking, such as operating as a CA, can expand a bank's geographic reach, increase customer convenience, and reduce transaction costs. *See* OCC Bulletin 98-38, *Technology Risk Management: PC Banking, Guidance for Bankers and Examiners*, Aug. 24, 1998 [hereinafter OCC PC Guidance].

79. *See* Hallerman, *supra* note 15.

80. *See Banks Scent Opportunities in Secure E-commerce*, ELECTRONIC PAYMENTS INT'L, Apr. 1, 1999, *available in* 1999 WL 11541366.

81. Zions letter, *supra* note 11, at 35. The OCC expects that some form of electronic system will be needed for the electronic checking system, and a bank-based system of digital signature certificates could provide an essential foundation. *See id.* Digital signature technology could also be used to authenticate letters of credit or any other situation where remote clients need to be authenticated by a server (i.e. remote banking and Internet-based cash management systems). *See id.*

"ability to participate directly in the business functions related to issuing and storing digital certificates."[82]

Although several private non-bank CAs are currently in operation,[83] banks have several advantages over them. Notwithstanding the financial strength and reputation for trustworthiness, another major advantage is that banks are regulated by the OCC. Banks will be required to have certain standards of security and levels of assurance,[84] which non-regulated CAs are not required to have.[85] This makes it easier for banks to sell trust.

B. *The Beginning of Bank Involvement: The Zions Letter*

In January 1998, the OCC issued a conditional approval to Zions First National Bank ("Zions") to establish Digital Signature Trust Company ("DST").[86] DST is a subsidiary of Zions that will act as a CA and public key repository.[87] This approval brought certification activities to the attention of the banking industry and marked the beginning of bank involvement in the CA business. In the Zions letter, the OCC concluded that the CA activities proposed by Zions had many "functional similarities" to already recognized banking activities such as notarial and other authentication services.[88] Because of this similarity, the OCC condition-

---

82. *See* Corwin, *supra* note 73, at 17. With the experience they already have in storing information, banks could also consider serving as a repository. *See id. See also* Smith & Tufaro, *supra* note 4, at 825.

83. Several private commercial CAs are currently operating. *See* Hallerman, *supra* note 15. Among them are Verisign, Inc., GTE Cybertrust, CertCo, L.L.C, and Entrust Technologies, Inc.

84. *See* Smith & Tufaro, *supra* note 4, at 820.

85. *See* Smith & Tufaro, *supra* note 4, at 820.

86. "DST helps government and industry clients benefit from savings and service opportunities offered by the Internet through providing trusted, PKI-based digital certificate services and secure electronic commerce solutions." *Digital Signature Trust Wins U.S. Department of Defense Contract to Issue Digital Certificates*, PR NEWSWIRE, Sept. 22, 1999, *available in* LEXIS, Banking Library, PRNEWS File. DST was previously licensed by the Division of Corporations and Commercial Code of the Utah Department of Commerce. *See* Smith & Tufaro, *supra* note 4, at 822.

87. *See* Zions letter, *supra* note 11, at 1.

88. *See id.* at 23. Many banks have the power to provide notary services with the OCC's approval. *See id.* at 22. The OCC also noted the similarities between CA services and the established banking service of providing a letter of reference or

ally approved Zions' application.

The Zions letter is extremely important for many reasons. It is the "first explicit grant of authority by a federal agency to national banks to engage in certification activities".[89] The letter's detailed and thorough analysis leaves little doubt that national banks may offer CA services.[90] Second, the letter highlights the OCC's willingness to allow the banking industry to evolve with technology.[91] Third, it establishes guidance for banks wanting to get involved in e-commerce as they attempt to maximize the position of trust they have with their customers.[92] The Zions letter will ensure that banks maintain high standards of safety, security, and privacy.[93]

IV. WHY BANKS ARE NOT BECOMING CAS

Notwithstanding the prediction that the Zions letter would "open the floodgates" to the CA business,[94] Zions continues to be one of the few banks operating a subsidiary as a CA.[95] Despite the inherent qualities of the banking industry that make it suitable to provide this trust to the market, they have been extremely reluctant to do so. No one reason fully explains banks' reluctance to enter the CA business, but this paper highlights some of the risks and issues a bank faces once it decides to operate a CA as a subsidiary or provide CA services itself. The combination of all these factors may explain why banks are reacting so slowly to this new industry.

---

introduction. *See id.* at 23.

89. Smith & Tufaro, *supra* note 4, at 824.

90. *See id.*

91. *See id.* at 814

92. *See id.* The Zions letter serves as a guide for other applicants who will seek to expand their traditional banking services to keep up with technology. *See id.* The Zions letter, however, is not without its weaknesses. The guidelines are closely tied to the facts specific to Zions and DST, which may reduce the precedential value for banks not so situated. *See id.* For example, the OCC's approval is conditioned upon several expressed and implied representations made by DST and Zions and other banks may be reluctant to apply the recommendations to their bank. *See id.* at 826.

93. *See id.* at 820.

94. *See id.* at 813.

95. Bank of America and Wells Fargo are offering CA services to their corporate clients. *See* Hallerman, *supra* note 15.

A. *Identifying Risks*

Risks and uncertainty are involved with any new industry. The nature of the CA business makes this statement particularly true. Stepping into the middle of a commercial transaction and guaranteeing the identities of the parties demands that one take on risks. Recognizing the need for guidance in how to deal with such risks, the OCC issued basic guidelines for banks considering operating or currently operating CAs in 1999.[96] So as not to retard the growth of the "immature industry", the guidelines are broad.[97] Because the operational elements of a CA system are similar to that of a PC banking system, the OCC advised banks to use the CA guidelines in conjunction with the PC Banking Guidelines to identify all the risks involved in this new business.[98]

So what are the risks to banks and how do they arise? Because CA services are based on emerging technology, a CA exposes a bank to strategic, reputation, and transaction risks.[99] These risks are encountered when banks manage and issue digital certificates.[100] To issue a digital certificate, a CA must verify subscribers' identities; determine the appropriate content of the certificates; create, distribute, and ensure acceptance of digital certificates; and ensure internal activity.[101] Managing a certificate involves consumer disclosure, subscriber service and support, suspending and revoking certificates, and processing the re-

---

96. *See* OCC Guidance, *supra* note 13, at 1. The Guidelines were written to help bankers make informed decisions about the CA business. *See id.*

97. *See* E.W., *Digital Signatures Guidance, At Last, Arrives*, FIN. MODERNIZATION REP. (Am. Banker-Bond Buyer, New York, N.Y.), May 10, 1999, at 1.

98. *See* OCC PC Guidance, *supra* note 78, at 1. The OCC defines PC Banking as computer hardware, software, and telecommunication systems that enable retail customers to access both specific account and general bank information on bank products and services through personal computers (PC). *See id.* The bank's network design and telecommunication links may include the use of private networks (i.e. direct dial-in using leased or dedicated telephone lines) or public networks (i.e. the Internet). *See id.*

99. *See id.* at 2.

100. *See id.*

101. *See* OCC Guidance, *supra* note 13, at 11.

quests of relying parties.[102]

With each step of the CA process, a bank exposes itself to complex risk issues. For example, if the CA falsely or inaccurately identifies a subscriber, it may suffer financial loss or expose itself to legal action.[103] Similarly, if a CA does not properly protect its own signature with internal security, fraudulent certificates could be distributed in the CA's name, resulting in possible fraud losses and affecting legitimate subscribers or relying parties.[104]

B. Liability

Early on, industry participants were concerned that the uncertain exposure to liability would forestall the emergence of commercial CAs.[105] Currently state statutes provide the rules and regulations for banks acting as CAs, and many attempt to deal with liability issues.[106] In 1998, the American Bankers Association ("ABA") commissioned a report on CA liability.[107] From this report, five primary areas of potential liability were analyzed in detail: negligent misrepresentation, contract liability, statutory liability, intellectual property infringement, and liability for the conduct of others.[108] It is outside the purview of this paper to detail the various aspects of each area of liability, but a brief description of the above-referenced areas is warranted.

1. Tort Liability- Negligent Misrepresentation

Because a CA is in the business of providing information

---

102. *See id.* at 17.

103. *See id.* at 15-16.

104. *See id.* at 15.

105. *See* C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, 34 SAN DIEGO L. REV 1225, 1230 (1997).

106. *See* Liability Analysis, *supra* note 69, at 1.

107. *See id.*

108. *See id.* The report does not purport to analyze all the potential areas of liability. *See id.* Other areas of potential liability not discussed include antitrust, interference with contractual relationships, unfair competition, and defamation. *See id.*

that others will rely upon, the failure of the CA to exercise reasonable care could expose it to liability for the tort of negligent misrepresentation, to the extent that information is wrong or that parties rely to their detriment.[109] The scope of the CA's liability for negligent misrepresentation depends on whether the CA has a legal duty, and if it does, to whom the duty is owed.[110] Although negligent misrepresentation creates a duty to exercise reasonable care to verify facts, it does not make the CA a guarantor of the information provided.[111] Therefore, the CA is only liable if the error made is because of its own negligence.[112] The tort claims for negligent misrepresentation may also be limited by the "economic loss doctrine", which prohibits recovery in tort for product defect claims when the loss is purely economic.[113]

2. Contract Liability

The applicable law dictates which contractual and warranty obligations will exist for a CA.[114] Article 2 of the Uniform Commercial Code ("UCC") governs transactions in goods, while the common law applies to service transactions and contracts dealing specifically with information.[115] One must consider all the activities a CA is involved in to determine if contract or common law applies.[116] This categorization is important because the result determines which law a court will apply in interpreting the transaction, and one body of law may be more favorable than the other body.

---

109. *See id.*

110. *See id.* at 2.

111. *See id.*

112. *See id.*

113. *See id.* at 44 (*citing* Reeder R. Fox and Patrick J. Loftus, *Riding the Choppy Waters of East River: Economic Loss Doctrine Ten Years Later*, 64 DEF. COUNS. J. 260, 260 (1997)).

114. *See id.* at 3.

115. *See id.* at 3. If a transaction involves both the sale of goods and the provision of services, the jurisdiction determines whether the UCC or the common law applies. *See id.* at 54. The majority of courts apply the "predominant factor test" to determine if the transaction is a service or sale of good. *See id.*

116. *See id.* at 55.

3. Statutory Liability

Oftentimes statutes deal with the apportionment of liability for CAs. While operating under such a statute and subsequent enabling regulations, different liability issues may arise.[117] Some of the states that have enacted digital signature legislation deal specifically with CAs and the issue of liability.[118] Others, although they may consider the concept of a certification authority, do not specifically deal with the statutory liabilities.[119] CAs should also determine if federal or international laws would affect their services.[120]

4. Intellectual Property Infringement

Intellectual property laws protect rights "in intangible subject matters such as inventions and trademarks", including but not limited to patents, copyrights, trade secrets, and related rights emerging under unfair competition and privacy. [121] "Depending on the right infringed, remedies for infringement may include damages, profits, punitive damages, attorney's fees and injunctions against further infringement".[122] Each of these areas present challenges in the law for CAs.

5. Liability for the Conduct of Others

Most of the injuries that result from CA activities will more than likely come from the CA's employees, contractors, subscribers, and other third parties, rather than the corporate persona of

---

117. *See id.*

118. For example, Utah's digital signature legislation dealt specifically with liability apportionment. *See id.* at 88; *see also infra* notes 145-160 and accompanying text.

119. *See id.* at 88.

120. *See id.*

121. *See id.* at 6.

122. *Id.*

the CA itself.[123] Therefore, the CA "should be aware that it may be legally accountable for the use (and misuse) of its CA services by CA employees and contractors."[124]

C. *Costs*

The cost to build the necessary components of a PKI is another factor that may discourage banks from deciding to operate a CA. "The cost structure of technology requires tremendous investment in the infrastructure to make it possible to efficiently process information and to handle heavy traffic and deliver satisfactory service."[125] Some of the financial requirements of a network security solution include "high fixed costs, long implementation timeline[s], economies of scale, and ongoing support costs."[126] A 1998 study by GIGA Information Group revealed that support costs for a five-year long project are between $4.2 and $9.8 million for a 20,000 Certificate PKI, with full life cycle management.[127]

Costs as great as these create a "chicken-and-egg" riddle.[128] The PKI must be built, but one must find justification for the building of the infrastructure.[129] Even if the creation of CAs is a requirement before the projections of growth in e-commerce become reality, the ratio of initial investment costs to the value of digital transactions may be a factor in preventing this growth from becoming a reality.[130] But once the infrastructure is built,

---

123. *See id.* at 7. Although not directly responsible, the CA could be liable "under the theories of (a) vicarious liability, (b) agency, (c) contributory infringement, (d) corporate negligence, and (e) liability for the criminal conduct of a third party." *Id.*

124. *Id.* at 8.

125. Whinston, *supra* note 7.

126. *Digital Signature Trust Company, Outsourced CA Services* (visited Feb. 28, 2000) <http://www.digsigtrust.com/why.html>. DST offers full service CA outsourcing. *See id.*

127. *See id.* This, of course, varies according to PKI software vendor, internal business requirements, existing infrastructure, and specific organization. *See id.*

128. *See* Corwin, *supra* note 73, at 17.

129. *See* Greco Interview, *supra* note 47.

130. *See id.*

the cost decreases with the number of products offered.[131] The few banks participating in the CA business have turned to outsourcing some of the CA functions to help reduce these costs.[132]

D. *Potential Profit: How Much Can Banks Make From CA Services?*

This paper has assumed that since CAs are necessary for a viable e-commerce, once banks decide to operate as CAs, the projections of the success of e-commerce will lead to enormous profits for banks. Some experts are skeptical of the promises for profit because it remains unclear "if this [CA] concept will develop into a viable commercial service."[133] A commercial equivalent to CA services does not currently exist, and while proponents have been confident that the need for security on the Internet would trigger a demand for CA among commercial parties, there is no precedent to support operating an identification service for profit.[134] As of now, not many applications for digital signatures exist.[135]

The function of digital certificates as a "uniform identification in cyberspace" has been compared more to the ministerial functions performed by government officials while conducting official business, rather than a service commercial parties rely on to transact with strangers.[136] Furthermore, commercial parties commonly rely on letters of credit services offered by banks, which not only attest to the identity of the parties, but also their creditworthiness. Thus, the functions that a CA would perform are redundant.[137]

---

131. *See* Whinston, *supra* note 7.

132. *See* Hallerman, *supra* note 15.

133. *See id.*

134. *See id.*

135. *See* Greco Interview, *supra* note 47.

136. *See* Winn, *supra* note 3, at 772. The CA business model as discussed by Winn is that described in the Digital Signature Guidelines released by the ABA. *See id.* For the purposes of this paper, however, no one particular model is favored over another.

137. *See id.*

Despite the above suggestions, the potential for profit from CA services is still an incentive. Even if the cost per transaction is low, the mere number of transactions a CA would perform could result in substantial financial benefits.[138] In addition, banks operating CAs could determine the pricing structure that would be the most financially beneficial to them.[139] Digital certificates could also be forging into new territory in the security industry by replacing the current password schemes,[140] and creating another potential profit producing product. In some instances, digital certificates could replace multiple passwords with a single sign-on.[141] This would decrease password administration costs and nearly justify the costs of developing PKI technology.[142]

E. Knowledge

The fact that the banking industry is still learning about digital signature technology and its possibilities may add more insight into this issue. Banks are still in the "typical technology adoption cycle,"[143] and until they understand the technology and the business benefit, they will not employ it. Insiders suspect that those in the legal and medical professions will be the first to seize and utilize digital signature technology because they face the most liability if the work they display on cyberspace is not secure.[144]

---

138. Hallerman, *supra* note 15.

139. Zions, for example, prices digital signature services based on the type of service: transactions, consulting-type services, or the delivery of turnkey solutions to the user. *See Zions: Melding Tradition and Innovation*, FIN. MODERNIZATION REP. (Am. Banker-Bond Buyer, New York, N.Y.), Feb. 1, 1999, at 1, *available in* LEXIS, Banking Library, ABBB File. The fee could be adjusted for those customers who do a high volume of business. *See id.*

140. *See* Hallerman, *supra* note 15. When dealing with more serious transactions, more security is required. *Id* As of now, passwords do not provide that higher level of security. *See id.* Digital certificates are also easier to use and more secure than passwords. *See id.*

141. *See id.*

142. *See id.*

143. *See* Hallerman, *supra* note 15.

144. *See* McCann, *supra* note 47, at E1.

F. State Legislation

State legislation plays a significant role in the potential growth of CAs. The "duties and liabilities imposed upon CAs under United States law are unclear", as might be expected due to the complete absence of federal statutes, case law, and the relatively small number of functioning CAs.[145] The most basic issue to be addressed by e-commerce legislation is enforceability of e-commerce transactions.[146]

Recognizing the problems posed by e-commerce legislation, almost every state has enacted some sort of e-commerce or digital signature legislation,[147] which ultimately affects the plight of CAs. States have taken various approaches to this legislation, ranging from minimal to very formal and highly regulatory.[148] Even though states are responding to the sudden emergence of digital signature technology by enacting legislation, this state-by-state approach makes it more difficult and cumbersome for operating CAs.

A brief examination of two state statutes concerning the licensing of CAs, Utah and North Carolina, demonstrates the discrepancies that banks will find in statutes. The Utah Digital Signature Act, [149] which licensed DST Company, was the first comprehensive digital signature legislation and is the "most prescriptive" legislation thus far passed.[150] The Act imposes strict requirements on CAs by specifying what constitutes as adequate record-keeping and detailing procedures CAs must follow when they issue, revoke or suspend a digital signature certificate.[151] The Act adopted a voluntary licensing procedure for CAs.[152]

---

145. Smith & Tufaro, *supra* note 4, at 818.

146. *See* Smedinghoff & Bro, *supra* note 6, at 726.

147. The Chicago law firm McBride, Baker, and Coles provides a comprehensive summary of enacted and pending digital signature state legislation at <http://www.mbc.com/ecommerce/legis/table01.html> (visited Feb. 28, 2000).

148. *See* Smedinghoff & Bro, *supra* note 6, at 728.

149. Utah Code Ann. § § 46-3-101 - 46-3-544 (1999) [hereinafter the "Act"].

150. *See* Liability Analysis, *supra* note 69, at 88.

151. Smith and Tufaro, *supra* note 4, at 819.

152. UTAH CODE ANN. § 46-3-201 (1999).

Utah apportioned liability such that licensing a CA substantially decreases the amount of liability shouldered by the CA. More specifically, a licensed CA in Utah enjoys a liability safe harbor,[153] protection from reliance on a forged digital signature,[154] a cap on liability,[155] and a limit on compensatory damages.[156]

In 1998, North Carolina passed the Electronic Commerce Act[157] to "facilitate electronic commerce with public agencies and regulate the application of electronic signatures when used in commerce with public agencies."[158] North Carolina has a mandatory licensing process, requiring CAs to be licensed by the Secretary of State.[159] The statute, unlike the Utah Act, does not set forth any standards by which the CA is to operate.[160] It leaves that task to the Secretary of State.[161] But if the Secretary of State for North Carolina decides to require substantially different regulations than the Utah statute, a CA faces the difficulty of complying with both statutes.

V. CONCLUSION

Though the OCC has paved the way for banks to operate as certification authorities, it is still unclear whether banks will "jump on the bandwagon" as predicted. Although many technological and liability issues are currently a part of the reality of the certification business, the demands of e-commerce and the need for more security will push banks reluctantly into the industry.

---

153. § 46-3-309.

154. § 46-3-309(2)(a). The CA must comply with all material requirements of the Act. *Id.*

155. *Id.* The CA shall not be liable in excess of the recommended reliance limit for either a loss caused by reliance on a misrepresentation in the certificate or for failure to comply with the Act's guidelines for issuing certificates. *Id.*

156. § 46-3-309(2)(c). This limit does not include damage for lost profits or for pain and suffering. § 46-3-309(2)(c)(iii).

157. N.C. GEN. STAT. § § 66-58.1- 58.11 (1999).

158. § 66-58.1.

159. § 66-58.3.

160. *Id.*

161. *See id.* These standards may include, but are not limited to technical, physical, procedural and personnel security controls, repository obligations, and financial responsibility standards. *See id*

The best option for banks considering operating a CA is to create a subsidiary and outsource the technology aspects. This strategy allows banks to limit their liability, decrease the cost of building the PKI infrastructure, minimize the necessity to understand and know the technology while providing this service to its customers. The bank could still brand the product as its own.[162] As industry forerunners, the American Bankers Association ("ABA")[163] has partnered with DST to do just that. In September 1998, DST partnered with the ABA to create the subsidiary ABAecom.[164] DST will provide ABAecom with CA services, including digital certificates, PKI, and CA outsourcing and consulting for ABA-members.[165] ABAecom's first product is SiteCertain, an interactive seal on the member bank's Web site that connects customers to ABAecom's secure online database.[166] ABAecom, with DST performing the PKI services, serves as the CA for SiteCertain. This way, the bank brands the CA service and decides who is certified, while the provider runs the PKI.[167]

The mere fact that banks may make money from the CA enterprise will not be the only factor that motivates mass bank involvement. The opportunity to take advantage of new tech-

---

162. *See* OCC Guidance, *supra* note 13, at 11. The OCC projected that continued emphasis on PC banking would force a bank to rely on service providers and software vendors to design, implement, and manage these systems. *See* OCC PC Guidance, *supra* note 79, at 7. The extent to which banks decide to do this will affect the extent of the bank's actual involvement and risk. *See id.*

163. "The ABA brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership-which includes community, regional, and money-center banks and holding companies, as well as savings associations, trust companies, and savings banks makes ABA the largest banking trade association in the country." DST for ABA, *supra* note 5.

164. *See* Hallerman, *supra* note 15. ABAecom's goal is to help banks build stronger relationships with their customers and increase usage of their online products by issuing digital signatures. PR NEWSWIRE, September 28, 1998.

165. *See ABA Launches Electronic Commerce Subsidiary; ABAecom Will Serve As Catalyst for Secure Online Transactions*, Sept. 28, 1999, *available in* LEXIS, Banking Library, PRNEWS File.

166. *See id.*

167. Credit card company Visa has partnered with VeriSign, Inc. to offer Secure Socket layer (SSL) certificates to large banks that manage the merchant accounts of businesses and handle their payments (so-called acquiring banks). *See Visa Helps Banks Offer Secure E-Commerce*, COMM. WEEK INT'L 13, June 21, 1999, *available in* 1999 WL 11859598.

nology that could revolutionize the banking industry is an even better motive. The most exciting feature of PKI technology is the fact that banks will have the ability to send blue prints, purchase orders, contracts, and other electronic data securely over the Internet. This capability would change not only how banks do business but also with whom they do business.[168] Banks have the unique opportunity to provide the trust and security needed for e-commerce, while utilizing cutting edge technology. Even though they have not "jumped on the bandwagon," they should.

TARA C. HOGAN

168. *See* Greco telephone interview, *supra* note 47.