Comptroller of the Currency
Administrator of National Banks

Washington, DC 20219

January 12, 1998

Stanley F. Farrar, Esq.
Sullivan & Cromwell
444 South Flower Street
Los Angeles, CA 90071-2901

Re: Operating Subsidiary Application by Zions First National Bank, Salt Lake City, Utah, Application Control Number: 97-WO-08-0006

Dear Mr. Farrar:

Zions First National Bank (the "Bank") has filed an application ("Application") to establish an operating subsidiary that will act as a certification authority and repository for certificates used to verify digital signatures. The proposed subsidiary (the "Company") will be located at the Bank's main office at One South Main Street, Salt Lake City, Utah. Based upon the commitments and representations in the Bank's notification letter and other materials, the Bank's establishment and operation of the Company is approved, subject to the conditions set forth herein.

A. Background

1. Digital Signatures and Public/Private Key Infrastructure

Digital signatures are a form of electronic authentication.[1] Specifically, a digital signature is a string of characters appended to an electronic message that serves to uniquely identify the sender to the recipient and, thereby, provides electronic authentication. Digital signatures can be generated using public key cryptography.[2] Some signatures created with public key

[1] Electronic authentication is any electronic means by which the recipient of a message can be confident of the senders's identity. For example, a personal identification number (PIN) provides electronic authentication for transactions initiated at a bank ATM. Other forms of electronic authentication are being developed in addition to digital signatures.

[2] Public key cryptography is a complex encryption method in which the sender uses one mathematical function to convert a message from clear to encoded text, and the receiver uses a different, but related, mathematical function to convert the encoded message into clear text. Public key cryptography is sometimes called asymmetric

cryptography also provide for message integrity. These digital signatures are a compressed and encoded version of the message (a hash) to which they are attached. With such signatures, the recipient of the message is able to compare the decoded signature hash with a hash created from the message text, thereby confirming that the message has not been altered in transmission.

In order for a digital signature system to operate successfully, message recipients must have assurance that the public key used to decode a message is uniquely associated with the purported sender of the message. One method of providing that assurance is for a trusted third party to issue a digital certificate attesting to this association. A digital certificate is an electronic document that formally associates a digital signature public key with the "owner" of the public/private key pair used to create and verify a digital signature. In other words, the certificate attests that the public key associated with a digital signature is "bound" to its owner and the certificate contains the public key or information directing the message recipient to the public key. The message recipient can verify the validity of the digital certificate because the certificate also contains the digital signature of the trusted third party. In addition, the digital certificate may contain other information such as its validity period, the type and number of messages for which the signature is authorized, as well as some indication of the issuer's liability related to use of the certificate.

A trusted third party that issues a digital certificate is called a certification authority ("CA"). The CA electronically generates and signs (using its own digital signature) digital certificates to verify the identity of a person transmitting a message electronically. The transmitting person holding a certificate, called a subscriber, may be a firm, individual, or even a computer facility. The recipient of an electronic message who depends on digital certificates for authentication is called a "relying party." A CA is also likely to perform additional functions within an electronic messaging system using digital certificates such as providing a listing or repository of public keys and a certificate revocation list, both discussed below.

2. Proposed Activities

As a certification authority, the Company's primary role will be to verify the identity of a subscriber and bind the subscriber to a public/private key pair by means of a digital certificate. After taking appropriate steps to ensure the identity of the subscriber and their relationship to

---

cryptography because the functions to encode and decode are not the same. The mathematical function the sender uses to encode a message is referred to as the sender's "private key." The related function that the recipient of the message uses to decode is called the sender's "public key;" it is publicly available. The recipient uses this public key to convert to clear text a message that has been encoded by the sender using his or her private key. A public/private key pair is a set of uniquely associated mathematical functions; a particular public key will decode only messages encoded by its associated private key. Thus, provided one has assurance that a specific private key is associated with a person and under their sole control, any message that can be decoded using that person's public key may be assumed to have been sent by that person.

their public key, the Company will issue the certificate containing and confirming the authenticity of the public key.[3] To provide a complete public key infrastructure, the Company will also act as a public key repository[4] so that relying parties will be able to verify the validity of the signer's public key and, thereby, the authenticity of the digital signature and the integrity of the signed message.

The Company has obtained a license to operate as a certification authority and repository under Utah law. See Utah Code § 46-3-201.[5] The Company will issue and sign its own root certificate.[6] As a certification authority and repository, the Company will establish and maintain facilities including data processing, data storage, and data communications devices.[7] The Company may provide and sell software that generates public/private key pairs for

---

[3] The Company will not "issue" public/private key pairs, but only certificates to authenticate subscribers and their relationships to their keys. The subscribers will generate their own signing key pairs. The Company will have no access to a subscriber's private signing key.

[4] A repository is an accessible database or system for storing and retrieving digital certificates or information about digital certificates.

[5] Several states, including Utah, have recently passed laws legitimizing and regulating the use of "digital signatures." The Utah Digital Signature Act (the "Act"), a copy of which is included in the public exhibits to the Application, has as its purposes: "(1) to minimize the incidence of forged digital signatures and enable reliable authentication of computer-based information; (2) to enable and foster the verification of digital signatures on computer-based documents; (3) to facilitate commerce by means of computerized communications; and (4) to give legal effect to [various industry] standards…." Utah Code § 463-102. The Utah law provides for voluntary licensing.

[6] In some cases, relying parties will want to look behind the certificate issued by a CA to determine the authenticity of *that* certificate. To permit this verification, someone will need to certify the CA's public key, i.e., act as the "root" certification authority. Here, the Company will not rely on any third party to act as its root CA. However, as the number of CAs increase, a CA might arrange to certify the certificate of another CA so that the certificates issued by each can be relied upon by subscribers to the other authority. This process is called "cross-certification." The Company, however, does not currently have any contracts or arrangements with other CAs to provide for cross-certification. If in the future the Company wishes to enter into a cross-certification arrangement, it will need to submit a further application to OCC describing such an arrangement.

[7] As a condition of this approval, the OCC will require the Company to submit a complete description of the Company's information systems and back office operations architecture prior to commencing service operations. This description should include the following items: proposed third party software and vendor services to be used; operating processes; security controls; internal controls; and internal audit plans. The Company's internal data processing systems will be year 2000 complaint within the time frames specified in OCC Advisory Letter 97-6 and other subsequent OCC issuances. Further, the Company will perform due diligence to ensure that any third-party data processing service providers or purchased applications or systems it uses will also be year 2000 compliant in accord with OCC issuances. Moreover, as a condition of this approval the OCC will require that the Company notify all potential vendors in writing of the OCC's examination and regulatory authority under 12 U.S.C. § 1867(c) and that all vendor contracts shall stipulate that the performance of the services provided by the vendors to the Company is subject to the OCC's examination and regulatory authority.

subscribers. The Company may also purchase or develop, and may provide to its customers, software enabling them to create or receive messages with digital signatures, verify digital signatures with one or more authenticated public keys, and confirm that the messages were properly signed by the sender.[8]

As noted, the Company will operate a repository maintaining a database of certificate information. In that capacity, it will accept requests for certificates and will publish such certificates. It will also publish notification of revoked certificates by means of a certificate revocation list available to registered users of the repository. In connection with the foregoing, the Company will transmit signed and unsigned digital messages to subscribers and other parties. The information stored by the Company in its repository will be provided to registered users on a fee-for-service basis, such as fees for downloading a certificate. The Company's systems are also expected to provide registered users with transaction/billing logs and, if such users are registered for direct or automatic billing, to allow them to authorize automated account billing.[9]

The Company, as part of its function as a certification authority and repository, will provide connected data processing services. Such services will include the receipt and transmission of digital signature certificates through dedicated, private networks or over the Internet or, by modem, over the public switched telephone network. The Company will also manage such documents, store them on magnetic, optical or other media, and establish systems for providing and controlling access to the data.

In addition to its certification authority and repository service, the Company may provide related services and products. It may sell or rent software or hardware, such as "smart card" readers, for use on computers creating or transmitting digital signatures or signed documents.[10]

---

[8] Because digital signatures use encryption technology, the software used and provided by the Company is capable of being used for message encryption. However, the Company does not expect to specifically market or develop any services or software for the purpose of facilitating message encryption, even though it may, as an incident to its other functions, use third-party software standards for legally allowable levels of security for its Internet communications. The Company has committed that it will comply with all applicable laws and regulations regarding encryption technology, including key recovery and export restrictions. Should the Company wish to market message encryption services, it will need to file an application with the OCC.

[9] One of the Company's first activities is expected to be issuance of certificates to support the transmission and authentication of filings in Utah state courts. The court filing fees and fees for transmission and verification are expected to be collected by the Company and the Bank, with the filing fees being collected automatically and transferred to an account maintained by the State of Utah with the Bank.

[10] Any equipment to be sold by the Company will be sold for the purpose of being used only in connection with the Company's certification authority and repository services and other digital signature or data security systems.

The Company may also provide consulting or advisory services to help customers, including other banks, to implement digital signature systems.

In connection with its CA activities, the Company will acquire confidential information relating to subscribers. It will obtain the information directly as part of the personal identification and registration process. Also, the Company will indirectly acquire information through the repository function regarding the transactions that subscribers are conducting using digital signatures to the extent that relying parties verify those signatures through the repository. The Company will describe in detail its confidentiality treatment of such information in its certificate practice statement ("CPS").[11]

Further, the Company is committed to provide clear and appropriate disclosures on issues of significance in addition to privacy, such as potential consequences and liabilities from unauthorized use of private keys, procedures for reporting compromised keys, error resolution procedures, and relevant fees and charges.[12] In addition, the Company will ensure that clear and appropriate information is available to relying parties.

Finally, as a separate service unrelated to digital signatures or its CA activities, the Company may also hold in escrow keys that are used for encryption. This will allow customers using key encryption, e.g., for internal secure data storage, to recover encrypted data if a encryption key is lost or abused. Thus, the Company may hold in escrow duplicates of the encryption keys of employees of a client to prevent negligent or malicious loss of data resulting, for example, from the departure of such an employee.[13] The Company will not hold in escrow private keys used to create digital signatures.

3. Risk Controls

---

[11] The CPS will state that the Company will release consumer information to law enforcement authorities upon receipt of a relevant search warrant or subpoena, and will respond similarly to a relevant discovery order or subpoena in a civil litigation setting. The Company will not release information in any other manner. Similarly, while the repository software will automatically maintain audit trails of all repository activities, the Company has no intention of compiling this information in a manner that associates particular relying paries with particular subscribers unless required to do so by warrant, subpoena, or order. The Company will not sell such information or use it for marketing.

[12] The Company understands that such disclosures will be particularly important when it begins to offer its services directly to consumers who have limited knowledge about the functionality and prudent use of the technology. Initially, the Company does not plan to offer certification authority services directly to consumers or enter into arrangements under which consumers would look to the Company for support services or error resolution processes. However, when the Company does deal directly with consumers, the Company will have appropriate consumer support and error resolution procedures.

[13] Under Utah law, the Company holds any such encryption keys as a fiduciary. See Utah Code § 46-3-303. The Company does not currently foresee any need to hold, invest, or distribute trust funds.

The Company will implement a range of measures designed to mitigate and control risks arising from its CA and other activities. To that end, the Company will at a minimum and among other things conform with relevant standards established by various independent industry groups and standards organizations such the American National Standards Institute ("ANSI"), National Institute of Standards and Technology ("NIST"), and National Security Agency ("NSA").

The Company will apply the Bank's established internal policies and procedures on customer identification, albeit modified to apply to CA activities. Thus, for example, the Company will not issue a certificate to anyone who does not physically present themselves at an office and provide reliable photo-identification. More specifically, the Company will develop a written CPS that will describe identification practices, including both the mandatory identification items and specified cross-checks on those items.[14] The CPS will also describe in detail the types of certificates that may be issued, including liability limits on certificates, expiration dates, and transaction limits (types and frequency) on certificate uses.[15]

The Company recognizes that one of its most serious risks is that *its* private key might be compromised. However, it will employ numerous safeguards --software, hardware, and procedural-- against this risk. The Company's system architecture will also be confirmed by an entity accredited by the National Voluntary Laboratory Accreditation Program ("NVLAP") of NIST. Similarly, the Company will use software, hardware and procedural measures to prevent and detect unauthorized efforts to access or revise repository data that might suggest tampering with a public key in the repository.[16] Prior to commencing operations, the Company plans to engage an independent consulting firm to perform a full functionality and security review of the proposed system. Further, once operational, the Company plans to

---

[14] The Company plans to use local registration agents ("LRAs") for some subscribers. The LRAs will collect documentary evidence of personal identification of potential subscribers by reviewing documentary evidence and/or personally interviewing the applicant. This information would be transmitted to the Company for certification issuance. Among other situations, these LRA arrangements will arise when the Company provides service bureau CA services to organizations. As part of the service arrangement, the organization would agree to act as the LRA in establishing the identity of the individuals within the organization that it wishes to be certified. The Company will build additional risk controls into their LRA contractual agreements. For example, the Company will require the LRA to hold the Company harmless as to authentication risk and to indemnify the Company from potential damages for negligence or fraud in authentication. The Company may also require that some LRAs post a surety bond or letter of credit in favor of the Company. While the Bank or its branches may be used as a LRA, the Bank will not issue such indemnification or post such security if it acts as a LRA.

[15] The Company may tier its mandatory level of identification to different reliance limits so that as the risk level increases, the verification requirements also increase. The OCC will review the Company's CPS statement and other critical operational components before the Company begins full operations.

[16] The Company will not escrow or have access to the subscribers private signing key, thus avoiding the risks that the Company might be held liable for a failure to securely hold such keys. The risks with respect to escrowing private encryption keys are discussed below.

engage an independent public accounting firm to audit on a periodic basis, among other things, the adequacy of its systems security and internal controls.

Additionally, the Company plans to use a number of legal devices to control and limit its risk of liability. For example, the Company plans to take certain steps to ensure that Utah law, which contains limitations on the liability of licensed CAs, is the law that will control its relationships. Thus, the Company will insert in its subscription contracts a choice of law provision designating Utah law as controlling.[17] The Company may also place in the contracts limits on the use of the certificates.[18] With respect to risk of liability due to errors in authentication of digital signatures, the Company will seek indemnification by clients and protection under statutory limitations on liability under Utah Code §§ 46-3-308(2) and 46-3-503. The Company recognizes, however, that its ability to control its liability by contract is not complete and will take appropriate steps to manage its liability.[19] One such measure could include placing disclaimers in the CPS.

The Company is also exploring the procurement of insurance to cover risks. The Company expects that the insurance will be modeled after service bureau coverage and will include traditional E&O (quality control), a fidelity bond (personnel), and computer crime (system security) coverage.

Finally, the Company also recognizes that the escrowing of encryption keys could present special additional risk because any misappropriation of key data could result in harm to a customer. The Company will mitigate this risk by using a dual control system of key escrow

---

[17] The Company will do business with subscribers outside of Utah, but only with wholesale customers, not retail consumers, so the Company believes that the risk of having its choice of law provisions overridden is slight. The Company will eventually, however, do business with retail consumers in Utah. Moreover, for the first five years, the Company will largely provide certificates for use in "closed systems" where contractual relations exist between or among all parties using or relying upon the certificates, thus, increasing its ability to ensure that all parties are bound by choice of law covenants. In connection with this application, the Bank has agreed that the Company will provide OCC thirty days advance notice of the material details and provisions in any binding commitment by the Company to provide digital certificates for a non-closed system unless the OCC has waived in writing such notice generally or with respect to a particular non-closed system.

[18] For example, in the subscription contract and the CPS, the Company may place limitations to control liability exposure including reliance limits, limitations on the number of transactions that a certificate can be used for, an expiration date on the certificate, and limitations on the types of transactions for which the certificate can be used (e.g., only non-financial transactions).

[19] For example, some warranties deemed to be made by a certification authority under Utah law may not be limited or disclaimed by contract. Utah Code § 46-3-404(1)(b). Moreover, contractual limitations will be ineffective to limit liability to relying parties with whom there is no contract.

in which both the client and the Company would have separate keys needed to be used jointly to recover the escrowed key.[20]

4. OCC Supervision

As an operating subsidiary, the Company will be subject to OCC examination and supervision. 12 C.F.R. § 5.34(d)(3). As part of the application process, OCC examiners evaluated and assessed the Company's proposed activities and how the OCC would supervise those activities. The OCC examiner assigned to the bank also has regularly met with management of the Bank and the Company to discuss their plans and monitor the direction of the project. In addition, an OCC examiner with special expertise in bank information systems regularly met with key employees of each of these entities to discuss their plans, monitor project management and observe trial implementations. OCC also conducted an onsite examination of the Bank and its data processing subsidiary in March 1997. Included in the scope of that review was a thorough examination of the digital signature project with the objective of enhancing the OCC's familiarity with the proposed activity and identifying risks to the bank in implementing this business. In addition, the OCC Bank Technology policy and operations staff is developing a supervisory issuance on national bank CA activities.[21] The issuance will provide basic information and general risk analysis for banks that are considering investing in, providing services to, or operating a certification authority. The Company will be subject to this guidance.

Going forward, the OCC will continue to monitor developments in the certification authority industry and the specific operations at the Company. Supervision of the Company will be the responsibility of the team of examiners assigned to the bank, a team with expertise in banking operations and bank information systems. This team will conduct an on-site exam focusing on the security architecture and internal controls as the Company begins operations, and will maintain contact with Company management between regularly scheduled annual on-site exams. In addition, the team will monitor and examine as necessary the performance of any major non-bank service provider of the Company.

As part of its on-going supervision of the Company, the OCC also expects the Company to prepare and implement a risk management plan that identifies all specific material risks and identifies the mechanisms the Company will use to manage those risks, including a description of proposed control mechanisms. The Bank is currently a well capitalized and well managed institution and has the willingness and ability to provide the capital necessary to support this

---

[20] Under this system, the escrowed private key would itself be encrypted with two separate single-key passwords held in a physically secure manner by each of the Company and the customer.

[21] This OCC unit has responsibility to monitor developments in information technology at bank and nonbank firms to ensure that the OCC implements an appropriate supervisory strategy to address the risks that national banks face in offering products, services, or processes that utilize new technologies.

Company. The OCC expects the Company to maintain an adequate level of capital based upon, among other factors, the level of operations of the Company, the level of risk in those operations, and the working capital needs of the Company. The OCC will evaluate the adequacy of such capital as part of its on-going supervision of the Company.

B. Discussion

The National Bank Act, in relevant part, provides that national banks shall have the power:

> [T]o exercise … all such incidental powers as shall be necessary to carry on the business of banking; by discounting and negotiating promissory notes, drafts, bills of exchange, and other evidences of debt; by receiving deposits; by buying and selling exchange, coin, and bullion; by loaning money on personal security; and by obtaining, issuing, and circulating notes …

12 U.S.C. § 24(Seventh).

The Supreme Court has held that the powers clause of 12 U.S.C. § 24(Seventh) is a broad grant of power to engage in the business of banking, including but not limited to the enumerated powers and the business of banking as a whole. See NationsBank of North Carolina, N.A. v. Variable Life Annuity Co., 512 U.S. 251 (1995) ("VALIC"). Judicial cases reflect three general principles used to determine whether an activity is within the scope of the "business of banking": (1) is the activity functionally equivalent to or a logical outgrowth of a recognized banking activity; (2) would the activity respond to customer needs or otherwise benefit the bank or its customers; and (3) does the activity involve risks similar in nature to those already assumed by banks. See, e.g., Merchants' Bank v. State Bank, 77 U.S. 604, 648 (1871) (certification of checks has grown out of the business needs of the country and involves no greater risk than a bank giving a certificate of deposit); M&M Leasing Corp. v. Seattle First Nat'l Bank, 563 F.2d 1377, 1382-83 (9th Cir. 1977), cert. denied, 436 U.S. 987 (1978) (personal property lease financing is "functionally interchangeable" with the express power to loan money on personal property); American Ins. Assoc. v. Clarke, 865 F.2d 278, 282 (D.C. Cir. 1988) (standby credits to insure municipal bonds is "functionally equivalent" to the issuance of a standby letter of credit). Further, as established by the Supreme Court in VALIC, national banks are authorized to engage in an activity if it is incidental to the performance of the five enumerated powers in section 24(Seventh) or if it is incidental to the performance of an activity that is part of the business of banking.

For the reasons below, we find the activities of certification authority and repository and key escrow to be part of the business of banking because they meet the three part test.[22] Specifically, certification authority activity is part of the business of banking regardless of whether the certificates are used for financial transactions because the activity is: 1) the functional equivalent of notary and other authentication services already provided by banks, and 2) a logical outgrowth of the identification and verification skills that are a core competency of banks. Further, the key escrow service is part of the business of banking because it is the functional equivalent of traditional bank safekeeping services. Each of these activities benefit the bank and its customers and present risks (albeit manifested in a technologically advanced form) similar to those that banks have previously and successfully assumed.

1. CA activity is a functional equivalent to recognized banking activities.

National banks have a well established power to provide notary services as part of the business of banking. The OCC has previously opined that a national bank and its employees may provide notary public services. See Unpublished letter from Wallace Nathan dated June 11, 1985; Unpublished letter from William Glidden dated January 17, 1992; and Unpublished letter from OCC Law Department dated September 16, 1975. Similarly, the courts have found that notary services are within the business of banking. Transamerica Insurance Company v. The Valley National Bank, 462 P.2d 814 (1969). Finally, the American Society of Notaries reports that the banking industry is among the greatest employers of notaries. Letter of Lisa Fisher, Executive Director, American Society of Notaries, Exhibit C to the Application. According to the American Society of Notaries:

---

[22] The Bank proposes to engage in certification authority and repository services. At first glance, these would seem to be separate services which ought to be analyzed separately to determine whether they are permissible. However, we believe that there are several activities that are so essential to the operation of a public key infrastructure that they must be deemed part of a certification authority service for purposes of bank powers analysis. Cf. Interpretive Letter No. 345, reprinted in [1985-1987 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶85,515 (July 9, 1985) (essential integrated equipment should not be deemed to be separate from the related service). For example, a public key system needs a "certificate revocation list" so that a relying party can determine if a particular certificate was revoked or suspended. Information Security Committee, Science and Technology Section, American Bar Assn., DIGITAL SIGNATURE GUIDELINES (1996) 15-16 (hereinafter: "ABA Guidelines"); and Thomas J. Smedinghoff, "Digital Signatures: The Key to Electronic Commerce," Paper Presented at conference: The Emerging Law of CyberBanking and Electronic Commerce, (Washington, DC Feb. 6-7, 1997) 24-25. Similarly, a repository of public keys is essential so that a party can confirm a public key and determine whether they can rely upon a digital signature. ABA Guidelines, supra, 16; Working Group on Electronic Commerce, United Nations Commission on International Trade, "Planning of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues" UN Doc. A/CN.71 (Dec. 31, 1996) 12. Thus, repository services are essentially part of the digital signature certification authority activity. Likewise, the proposal by the Company to sell equipment that can be used only in connection with the Company's certification authority and repository services and other digital signature or data security systems is part of the CA activity and, thus, part of the business of banking. The hardware would constitute "specialized hardware" and not "general purpose hardware." See Interpretive Letter No. 345, supra.

> Nearly all bank branches have at least one notary, and many banks advertise their notary services. … Notaries in banks most frequently notarize documents signed by the banks' customers in connection with the customer's banking transactions. In our experience, many banks will also provide, upon request, notary services for non-customers and for non-banking documents.

Id.[23]

The role of the notary is to verify signatures and, thus, requires, among other things, that the notary verify the identity of the signer. Letter of Lisa Fisher, supra. In witnessing or attesting to a signature, a notary must determine either from personal knowledge or satisfactory evidence the identity of the person appearing before the officer or named therein. Uniform Law on Notarial Acts, Sec. 2, 14 West Uniform Laws Annot. 129. Thus, the root activity of the notarization process is verifying the identity of the signing party so as to be able to authenticate the document.

The functional similarities between a notary public and a CA are clear. ABA Guidelines, supra, 54. In both instances, the bank verifies identity and provides a basis for authenticating a signature (or its digital equivalent) based either upon (1) personal knowledge of the party signing or (2) satisfactory evidence that the signature is of the party to whom it is attributed. The main difference is in the technology used. However, "the fact that modern … technology has given these services a different appearance cannot alter the permissibility of their performance by national banks." Unpublished letter by Peter Liebesman dated December 22, 1982.[24]

The certification authority activity also has marked functional similarities to another established banking service: a letter of reference or introduction. National banks and other financial institutions have long performed the function of identifying customers and parties to third parties through the issuance of letters of introduction or letters of reference. See McLeod v. Fourth National Bank of St. Louis, 122 U.S. 528, 534 (1887) and Wallace v. Ohio Valley Bank, 2 F.2d 53, 54 (4th Cir. 1924). OCC recognizes that national banks engage in this activity as part of their banking business. See Interpretive Letter No. 610, reprinted in [1992-1993 Transfer Binder] CCH Fed. Banking L. R. 83,448 (Oct. 8, 1992) and Unpublished letter from James Kane dated October 24, 1985.

---

[23] Indeed, some primitive banks of deposit were notaries who kept accurate records of business transactions. Abbott P. Usher, "The Origins of Banking: The Primitive Bank of Deposit, 1200-1600," collected in Enterprise and Secular Change: Readings in Economic History (1953) at pp. 273-74.

[24] See also, Interpretive Letter 742, reprinted in [Current Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81-106 (Aug. 19, 1996) (referring to OCC Interpretive Ruling codified at 12 C.F.R. § 7.1019 authorizing national banks to "perform, provide, or deliver through electronic means and facilities any activity, function, product, or service that it is otherwise authorized to perform, provide or deliver").

As with notary services, the functional similarity between a digital signature certificate and a letter of reference is clear and has been noted:

> Cryptographic signatures are also used to create "letters of reference" (cryptographic certificates) that allow a public verification key to be used to verify the signer's signature. *** Since the signer computes his or her signature on a document using a private key, and since the verifier verifies the signer's signature using the signer's public key, there must be a way for the verifier to trust that association between the signer … and the public key used to verify the signer's signature…. The signer can expedite the establishment of trust by enclosing with the signed check a "letter of reference" (cryptographic certificate) stating the signer's name, account number and the signer's public signature verification key, all signed by the bank holding the account.

J. Doggett, "Electronic Checks - A Detailed Preview" 18 Journal of Retail Banking Services 8 (Summer 1996).

2. CA activity is a logical outgrowth of core bank competencies.

CA activities are not only functionally equivalent to recognized banking services, they are also a logical outgrowth of such services. Among other things, the "logical outgrowth" test recognizes that the "business of banking" is defined not only by the services and products that banks provide, but also by the core competencies that banks use to produce them. The OCC has said:

> The functional equivalence and logical outgrowth lines of analysis which the courts have applied to current banking functions in the process of reviewing new activities of national banks can be multi-dimensional -- the equivalence or outgrowth can involve both evolutionary advances in products and services *as well as the integration of adjacent types of businesses that are useful to perform and deliver modern forms of banking and financial transactions*.

OCC Conditional Approval Letter No. 220 (dated Dec. 2, 1996) (to be published).

Clearly, "the business of banking is not static…." New York State Ass'n of Life Underwriters v. New York State Banking Department, 632 N.E.2d 876, 880 (N.Y. 1994). OCC recognizes that the evolution of "business of banking" is not restricted to lines of business reflecting only products banks have sold or functions banks have served previously. Rather, the "business of banking" must be -- and is -- sufficiently flexible to enable banks to develop and exploit their unique core competencies and optimize the return on those competencies by marketing products and services reflecting or using those competencies. Today, banks face a rapidly changing market that demands rapidly evolving skills. Thus, it is vital that they be able to plan strategically and adapt and respond appropriately. As one authority has said:

> The essential skill in strategic planning in a changing market, technological and competitive environment is two-fold: (1) to identify the firm's core competencies (how it can add value), and (2) to identify which markets these core competencies can serve with comparative advantage.[25]

The concept that the "business of banking" can evolve to reflect logical outgrowths from the special skills, expertise, and competencies of banks is not new.[26] In discussing the scope of permissible national bank powers, courts have considered whether proposed activities use expertise special to banks. See, Norwest Bank v. Sween Corp., 118 F.3d 1255, 1260 (8th Cir. 1997). The OCC has used a similar analysis. For example, the OCC concluded that reinsurance arrangements are a logical outgrowth of established banking activities because those activities involve the exercise of the same core competencies as credit origination. Specifically, the OCC said:

---

[25] Llewellyn, Banking in the 21st Century: The Transformation of an Industry, (paper presented at the 49th International Banking Summer School, Sorrento, June 1996) at 2-3. The flexibility of the "business of banking" to reflect logical outgrowths of core competencies, as well as established functions, is essential because the core competencies that banks use to perform their functions (both old and new) continue to evolve. For example, as Federal Reserve Board Chairman Alan Greenspan has noted:

> Banks still perform [their traditional intermediation] functions. But today we are increasingly recognizing that banking also involves understanding, processing, and using massive amounts of information regarding the credit risks, market risks, and other risks inherent in a vast array of products and services, many of which do not involve traditional lending, deposit taking, or payments services. Today, banks can be said to be part of a technological revolution in risk information processing. Moreover, risk information processing --defined broadly to include the measurement, management, and taking of risk-- can be said to have remained the basic business of banking. A crucial difference between the banks of today and those of our traditions, however, is that risk information processing now lies more visibly closer to the core of the banking business because of the blossoming of new financial products and services that rely so critically on fast and high quality risk information and risk analysis.

Alan Greenspan, "Optimal Bank Supervision in a Changing World," speech delivered at the 30th Annual Conference on Bank Structure and Competition, May 1994, reprinted in The Declining(?) Role of Banking, (Federal Reserve Bank of Chicago).

[26] Historical experience indicates that some important institutional features and functions of the current banking system reflect a logical evolutionary process. Specifically, some banking services and functions evolved as logical outgrowths of core competencies, possessed by banks or proto-banks, that were applied in new ways to satisfy demands in the marketplace for new functions or services. See, e.g., George Selgin and Lawrence White, "The Evolution of a Free Banking System," 25 Economic Inquiry 439 (July 1987). For example, money changers and bill brokers in twelfth century Genoa and at medieval trade fairs in Champagne mark the earliest recorded forms of banks providing transfer banking functions and these functions grew out of the core competence of reliable account-keeping demonstrated in the money changing function. Id. at 442. Similarly, the well know story of the origins of goldsmith banking in seventeenth century England illustrates how money-transfer functions for those specific proto-banks developed from their core competence of safekeeping. Id. at 442-43. See also, Edwin Green, Banking: An Illustrated History (1989) at 36-37 and 44-45. Cf. Oulton v. German Sav. & L. Soc., 84 U.S. 109, 118-19 (1873).

> Through the reinsurance vehicle, the Bank is engaged in credit judgements and assumes credit risks comparable to those involved in making … mortgage loans without mortgage reinsurance. With both arrangements, the Bank's decision to accept these credit risks are determined by the Bank's underwriting standards, which are derived from the Bank's lending experience and expertise.

Interpretive Letter No.743, reprinted in [1996-97 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 81-108 (Oct. 17, 1996). See also, Interpretive Letter No. 494, reprinted in [1989-90 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 83,083 (Dec. 20, 1989) (national bank may offer futures and options brokerage services because, inter alia, those services involve skills within the core expertise of banks).

Turning now to certification authority activities, undoubtedly one of the core competencies of banks is verification of identity and the authentication of transactions based upon that verification. Beginning with the Bank of the United States, the role of banks in identifying customers and parties to financial transactions has been central in conducting the business of banking.[27] In conducting their most basic banking transactions (e.g., opening a deposit accounts, cashing checks, or lending money), national banks undertake to identify the parties who seek to participate in such transactions.[28]

These identification skills extend to bank interactions with both customers and non-customers. For example, banks commonly must verify the identity of non-customers who come to the

---

[27] As early as the formation of the Second National Bank, Congress recognized the essential role of the Bank of the United States in identifying persons transacting business with the Bank. Among the rules of the Bank of the United States, Article VIII provided that the Bank was required to maintain a Book of Signatures for the purpose of facilitating customers' transactions with the Bank. Senate Document No. 571, 61st Cong., 2d Sess., National Monetary Commission, reprinted in John Thom Hodsworth and Davis R. Dewey, THE FIRST AND SECOND BANKS OF THE UNITED STATES (1910) 283. The Book of Signatures was used to identify the responsible names in connection with deposit accounts, bills and notes discounted by the Bank.

[28] The practice of national banks requiring customers opening accounts to provide identification, including their signature (and in some cases a finger print or other biometrical data), continues in order to assist in the identification of account owners and to otherwise facilitate the negotiation of banking business. National banks identify customer accounts and the authenticity of signatures on checks drawn on such accounts, by comparisons of signatures on account signature cards. Under Article 3 of the Uniform Commercial Code, a drawee bank is held to knowledge of the drawer's signature and, thus, is generally liable to the drawer if the bank pays a check bearing a forged signature. 6 Weisblatt, BANKING LAW, §127.03. Similarly, Articles 3 and 4 of the Uniform Commercial Code provide that transferors of checks and other instruments must absolutely warrant that all signatures on negotiated instruments presented for payment are genuine and authorized. Id. § 126.11 (1997). Many other laws and regulations require that banks verify customer identities. See, e.g., 31 U.S.C. 5325, 12 C.F.R. 103.28, and 12 C.F.R. 330.7.

bank to cash checks;[29] non-customers cashing checks represents about 3% of total teller transactions.[30]

Banks have extended this identity verification and authentication competence into the electronic realm. They have developed and managed systems to verify the identity of customers communicating with banks via electronic means such as automated teller machines and personal computer home banking. Most of these systems use appropriately managed and controlled PINs as a substitute for manual signatures.

National banks' identification and verification competence has been relied upon by other businesses. In addition to the notary services and letters of reference, discussed above, banks provide check and credit card verification services,[31] letter or credit advising services[32] and signature guarantees[33] among other identity verification services.

---

[29] "Banks Make Check Cashing Work," 85 ABA Banking J. 51 (Dec. 1993).

[30] M. Singletary, "Giving a Hand to Cash a Check", Washington Post, April 3, 1997.

[31] OCC has long held check verification and check guaranty services are permissible activities for national banks. Unpublished letter from Peter Liebesman dated March 26, 1982; Unpublished letter from C. Westbrook Murphy dated June 15, 1976; and Unpublished letter from John E. Shockey dated June 7, 1976.

[32] A. Cardinale, "Death of the 'Old' Advising Bank: How Technology is Taking Over," The American Banker/Management Strategies December, 1997.

[33] A signature guarantee by a securities transfer agent is similar to a notary's attestation to the authenticity of a signature on a document. A signature guarantee is a warranty that, at the time of signing, the signature is genuine; the signer is an appropriate person to endorse or originate an instruction to transfer, pledge or release a security; and the signer has legal capacity to sign. U.C.C. § 8-312(1), (2) (1977). The OCC has long held that national banks may issue signature guarantees. OCC Digest of Opinions ¶ 230 (1960). See also, Unpublished letter from William B. Glidden dated December 5, 1985 and Unpublished letter from Donald Lamson dated August 3, 1993.

The issuance of digital signature certificates would not involve the types of broader performance-type guarantees that have been deemed impermissible activities for national banks. See Bowen v. Needles Nat'l Bank, 94 F. 925 (9th Cir.1889 and Border Nat'l Bank v. American Nat'l Bank, 282 F. 273 (5th Cir. 1922), cert. denied, 260 U.S. 701 (1922). Typically, in these prohibited guarantee cases, a "guarantee" is a promise to answer for the payment of some debt or the performance of some obligation in the case of default by another party that is primarily liable for such payment of performance. Border v. American Nat'l Bank, supra, 282 F. at 277-78. However, a bank acting as a certification authority does not covenant to be secondarily liable if a subscribing party default upon their performance obligation. Indeed, a CA does not assume liability for transactions using digital signatures. Rather, the CA generally functions like a notary. A notary's certificate cannot be deemed to certify or guarantee the facts stated in the instrument to which it is attached. 58 Am Jur 2d, Notaries Public, §§ 45 and 75. Moreover, the notary is not a guarantor or insurer. Id. § 58. Thus, the CA does not commit to perform the obligation of the subscriber. Nor does the CA guarantee or underwrite the factual accuracy or legal significance of the information that it confirms in issuing a certificate. ABA Guidelines, supra 34. In this regard, the OCC has distinguished instances where a national bank warrants a party's identity from guarantees. Unpublished letter from William B. Glidden dated

Thus, in carrying out banking functions involving customers and other parties, national banks have developed special identification and authentication competencies. Digital signature certification authority competencies are a logical outgrowth of these identity verification competencies of banks. Certification authority services for digital signatures may be analogized to current and historic identification services used by banks, including the use or provision of signature cards, letters of introduction, notary services, signature guarantees, and check and credit card verifications involving PIN technology.[34] Certification authority activities are, thus, part of the business of banking.

3. Key escrow services are the functional equivalent of bank safekeeping services.

In addition to and separate from its certification authority activities, the Company proposes to provide a service escrowing encryption keys. This activity is part of the business of banking. Banks have traditionally performed the function of keeping safe valuable or confidential items for their customers. For example, national banks, as part of the business of banking, provide safe deposit services. *Colorado Nat'l Bank v. Bedford*, 310 U.S. 41 (1949); *Bank of California v. Portland*, 69 P.2d 273 (Ore. 1937). The key escrow service proposed by the Company is a functional equivalent to this recognized safekeeping service, although it uses electronic technology suitable to the digital nature of the item to be kept safe. 12 C.F.R. 7.1019.

4. Acting as CAs will convey significant benefits to banks and their customers.

The ability of banks to act as certificate authorities for digital signatures is expected to be vital to their role in the evolving electronic payments systems. For example, the Secure Electronic Transaction ("SET") protocol, developed by MasterCard and Visa to permit secure use of credit cards over the Internet, contemplates that participating banks or bank controlled entities,

---

December 5, 1985.

[34] Thus, given this special competency in identify verification and authentication, it is not surprising that a number of authorities have noted that banks have special competencies and skills that uniquely qualify them to conduct certification authority activities. As one authority has observed:

> New payment modes may also enable banks to redefine their relationships with their customers. … Other opportunities include becoming a trusted central repositories (sic) to hold encryption and encryption keys to authenticate electronic transactions for electronic information exchange and access. Banks may be uniquely well positioned for roles such as these that are logical extensions of the current franchise.

Bank Administration Institute/Boston Consulting Group, The Information Superhighway and Retail Banking, Volume II, 36 (1995).

among others, will issue digital certificates to participating entities.[35] As noted by one authority:

> Many credit card companies or banks are going to set up their own hierarchical networks [of digital signature certificates] because they need specific guarantees of identity to satisfy their models of risk. * * * The leaders are the banks. They recognize that Internet commerce demands a way for people to check the authenticity of documents like checks or credit card authorizations. The SET protocol endorsed by Visa and MasterCard is one of the most sophisticated uses of digital signatures, and these companies plan to make it a standard part of electronic commerce.[36]

Likewise, while the "electronic check" is still under development,[37] some form of electronic authentication system will be needed for the electronic checking system and a bank-based system of digital signature certificates could provide an essential foundation.[38] Similarly, digital signatures could be used to authenticate letters of credit.[39] Finally, it has been observed that "financial institutions are considering use of digital certificates for Internet-based cash management systems, remote banking and other transactions where a remote client needs to be authenticated by a server."[40]

---

[35] "Wells Fargo to Certify Net Payments -- Bank Will Provide Credit-card Verification of Merchants Collecting Via the Internet", Information Week, December 16, 1996. See generally, the SET specifications at WWW.Visa.com/cgi/nt/ecomm/set/downloads.html. See also, J. Kutler, "SET Is Nearly Ready to Go, But Will It Ignite the Marketplace", The American Banker, September 22, 1997 and B. Tracey, "Bankers Striving to Find Way to Cope with On-Line Consumer Identity Crisis", The American Banker, February 25, 1997.

[36] P. Wayner, "Who Goes There?", Byte, June, 1997, at 73-80.

[37] "Pilot Tests of Electronic Checks Being Developed by FSTC Should Start Mid-Year", BNA's Banking Report, February 10, 1997 ("The project uses public key cryptography to allow an individual to electronically issue and digitally sign a payment instruction, such as a check, and to transmit it over public networks, where it can be verified by the recipient as being a legitimate authorization from an authentic account."); Matt Barthel, "BankBoston, NationsBank Prepare for Internet Card Test," The American Banker (Oct. 10, 1997).

[38] As one authority has observed:

> The electronic check is modeled on the paper check, except that it is initiated electronically, and uses a smart card as an electronic check-book, a tamper-proof electronic document for the check, digital signatures for signing and endorsing, and digital signatures to authenticate the payer, the payer's bank and the bank account.

J. Doggett, supra, 3.

[39] A. Cardinale, supra.

[40] Ira Parker, "Securing the World of Electronic Banking and Commerce", Electronic Banking Law and Commerce Report, March, 1997 4. See also, Alan Asay, "Banking Prospects for Digital Signature Technology"

Thus, we agree with the Bank that the banking industry and its customers would benefit from the ability of a bank (or bank controlled entity) to act as certification authority and key escrow. Among other things, a bank entity will uniquely understand (and thus will be likely to provide) the level of service and security appropriate for banking functions.[41]

5. CA and key escrow activities present risks similar to recognized banking activities.

As established above, the activities as a certification authority would involve core competencies of national banks and thus would expose them to risks similar to those that banks are already expert in handling. Clearly, there are new risks that arise from a new use of technology. Nevertheless, the risks of the functions performed via the new technology are comparable to risks with which banks are already familiar. "[B]anks in recent years have developed expertise in safeguarding their own encryption keys…"[42] See also, the discussion of the Company's risk controls supra at pp. 6-9.

6. CA and key escrow activities do not require trust powers under 12 U.S.C. 92a.

The OCC requires that national banks exercising "fiduciary powers" obtain prior approval under 12 U.S.C. § 92. 12 C.F.R. § 5.26. Under OCC regulations, the definition of "fiduciary capacity" includes acting as a trustee, executor, administrator, registrar of stocks and bonds, transfer agent, guardian, assignee, receiver, custodian under a uniform gifts to minors act, or investment adviser, as well as activities involving the exercise of investment discretion. 12 C.F.R. § 9.2(e). For the reasons below, digital signature certification authority and key escrow services do not require trust powers under Section 92a because those activities are not fiduciary activities covered by Part 9.[43]

As noted, certification authority activities are the functional equivalent of recognized identify verification and authentication services provided by banks. The OCC made clear in its revision of Part 9 that "acting in a fiduciary capacity" included only those activities enumerated in Part 9,

---

Electronic Banking Law and Commerce Report, May, 1996 13.

[41] Thus, at least one bank has implemented a digital signature system in which it acts as its own certification authority. See, Wendy Mead, "Morgan Adopts Strong Encryption for Customers", The American Banker 8 (June 2, 1997).

[42] T. Clocker, "Code Export Policy Presents Opportunities", The American Banker, February 14, 1997.

[43] The Bank has committed and agreed that the Bank and the Company will not indicate in any marketing of the Company or its products or services that (1) the OCC has approved or endorsed the security, functionality, or effectiveness of the Company's products or services, (2) the Company is a trust company chartered by the OCC, or (3) the Company's products or services warrant special trust or confidence due to the fiduciary powers of the Bank under 12 U.S.C. § 92a.

activities involving the exercise of investment discretion, or any other similar capacity authorized by the OCC pursuant to section 92a. 61 Fed. Reg. 68,543, 68,545 (1996). A certification authority is not acting in one of the roles listed in Part 9 -- trustee, executor, administrator, registrar of stocks and bonds, or guardian of estates -- nor does it exercise investment discretion or act in any other similar capacity. Instead, a certification authority provides services for which the OCC previously has not required trust powers. For example, the OCC has not required banks to obtain trust powers to offer notary public services.

Similarly, key escrow services, even though arguably involving a fiduciary relationship, are the functional equivalent of activities for which OCC has not required trust powers. The revised Part 9 does not address explicitly the status of escrow services or whether they constitute an activity that requires trust powers. Nevertheless, the OCC has concluded that national banks do not need trust powers to offer escrow and other safekeeping services, stating that "[agency services arrangements that do not involve the exercise of discretion or similar fiduciary responsibilities, such as escrow, safekeeping and custody, may be performed by a bank under the incidental powers of banking without having trust powers." Comptroller's Handbook for Fiduciary Activities ¶ 9.2600.

Even if the provision of safekeeping services creates a fiduciary relationship under state law, it does not require a grant of trust powers. OCC regulations and precedent recognize the distinction between being a fiduciary and engaging in an activity requiring trust powers. See 12 C.F.R. § 9.2(e).[44]

C. Conclusion

On the basis of the Bank's representations and commitments in its application and other communications with OCC, and subject to the conditions set forth below, the Bank's application to establish and operate the Company is hereby approved.

---

[44] Parties can assume fiduciary duties through contract in the absence of a traditional trust or trust relationship. Fratcher, I SCOTT ON TRUSTS § 2.5 (4th Ed.) (1987). Fiduciary duties that one party can owe another outside a trust relationship include the duty of loyalty (administration or conduct solely in the interest of a beneficiary) and the duty of care (acting as a person of ordinary prudence would in dealing with his/her own property). Id. at §§ 170 and 174. However, digital certificate certification services are not "fiduciary" in nature and, thus, generally the CA is not a fiduciary. See ABA Guidelines, supra, 62. The degree of care required is ordinary care rather than the higher level expected of fiduciaries. Cf. Id. at 77.

In contrast, the key escrow service would likely be held to give rise to a fiduciary relationship for purposes of state law. See Id. at 25-26. Thus, the proposed operating subsidiary likely would have to exercise care in protecting the integrity and confidentiality of such keys and the standard of such care would be grounded in fiduciary law, since customers would be giving control of property to the operating subsidiary that, if stolen, misused, or compromised, could cause financial losses and raise doubts about the security of data. See SCOTT ON TRUSTS, supra, at § 174.

The following supervisory conditions are conditions imposed in writing by the agency in connection with the granting of any application or other request within the meaning of 12 U.S.C. § 1818:

1. Prior to commencing service operations, the Company will submit to OCC a complete description of the Company's information systems and back office operations architecture. This description should include the following items: proposed third party software and vendor services to be used; operating processes; security controls; internal controls; and internal audit plans.

2. The Company shall notify all potential vendors in writing of the OCC's examination and regulatory authority under 12 U.S.C. § 1867(c) and all vendor contracts shall stipulate that the performance of the services provided by the vendors to the Company is subject to the OCC's examination and regulatory authority.

Please fell free to contact John Graetz, Licensing Expert, at (202) 874-5060 if you have any further questions.

Sincerely,

Julie L. Williams
Chief Counsel