Comptroller of the Currency
Administrator of National Banks

Washington, DC 20219

Conditional Approval #479
September 2001

July 27, 2001

Mr. A. Scott Anderson
President & CEO
Zions First National Bank
One South Main
Salt Lake City, UT 84111

Dear Mr. Anderson:

Zions First National Bank (the "Bank") has filed an application under 12 C.F.R. § 5.34 to establish an operating subsidiary that will provide an integrated, online information service for secure web-based document storage, retrieval and collaboration of documents and/or files containing personal information or valuable confidential trade or business information. The proposed subsidiary will be named EnterVault, Inc. (the "Company"), and will have its primary headquarters in Salt Lake City, Utah. Based upon the commitments and representations in the Bank's application and other materials, the establishment and operation of the Company is approved, subject to the conditions set forth herein.

A. Background

Initially and as approved, the Company will have two main lines of business: (1) Personal Vault and (2) Business Vault; the former will store electronic data for retail customers for their personal uses, the latter for businesses. For both, all data will be stored in the Bank's Data Center and will be accessible by the customer via the Internet or through a dedicated line.[1] For both, the stored data will be encrypted. Although all data will be encrypted, the customer will have a choice of access features. Initially, the customer will have the alternative of selecting either a basic security level composed of a user ID and a Password or an access level using a Digital Certificate to which the client will have the only "passkey."[2] Except for storage, access,

[1] See discussion in section 3 ("Technical Operations") *infra*.

[2] At the most secure level, access will require use of both the digital certificate and of a password known only to the customer. EnterVault is developing, in partnership with Digital Signature Trust Company ("DSCo"), an application that will automatically store a document into the customer's Vault when a digital signature is applied. DSCo is also a subsidiary of the Bank. The Company is also developing a biometric access feature that it intends to make available in the future. Through the customer agreement, the Company has reserved authority to access the content under certain limited circumstances, *e.g.*, in response to a court order or other legal or regulatory process.

and retrieval, the Company will not process or manipulate the information stored in an electronic vault.

1. Personal Vault

Personal Vault will be a secure repository aimed at individuals wishing to store personal documents and files in digital form. The types of electronic documents and files that individual users are likely to store in their Personal Vault are comparable to those they would store in their physical safe deposit box: personal financial data, important documents (both electronic and scanned "analog" files) such as wills, trusts, birth, wedding and death certificates, deeds of trust, insurance policies, tax returns, etc., as well as personal "keepsake" documents such as children's drawings, report cards, and photos. Customers may also store important data files, such as system backups, applications, or databases. In order to verify this characteristic of a customer's intended use of their Personal Vault, customer agreements with the Company will state that their use of the Vault will be for their personal purposes.

The proposed service will make these electronic documents accessible and reproducible when needed. However, users must agree not to download or store any file, document, or information that will result in a violation of any law, rule, or regulation.

[

].

2. Business Vault

Business Vault is designed to meet the financial and business data storage needs of businesses. Business Vault will allow businesses to store digital copies of valuable trade or business information and documents and to access such digital documents through the Internet or dedicated line. The Company will target several types of business-related data and documents, including customer banking, tax and financial records, customer account and economic information, contracts and legal documents, and other business records.

Business Vault will also offer its business clients electronic storage for mission-critical business software, making the stored software available online for business restoration through the Internet.[3] Only the client will have access to the encrypted contents of the Business Vault with proper authentication to access and recover software and data.

Thus, Business Vault will enable business clients, in the event of a disaster, to retrieve and restore the mission critical data and software for their business immediately through the Internet

[3] While some firms use "off the shelf" software to run their businesses, many firms have modified their software extensively with macros and other unique features. These modifications would need to be re-created when recovering from a disaster if the software was not backed-up.

or dedicated line.[4] Likewise, should the client's active files become compromised or corrupted, those files can be restored from back-up data maintained in the Business Vault. [

].

[

].

Users will represent in their agreements with the Company that their use of the vault will be to store valuable or confidential information relating or useful to their business. Business Vault users must also agree not to download or store any file, document or information that will result in a violation of any law, rule or regulation.

3. Technical Operations

The EnterVault technical infrastructure is comprised of one logical system and two physical environments.[5] The physical environments include the electronic document storage environment and a web server environment. The EnterVault technologies are separated and self-contained from the Bank's environment. The main system will be housed at Zions Management Services (ZMS) Data Center in Salt Lake City. The web servers and other storage drives have built-in redundancy to reduce risk of data loss and down time. Additionally, the Company will implement a real time, offsite back-up site. The back-up site will allow for recovery of customer records and Enter Vault systems in the event the data center in Salt Lake City is unavailable for an unacceptable period of time. The back-up site is configured to become a hot site when subscriber volume dictates that a hot site is required.[6] The system has been designed to exceed the maximum expected user loads.[7]

---

[4] [

].

[5] A "physical environment" is the actual physical location where the processing operations take place. More than one "environment" can be in a single physical location.

[6] A "hot site" is an alternative location that can become fully operational for processing should the primary processing site become unavailable. Usually the hot site will have identical hardware and software available for immediate use to continue normal business operations.

[7] The technical team worked with Novel, NetDocuments, Oracle, and Microsoft to determine the high-end capacity and develop benchmarks for the designed system. EnterVault is designing the system to concurrent customer connection volume that far exceeds their business expectations. OCC expects that the Company will ensure that its systems will be designed with adequate transaction and communication capacity to meet reasonably anticipated customer access demands.

All Enter Vault functions are accessed by the customer through a standard Internet browser. **[**

]. This application includes the security level selected by the customer (including a Digital Certificate from DSCo where that option is selected) and a small application that allows automated storage of the customer's qualified applications.

4. Risk Controls

The Company will address its major sources of risk, notably those relating to the operation of a electronic storage service as well as remote customer verification, authentication, and transaction authorization that are necessary for the operation of this service as an electronic business line. If a customer selects an ID and password without a digital certificate, possession of the password will act as authorization to access the vaults. Digital certificate customers will be authenticated using the certificate as well as a password.

For providing a safe and sound electronic safety deposit box service the Company will develop proper internal controls, operating procedures and safeguards, and audit coverage. The Company assumes the responsibility of exercising reasonable care and precaution against the loss of the stored information. Thus, the Company will create an appropriate disaster recovery plan that provides for sufficient recovery of the electronic contents stored.[8] Typically heavy volume and record keeping nature of the EnterVault activities will expose the Company primarily to transaction risk. To effectively manage this risk, the Company has represented that it will have controls and systems in place to ensure the accuracy of their own recordkeeping and the integrity of electronic records stored.[9]

To operate a safe and sound service with adequate customer identification, authentication, and transaction authorization, the Company will implement a range of measures designed to mitigate and control risks. The Business Vault setup will include appropriate policies and procedures designed to limit transaction and reputation risk. For the Personal Vault Service, the Company will establish an appropriate privacy policy in accord with the Standard Bank Policy and security program to ensure compliance with the requirements of §501(b) of the Gramm-Leach-Bliley Act (effective July 1, 2001).[10]

---

[8] See footnote 6 and accompanying text.

[9] For example, if a digital certificate is compromised or becomes unavailable, the customer will be required to call the company's customer support and go through the certificate revocation and certificate issuance process to regain access to their data.

[10] Prior to implementing the Vault Service, the Company will be required to have a risk assessment plan and appropriate risk mitigation controls that shall be approved by OCC. In designing this plan, the Bank should consider the new *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, 12 C.F.R. § 30, 66 Fed. Reg. 8616 (February 1, 2001). Upon implementation, management should evaluate the impact on security risks posed by introducing any additional technology-intensive product, service, or activity. Management should determine whether the security program in place remains adequate in light of any additional or modified risk

To ensure the safe and sound operations in general, the Company will arrange to have independent security testing at appropriate intervals, including before beginning operations. The independent testing will incorporate all systems used for the EnterVault Service, including those that are provided to the Company by affiliated and unaffiliated third parties.

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 include in its User Agreement an express and detailed limitation on the Company's liability for claims arising out of the agreement. The User Agreement also contains specific provisions stating the terms and conditions upon which the Company may access a customer's electronic vault, covering such contingencies as customer death, court order, regulatory process, and termination of the Agreement.

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.

5. OCC Supervision

As an operating subsidiary, the Company will be subject to OCC examination and supervision. 12 C.F.R. ' 5.34(e)(3). As part of the application process, OCC examiners evaluated and assessed the Company's proposed activities and the OCC supervision necessary for 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 technology regularly met with key employees of each of these entities to discuss their plans and monitor project management. OCC also conducted an onsite examination of the Bank and its data processing facilities. Included in the scope of that review was a thorough examination of the EnterVault projects with the objective of enhancing the OCC's familiarity with the proposed activity and identifying risks to the bank in implementing this business.[11]

Going forward, the OCC will continue to monitor specific operations at the Company and developments in the industry as banks develop more products and services that allow for the

---

exposure. The Company should then adjust the security program as necessary before introducing the new technology-intensive product, service, or other activity.

[11] *See* FFIEC Policy Statement, 11/28/2000, *Risk Management of Outsourcing Technology,* published as OCC Advisory Letter 2000-12, for a complete description of issues and risks of using third parties for providing technology services to banks. *See also* OCC Bulletin 99-20, *Certification Authority Systems,* for an explanation of the risks of issuing and managing digital certificates. 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 OCC has approved or endorsed the security, functionality or effectiveness of the Company's products or services.

storage and retrieval of electronic documents for themselves and their customers. 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 technology. 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 the mechanisms the Company will use to manage those risks, including a description of proposed controls. As required by a condition to this letter, the Company will have in place a risk management plan approved by the OCC prior to beginning operations. The OCC expects the Company to maintain an adequate level of capital and liquidity based upon, among other factors, the level of operations of the Company, the level of risk in those operations, and the working capital and liquidity needs of the Company. The OCC will evaluate the adequacy of such capital and liquidity as part of its on-going supervision of the Company

B. Discussion

A national bank may engage in activities that are part of, or incidental to, the business of banking by means of an operating subsidiary. 12 C.F.R. § 5.34. 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 . . . .

The Supreme Court has held that this powers clause of 12 U.S.C. ' 24(Seventh) is a broad grant of power to engage in the business of banking, which is not limited to the five enumerated powers. Further, national banks are authorized to engage in an activity if it is incidental to the performance of the enumerated powers in § 24(Seventh) *or* if it is incidental to the performance of an activity that is part of the business of banking.[12] Since national banks must be able to make use of modern technology in performing their business, the OCC=s Interpretive Ruling 7.1019 permits national banks to Aperform, provide, or deliver through electronic means and facilities any activity, function, product, or service that [they are] otherwise authorized to perform, provide, or deliver."[13]

---

[12] *NationsBank of North Carolina, N.A. v. Variable Annuity Life Ins. Co.,* 513 U.S. 215 (1995).

[13] 12 C.F.R. § 7.1019.

For the reasons below, the proposed activities of the Company are part of the business of banking because they involve the use of modern technology to perform the established banking function of safekeeping. Accordingly, the activities are permissible for a national bank and for its operating subsidiary.

1. Safekeeping Activities of National Banks

The safekeeping functions of national banks are long established and extensively recognized. Among these are the powers of special deposit and rental of safe deposit boxes. The OCC has said of the special deposit authority:

> The safekeeping of valuable personal property is a traditional function that banks have performed since the earliest times: "Originally the business of banking consisted only in receiving deposits, such as bullion, plate and the like for safe-keeping until the depositor should see fit to draw it out for use. . . ." Oulton v. German Savings and Loan Society, 84 U.S. (17 Wall.) 109, 118 (1872); see also Bank of California v. City of Portland, 157 Ore. 203, 69 P.2d 273 (1937). [Among these is the power to hold property] as special deposits, which have been defined as deposits for safekeeping in which the depositor is entitled to the return of the identical money or thing deposited. Unlike a general deposit, which creates a debtor-creditor relationship, in a special deposit the bank is a bailee for the depositor, and merely assumes charge or custody of the special deposit without authority to use it. Tuckerman v. Mearns, 262 F. 607 (D.C. Cir. 1919); Bank of California v. City of Portland, supra. Special deposits may be money, securities, or other valuables. See First National Bank v. Graham, 100 U.S. 699 (1880). See generally 5B Michie on Banks and Banking § 328 (1983).

Unpublished letter from Chris Manthey (June 26, 1991). *See also*, *Comptroller's Handbook: Consigned Items and Other Customer Services* (June 1996) (in addition to safe deposit services, national banks have historically engaged in a range of customer safekeeping activities).

The Supreme Court has acknowledged the ability of national banks to receive special deposits. *Colorado National Bank v. Bedford*, 310 U.S. 41 (1940); *First National Bank v. Graham, supra*. Indeed, the authority of national banks to engage in the business of accepting special deposits was expressly recognized in former 12 U.S.C. § 133 (since repealed by Public Law 103-325, Title VI Sec. 602(e)(16)) that prohibited national banks from continuing the business of banking after default except "to receive and safely keep money belonging to it, and to deliver special deposits."

Moreover, the safekeeping or special deposit function "differs little if at all from a safe-deposit business," which the Court found to be a function authorized by Congress as part of the business of banking. *Colorado National Bank v. Bedford*, *supra*, 310 U.S. at 49-50.[14] The safe deposit box

[14] The United States Supreme Court held that the safe deposit business was within the business of banking based on the Court's finding that "national banks do and for many years have carried on a safe deposit business." Under 12 U.S.C. § 24(Seventh), a national bank's investment in the stock of a safe deposit business is restricted to an amount equal to 15 percent of the capital stock of the bank and 15 percent of the bank's unimpaired surplus. However, this

business involves renting, for remuneration, safe deposit boxes. *See* 11 AM JUR 2D *Banks and Financial Institutions* § 1012 and *Comptroller's Handbook: Consigned Items and Other Customer Services, supra*.

The scope of the special deposit authority is quite broad in its permissible objects for safekeeping. A series of cases recognize that banks may, among other things, store valuable and important papers as part of their safekeeping services. See *Young v. First National Bank of Oneida*, 265 SW 681, 682 (Tenn.1924) (bonds and other "valuable papers"); *Pennington v. Farmers and Merchants Bank*, 231 SW 545 (Tenn. 1920) (a bank may keep "valuable papers" in safekeeping); *Citizens Bank of Coldwater v. Callicott*, 174 So. 78, 78-79 (Miss. 1937) ("customary for the bank, at the request of its depositors, to take papers and other valuables of like nature for safekeeping."); *Kierce's Administrator v. Farmers Bank*, 191 SW 644, 646 (Kty. Ct. of Apps. 1917) (for the accommodation of its customers, a bank stored in its vault a box for the safekeeping of papers that the customers would place in the box); *Security National Bank v. McCutcheon*, 187 P. 697, 699 (Kan. 1920) (under its special deposit authority, a national bank could safekeep mortgage documents) and *Wood v. Home Savings Bank*, 109 NW 9 (Iowa 1906) (under its authority to accept special deposits, a bank may receive valuable papers for safekeeping).[15]

Moreover, when a bank rents safe deposit boxes, it has no control or supervision over what papers or other property may be placed in the box. *Young v. First National Bank of Oneida*, *supra*. Perhaps for this reason, the authorities are agreed that of the scope of items kept the safe-deposit boxes are extremely broad. As one has noted, "jewelry and all kinds of intangible assets are kept in boxes, including securities, bank books, business records, and other valuable papers." McBain, at p.1 (emphasis added). Likewise, the safekeeping function of banks has been said to include securities, contracts, wills, insurance policies, jewelry, plate and other valuable documents and property." Charles J. Woelfel, ENCYCLOPEDIA OF BANKING AND FINANCE (10th Ed.), (1994) at p. 1018. In addition, many state laws recognize that papers and documents can be stored as part of a permissible safekeeping activity. For example, N.Y. law provides that a bank "may receive upon deposit for safekeeping for hire money, securities, papers of any kind, and any other personal property...." New York Banking Law, § 96(3)(a)(b). See also Pennsylvania, Purdon Title 7, § 202(b) (banks have the "power to receive for safekeeping, or to rent out receptacles or safe deposit-boxes for the deposit of papers and other personal property").[16]

---

statute is merely a limitation upon investments permitted under a general authority to use "generally adopted methods of safeguarding valuables" that exists under the grant to conduct the business of banking. *Bedford*, *supra* at 50. *See also* OCC Corporate Decision No. 97-92 (October 17, 1997).

[15] In, *Myers v. Exchange National Bank,* 164 P. 244 (Wash. 1917) and *Britton v. Elk Valley Bank*, 211 NW 810 (N.D. 1926), the courts held that banks could not, under their special deposit powers, safekeep last wills and testaments. The courts in these two cases appear to have been concerned about the liability that banks might incur by storage of valuable documents. However, as discussed, the great weight of authority is to the contrary. Moreover, as discussed, banks have considerable expertise in safeguarding valuable and confidential documents and information and various means by which they can limit their potential liability in connection with those activities.

[16] The Supreme Court has expressly supported resort to state bank powers as a factor in determining the scope of permissible national bank safekeeping activities. In *Colorado National bank v. Bedford*, *supra*, the Court concluded

2. Electronic Safekeeping Activities

The proposed electronic safekeeping activities of Personal Vault and Business Vault are part of the business of banking because they are the electronic expressions of traditional safekeeping services provided by banks as described above. As one authority has observed: "Safe deposit boxes have become the latest physical-world service to be reincarnated in virtual form on the Internet." C. Power, *Safe-Deposit Services Gain Momentum on the Web*, AMERICAN BANKER, May 11, 2000. *See also* K. Gosselin, *Cybervaults: A Place to Store Valuable Documents*, THE HARTFORD COURANT, November 4, 2000, and *Net.B@nk to Offer Innovative On-line Safe Deposit Boxes,* PR NEWSWIRE, June 7, 1999.[17]

As previously noted, a national bank may use electronic means to perform services expressly or incidentally authorized to national banks.[18] An OCC Interpretive Ruling expressly authorizes a national bank 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." 61 Fed. Reg. 4849 (1996) *codified at* 12 C.F.R. § 7.1019.

OCC has recognized that national banks may conduct their safekeeping functions via electronic media. In OCC Conditional Approval 267 (January 12, 1998), OCC concluded that a national bank could escrow encryption keys used in connection with digital certificates. OCC said:

---

that national banks had the authority to conduct a safe-deposit business. As part of its analysis, the Court said: "State banks, quite usually, are given the power to conduct a safe-deposit business. We agree with the appellant bank that such a generally adopted method of safe-guarding valuable must be considered a banking function authorized by Congress." 310 U.S. at 50.

[17] There is considerable potential demand by customers for this concept. *See* K. Hoover, *Let's Invent a Cyber Safe Deposit Box to Keep Personal Information Private*, AMERICAN BANKER, August 25, 2000). Indeed, both banks and nonbanks have responded to this demand by developing and marketing such a service. *Virtual Bank Offers Information Service,* AMERICAN BANKER, March 1, 2001; *Online Safe-Deposit Boxes to Save Customers Trips to the Bank*, PR NEWSWIRE January 30, 2001; C. Power, *Safe-Deposit Services Gain Momentum on the Web*, AMERICAN BANKER, May 11, 2000; M. Trombly, *FleetBoston Unveils Virtual Safe-Deposit Boxes*, COMPUTERWORLD, October 12, 2000; D. Kilgour, *Online Deposit Boxes Already Available, With Features Expanding Every Day*, AMERICAN BANKER, September 1, 2000. The recently enacted E-Sign Act, which provides *inter alia* that documents cannot be denied legal validity or recognition solely because they are in electronic form, will undoubtedly spur demand for this service. However, banks offering this service should consider steps to ensure that their customers know that electronically stored documents may need to meet additional requirements to ensure admissibility in court. Customers should be advised that the law on admissibility of electric documents is still developing and varies among jurisdictions and, thus, that users may wish to consult with their legal counsel on the requirements for their jurisdictions.

[18] *See, e.g.,* OCC Conditional Approval No. 289 (October 2, 1998); OCC Interpretive Letter No. 677, *reprinted in* [1994-1995 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 83,625 (June 28, 1995); OCC Interpretive Letter No. 284, *reprinted in* [1983-1984 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶85,448 (Mar. 26, 1984); and OCC Interpretive Letter No. 449, *reprinted in* [1988-1989 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 85,673 (Aug. 23, 1988).

> 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.

See also, Unpublished letter from Julie Williams (October 2, 1996) (national bank may invest in the company that, among other electronic services, provided to participating consumer members "a secure electronic storage and retrieval system for legal documents and records").

Moreover, the offering of electronic safekeeping of data will expose banks to risks similar to those that banks are already expert in handling. As noted, national banks have long experience in safekeeping of physical items and documents for their customers. In that capacity, they have developed extensive procedures and regimes to handle the responsibilities and risks that arise from this bailment. *See, generally*, Ann Graham, 1 BANKING LAW, Ch. 10 (Safe Deposit Boxes); James McBain, *Safe Deposit Department*, 72 BANKING L. J. 533 (1955). Moreover, OCC has developed guidance on this activity. *Comptroller's Handbook: Consigned Items and Other Customer Services, supra*. Much of this experience, process, and guidance can and should be applied to electronic safekeeping activities. While the use of electronic media to store and access items raises additional risks, banks already have extensive expertise in dealing with these risks and OCC has provided guidance on addressing these risks.[19] In this regard, as noted above, OCC expects that banks offering this service will comply with the requirements under the new Interagency Guidelines Establishing Standards for Safeguarding Customer Information.[20]

It follows that the electronic storage of data and files for personal purposes[21] offered by the Personal Vault service is also part of the business of banking.[22] Likewise the proposed storage

---

[19] OCC Bulletin 2000-14 (*Infrastructure Threats - Intrusion Risks*) May 15, 2000; OCC Bulletin 98-3 (*Technology Risk Management*) February 4, 1998. Any bank operating electronic storage services should do so in conformance with all the OCC guidance cited in this letter and should have appropriate policies and procedures designed to limit transaction and reputation risks. For example, such banks should conform with forthcoming OCC guidance on authentication of customers in electronic financial services. These banks should also have necessary stringent controls for performing electronic safekeeping for their customers.

[20] 12 C.F.R. Part 30, 66 Fed. Reg. 8616 (February 1, 2001). Under the Guidelines, which became effective on July 1, 2001, OCC will expect national banks to make the appropriate changes to their information security programs before they offer new electronic safekeeping services.

[21] As noted, Personal Vault users will represent that their use of the vault will be for personal purposes. Thus, the Personal Vault operations do not entail either bulk warehousing operations (*See Bank of California v. City of Portland,* 157 Or. 203, 69 P.2d 273 (1937), *cert. denied*, 302 U.S. 765 (1938) or the storage of physical goods and commodities (See *American National Bank v. Adams*, 44 Okl. 129, 143 P. 508 (1915).

[22] These electronic safekeeping activities are not "fiduciary" activities within the meaning of 12 U.S.C. § 92a. Thus, no trust powers are necessary in order to conduct the activity. *See* OCC Conditional Approval No. 267, *supra* 1998) (Fiduciary powers not required for key escrow services). *See also* Letter from Richard G. Fitzgerald (July 14, 1983), *reprinted in* [1983-1984 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 85,429.

activities of Business Vault are permissible safekeeping activities because they will involve the type of information traditionally contained in "valuable" and "important" papers that banks have traditionally stored for their customers. Here, the Business Vault service will store and process predominantly valuable and/or confidential trade or business information and documents because subscribers will represent that they will use the vault to store information relating to their business.[23]

3. Additional Functionalities

The Company will offer a number of additional storage related functions to both Personal and Business Vault customers. Similar to other entities offering electronic storage,[24] the Company will offer its customers the ability to grant third parties controlled access to the stored documents and files so as to enable use of collaboration tools. However, banks have long permitted their customers to authorize access by others to the customer's safe deposit box.[25]

C. Conclusion

Based upon a review of the information the Bank provided, including representations and commitments made by the Bank's representatives, and subject to the conditions set forth below, the Bank's application to establish and operate the operating subsidiary is hereby approved subject to the following conditions:

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

---

[23] Given the nature of the business entities receiving this service, the nature of the data that they will store can be reasonably inferred. The Federal Reserve Board, in approving the acquisition of a company engaged in a variety of data processing activities for securities related customers such as exchanges and brokers, concluded that the acquisition was permissible even though the company included word processing and electronic mail components that could be used for nonfinancial applications and data. The Board found that "[b]ecause of the nature of the [company's] customers and financial orientation of the data system and software, it is likely that the customer data to be accessed will be account information or similar financial data." Citicorp, 72 Fed. Res. Bull. 497 (1986)

[24] M. Trombly, *supra*; D. Kilgour, *supra;* and K. Gooselin, *supra*.

[25] 11 AM JUR 2D *Banks and Financial Institutions* §1023 and Graham, *supra*, §10.04. However, banks doing so normally have a responsibility to investigate the authority of persons who seek entrance to a box even if they present the renter's key and many banks routinely include provisions relating to access by deputies in their safe deposit contracts. *Id.* OCC expects the Company to exercise similar controls with respect to its electronic shared access program.

2. The Bank shall develop a risk assessment plan and appropriate risk mitigation controls, which shall be approved by OCC prior to commencement of the proposed service, and these approved measures shall be implemented and continued on an ongoing basis.

Please be advised that each of the conditions of this approval are deemed to be a "condition imposed in writing by the agency in connection with the granting of any application or request" within the meaning of 12 U.S.C. § 1818.

Sincerely,

/s/

Julie L. Williams
First Senior Deputy Comptroller and
Chief Counsel