Comptroller of the Currency
Administrator of National Banks

The Internet and the National Bank Charter

January 2001

The Internet and the National Bank Charter

Entry

Comptroller's Corporate Manual

Washington, DC
January 2001

The Internet and the National Bank Charter

Table of Contents

Introduction

The Office of the Comptroller of the Currency (OCC) charters, regulates, and supervises national banks. National banks have broad authorities to engage in a wide range of financial services and activities, and recently they have been expanding their geographic reach, increasing customer convenience, and reducing transaction costs by using the Internet as an electronic delivery channel.

There are several ways in which organizing groups, investors, or existing banks may establish an Internet national bank. They may operate**:**

- Solely via the Internet (Internet-only bank).

- Predominantly over the Internet, but also have limited branch or nonbranch physical facilities, such as kiosks or ATMs (limited facility bank).

- Traditional branches in tandem with a substantial Internet transactional web-based delivery channel.

Unless otherwise indicated, all three types of banks are referred to herein as "Internet banks." This booklet provides guidance on these processes and the special issues and considerations presented by proposals for these types of banks.

Novel questions and issues about the use of the Internet for delivery of banking products and services often arise in the application process. The OCC approves proposals to establish national banks that will use an electronic delivery channel when the bank may reasonably be expected to operate successfully and in a safe and sound manner. In so doing, the OCC does not guarantee that a proposal to establish a national bank is without risk to the organizers or investors.

In particular, the market segment comprised of "Internet-only" financial institutions largely remains in its infancy. These institutions, for the most part, have not yet achieved consistent and sustained growth or profitability.

The marketing, delivery, and pricing of Internet banking products and services continues to evolve. Any interested group, therefore, should become familiar with the performance and experience of the existing "Internet-only" financial institutions that have entered the banking arena.[1]

Chartering a New Internet Bank

An organizing group filing for a new Internet national bank charter will find the process much the same as for any national bank charter, with some enhancements and variations for policy issues, described in this booklet.

Any organizing group must be comprised of five or more persons. Many, if not all, of the organizers normally serve as the bank's initial board of directors. The president of the proposed bank, who is usually the chief executive officer (CEO), must be a board member. Generally, every national bank director must own stock of the bank and be an U.S. citizen throughout his/her term of service (12 USC 72). The OCC requires that each organizer submit a complete biographical and financial report. (See the "Director Waivers" and "Background Investigations" booklets of the *Comptroller's Corporate Manual*.)

An organizing group should submit the specific information described in the "Charter" booklet of the *Comptroller's Corporate Manual* (Manual) along with the additional information described in this booklet.

Acquiring the Stock of an Existing National Bank

New investors and organizing groups also may acquire an existing bank or the holding company of an existing bank (see the following holding company discussion) and change the direction of the bank's existing business to operate as an Internet bank. A group that adopts this strategy, rather than charter a new national bank, must file a change in bank control notice (Notice) with the OCC and submit certain information in a Notice as described in the "Change in Bank Control" booklet of the *Manual*. This includes a full description of the proposed changes to management and the operating or business plan (business plan) of the existing bank.

---

[1] For instance, see OCC's *Quarterly Journal*, June 2000, Volume 19, No. 2, pages 29-46, "Who Offers Internet Banking?"

The acquirers must file the Notice at least 60 days prior to the acquisition. The OCC may extend the review period for up to 120 more days, depending on the complexity of the proposed changes to the business plan and the completeness of the Notice submitted. Normally, the OCC completes its review, including background investigations, during the initial 60-day review period. The Notice is subject to a public notice and comment period. The Change in Bank Control Act establishes the criteria for deciding whether the OCC will raise an objection to the filing.

Any group planning to acquire control of an existing national bank should contact the Licensing Manager in the appropriate district office to begin discussions about the acquisition. (See Appendix B for a listing of Licensing offices.)

Holding Company

An organizing group that charters or acquires control of a national bank may consider holding the bank stock either directly or through another corporate entity. If the group holds the stock through a separate corporate entity, that entity normally will be considered to be a bank holding company subject to Federal Reserve Board (FRB) regulation and examination. A group proposing to own a national bank through a bank holding company would have to apply to the FRB for approval of a holding company application. The OCC provides the FRB with its comments on the proposal prior to the FRB's decision.

A bank is a subsidiary of a holding company if 25 percent or more of its voting stock will be owned or controlled by a holding company. There are other circumstances under which control is determined, and organizers should consult with the appropriate regulator regarding their particular circumstances.

When investors acquire a bank through a holding company with the intent of changing the character of the bank's business to one that is an Internet bank, the comment on the proposal to the FRB is the only avenue the OCC may have to ensure that the fundamental supervisory concerns are addressed. Accordingly, the OCC encourages filings to contain a revised business plan that fully discusses the new electronic banking activities. The FRB and the

OCC work closely together to obtain all necessary information about the proposal, including conducting a joint field investigation to review the proposal.

At the OCC's request, the FRB normally will ask the holding company to commit to provide the OCC with a 45- to 60-day notice prior to implementing its Internet plan or otherwise significantly altering the existing bank's operations. This prior notice will ensure that the OCC has time to review the proposal, including the architecture and system security, marketing strategy, capital, and liquidity, for an Internet plan, solicit any necessary information, and resolve issues or concerns. If a holding company commitment cannot be assured, the OCC will issue an adverse comment on the proposal to the FRB, which then requires the FRB to hold a public hearing. Accordingly, those filing are encouraged to provide commitments that are satisfactory to the FRB and OCC.

Converting to a National Bank

Another alternative for entering the national banking system is to convert a financial institution with a different type of charter to a national bank charter. Under applicable statutes and regulations, state banks, state savings banks, and other state banking institutions engaged in the business of receiving deposits, as well as federal savings associations may be converted directly to national bank charters. Conversions are not subject to a public notice and comment period.

A conversion application should describe any significant change in the existing business plan, such as adding Internet banking for its customers or becoming an Internet-only delivery channel. If adding Internet banking upon conversion, the application should contain a revised business plan that fully discusses the new electronic banking activities and technology. A detailed discussion of conversion transactions is contained in the "Conversions" booklet of the *Manual*.

Products, Services, and Activities

National banks may engage in the "business of banking" and exercise "all such incidental powers as shall be necessary to carry on the business of

banking"[2] as well as powers granted in other statutory authority. Over the years, the OCC and the courts have based many of the activities performed by national banks on interpretations of this language. The OCC has compiled comprehensive listings of Internet and electronic activities and banking powers permissible for national banks. These lists appear on the OCC's Web site. The Internet and electronic activities list is located at the Internet Banking section entitled, "OCC Opinions and Letters." The list of activities permissible for national banks is at the Corporate Applications section, entitled, "Bank Activities" (see http://www.occ.treas.gov). These lists are updated routinely.

Types of Electronic Banking

A national bank may offer banking products and services through electronic means and facilities,[3] such as the telephone, personal and palmtop computers, pagers, and other devices.

Informational Web

This basic level of Internet banking is informational only. A Web site has marketing information about the bank's products and services on a stand-alone server. The risk is relatively low if informational systems have no path between the server and the bank's internal network. This level of Internet banking can be provided by the bank or by third parties. Although the risk to a bank can be relatively low, the server or Web site may be vulnerable to alteration. Therefore, appropriate controls must be in place to monitor and prevent unauthorized alterations to the bank's server or Web site.

Transactional Web

This level of electronic banking allows customers to execute transactions, exposing the bank to greater risks than informational Web sites. Transactional Web sites allow customers to purchase products and services and conduct banking transactions online. Customer transactions can include such activities as opening and accessing an account, purchasing products and services, applying for a loan, paying bills, and transferring funds. Wholesale,

[2] The National Bank Act, 12 USC 24(Seventh).
[3] See 12 CFR 7.1019.

retail, and fiduciary products and finder services also are included. Because a connection typically exists between the outside user and the bank or service provider's internal computer systems, this type of Internet banking may introduce risks of safeguarding customer information and thus merit strong internal controls.

Wireless

Although there are few emerging standards for wireless service, this technology permits banks to offer consumers existing and new products and services through another delivery channel. Banks may provide consumers products or services through wireless devices, such as cellular telephones, pagers, personal digital assistants, palmtop computers, or other devices that have wireless access to the bank. The products and services offered may range from informational (e.g., account inquiry or stock portfolio tracking), or transactional (e.g., transfer of funds between accounts), to "finder" services (e.g., bringing buyers and sellers of nonbank related products or services together). Because the products and services offered in most instances would involve sensitive or confidential information, ongoing security and monitoring is essential for banks that provide products and services through the wireless domain.

PC Banking

This type of electronic banking system allows some interaction between the bank's systems and the customer. It provides a closed delivery channel via proprietary software and a telephone — sometimes referred to as "home banking." The interaction may be limited to e-mail communication, transfer of money, and review and balance accounts, bill payment without checks, or static file updates (name and address changes). Because these servers may have a path to the bank's internal networks, the risk is higher with this transactional configuration than with informational systems. Appropriate controls must be in place to prevent, monitor, and alert management of any unauthorized attempt to access the bank's internal networks and computer systems.

Application Process

Before filing an application, the OCC encourages prospective applicants to contact the OCC Licensing staff, in the district office that serves the area in which the bank will be located, to discuss corporate proposals. The OCC also encourages each filer to appoint a contact person to serve as its primary liaison (spokesperson).

The OCC has a staff assigned to provide advice and to review and comment on electronic banking applications. This staff is composed of supervisory, compliance, legal, economic, and policy staffs and designated as the E-banking team (see Procedures for specific offices assigned). This staff will be involved in prefiling communications, which may take the form of formal prefiling meetings or more informal exploratory discussions or conference calls.

Exploratory Inquiry

Interested parties may wish to review the OCC's Web site for written guidance on Internet banking and the application process. The Web site contains decision statements on OCC Internet charter approvals and provides information on the policy matters that OCC considers prior to making a decision. The Web site also contains opinions and legal interpretations addressing a variety of electronic banking activities, including E-commerce alliances, and the manner in which they may be established and conducted. After becoming familiar with the agency's Internet and corporate filing information, a spokesperson of an organizing or investor group may wish to call the Licensing staff at the appropriate district office to ask for further information or assistance (see Appendix B.)

When key ideas are developed, the spokesperson may request an exploratory conference call or meeting to ask questions, clarify concerns, and become acquainted with the regulatory environment. The district Licensing staff will arrange an initial conference call with the appropriate OCC Licensing and E-banking staffs. If there are any written materials to be submitted, the documents should be submitted early enough for OCC staff to review prior to the conference.

Prefiling Discussions and Meetings

As soon as the organizers or investors are prepared to proceed and have a draft or outline of their plan, the spokesperson should schedule a prefiling meeting with the OCC's Licensing staff. The Licensing staff will assemble its E-banking team to conference or meet with the organizers. For a new bank charter, the OCC typically expects all organizers of the proposed new national bank to attend a prefiling meeting. When requested, OCC staff will consider conducting the prefiling meeting at a location proposed by the filer rather than at the OCC.

At the prefiling meeting, the Licensing staff reviews the OCC's chartering policy and procedures, its supervisory perspectives, and the requirements for filing the appropriate application. This includes discussion of the attributes of a national bank; the composition of the board of directors; the management team; business plan, including the alternative business strategy; planned information systems technology architecture; vendor management; and compliance issues, among other items. The Federal Deposit Insurance Corporation (FDIC) staff also may participate in the prefiling meeting to discuss pertinent procedures and requirements for obtaining deposit insurance. (See the FDIC's deposit insurance policy statement, available from its Communications Office, Public Information Center, 801 17th Street NW, Washington, DC 20434, or from its Internet site, http://www.fdic.gov.)

The OCC will provide assistance to ensure that applicants provide the essentials of a complete application.

Preparation of Filing

The OCC expects each applicant to prepare accurately and completely each filing it submits. Each applicant certifies that its filing, or supporting materials, contains no misrepresentations or omissions. In addition, each filer should:

- Submit all necessary information about a proposed corporate filing to aid the OCC in reaching an informed decision quickly.

- Determine compliance with all applicable statutes and regulations.

- Seek advice from legal counsel, as appropriate.

Application Issues

Many issues are evolving with the establishment of Internet banking operations. Some of the business issues for Internet-only banks are branching, capital and growth, liquidity, profitability, management resources, alternative business strategies, and business resumption planning. Other issues for Internet banks arise from the compliance perspective, such as security, authentication, privacy and confidentiality, disclosure notices, access to service, and cross border operations. An independent feasibility analysis or study may provide an objective opinion of the effect of these issues and the business plan viability. However, a thorough explanation and discussion of these issues should be provided in the application.

Branching

A national bank, upon formation, must have a main office for conducting business with the public. An Internet-only or limited facility bank does not have the usual "brick and mortar" building many think of as the traditional banking office. However, a national bank is not limited to conducting its business only from the main office location. Establishing branches or alternatives to branches, such as ATMs, kiosks, and banking by telephone or computer, may help national banks better serve their customers. An applicant should describe fully the delivery system for its products and services, especially disbursing loan proceeds, paying withdrawals, and receiving deposits. Certain nonautomated facilities, such as drop boxes, are branches, if established by the bank.

If a national bank seeks to establish or acquire one or more branches to receive deposits, pay withdrawals, or make loans to customers in person, it must obtain approval from the OCC, which applies standards established in federal law. Those standards, in turn, are based on ones set forth in state law as incorporated in 12 USC 36. A branch application may be submitted along with the charter application at no additional cost.

Alternatives to Branching. Assuming that a bank, for legal or operational reasons, is not entering a particular locality through branching, a national bank may establish an office that engages in more limited activities and is not

considered to be a branch. As a result, the office is not subject to geographic restrictions or OCC approval. It may:

- Engage in loan origination. These are called loan production offices (LPOs). A national bank may engage in almost any activity involved in lending at an LPO, except disbursement of loan proceeds to borrowers. Loan proceeds must be disbursed at an approved branch, or by another mechanism, such as by:

  — Check through the mail.

  — Disbursal through a third-party escrow agent.

  — Credit to a deposit account of the borrower.

  Other methods of disbursal that do not trigger branching concerns also may be available.

- Engage in deposit production. These are called deposit production offices (DPOs). A national bank may use a DPO to open deposit accounts and engage in other activities related to the deposit account function, but it may not take deposits from or pay withdrawals at a DPO. Deposits and withdrawals must be made through other mechanisms, such as by mail or ATM machines. A DPO with a deposit-taking ATM must be included in a bank's CRA assessment area.

- Conduct business through Remote Service Units (RSUs). Banks may use RSUs, including automated teller machines, automated loan machines (ALMs), and other automated devices, to receive deposits and pay withdrawals, among other account functions. An RSU may be located at a fixed site or moved from location to location to provide services at sites that generally may not support the need for a fixed-site RSU or that occasionally draw a number of people who could use the services of an RSU for a limited period of time (e.g., fairs, sporting events, meetings). Because RSUs are not branches under federal law, they are not subject to geographic restrictions or OCC approval. (See 12 CFR 7.) However, the location of a deposit-taking RSU must be included in a bank's CRA assessment area.

- Conduct business through kiosks. A bank may provide service to customers at kiosks established in places, such as retail stores or shopping malls and accessible at all hours that the store or mall is open. A kiosk for a bank that provides services over the Internet may contain a computer terminal connected to the bank's Internet Web site and a telephone by which customers and prospective customers can contact the bank's call center. The kiosk also may be staffed by a representative of the bank, who would perform only ministerial functions, such as answering questions about products and services, directing customers to the telephone to contact the call center, assisting customers with deposit forms and loan applications at the computer terminal, and verifying identification and income of new customers. A bank representative must not handle cash, checks, or other cash substitutes or otherwise have a role in effecting deposit, withdrawal, or loan disbursement transactions between the bank and the customer. Rather, these functions can occur only at an ATM or other RSU, either adjacent to the kiosk or at another freestanding location. Following the opening of a deposit or loan account, the representative may provide the customer with a bank (ATM) card to access their account. Facilities operated in this manner are not branches under federal law and, thus, are not subject to geographic restrictions or OCC approval. (See 12 CFR 7.) As previously stated, however, the location of a deposit-taking RSU must be included in a bank's CRA assessment area.

Capital

An organizing group must raise a sufficient amount of capital to pay all organization costs, to compete effectively in the market area, and to adequately support planned operations. The organizing group should present thorough arguments to support its proposed capital. The OCC may determine that higher amounts of capital from those originally proposed are warranted based on local market conditions or the business plan presented (see Appendix A for sample plan). In all cases, the fundamental principle applied is that a national bank should hold capital commensurate with the level and nature of the risks present in or projected for the institution.

There is no specific dollar amount for initial capitalization for an Internet-only or limited facility bank. Although the OCC does not have a stated capital minimum, Internet bank proposals have ranged from $10 million to $425 million in initial capital, depending upon the business plan, target market,

and growth plans. The OCC expects projected capital for new banks to remain at or above the "well-capitalized" level, as defined in 12 CFR 6.4(b)(1), for the first three years of operation. These are "minimum capital standards." Additional capital would be required to support high-risk operating strategies and plans. The Federal Deposit Insurance Corporation (FDIC) has requirements similar to those of the OCC for obtaining federal deposit insurance. The FDIC's Statement of Policy requires that initial capital should be sufficient to provide a Tier 1 capital to assets leverage ratio of not less than 8 percent throughout the first three years of operation.[4]

New Internet banks, similar to other technology ventures, may wish to raise capital through several private financing rounds ultimately leading to an initial public offering. However, tiered capital injections during the first three years of the business plan normally would not be approved if the bank does not have a parent company to serve as a source of capital strength.

The OCC has no general prohibition against the inclusion of preferred stock in the initial capital structure of a new national bank. However, the OCC may determine that the inclusion of a significant amount of preferred stock in a bank's capital structure could lead to instability in the bank ownership or otherwise adversely affect the safety and soundness of the institution. Such a determination would justify denial of the charter application.

Generally, the OCC is opposed to debt-based capitalization of a new bank. If a principal shareholder takes on personal debt or an affiliate issues debt to capitalize the bank, the organizing group must demonstrate that debt service requirements can be met without reliance on cash flows of any kind from the bank.

Liquidity

An Internet bank's business plan may underestimate the marketing and operating expenses necessary to attract and retain new deposits over the Internet as it establishes its product and marketing strategies, and thereby increase its liquidity risk. Liquidity risk is the current and prospective risk to earnings or capital arising from a bank's inability to meet its obligations when they come due without incurring unacceptable losses. Liquidity risk includes

[4]See FDIC Statement of Policy on Applications for Deposit Insurance, 63 Fed. Reg. 44756, August 20, 1998, effective October 1, 1998.

the inability to manage unplanned decreases or changes in funding sources. Liquidity risk also arises from the failure to recognize or address changes in market conditions that affect the ability to liquidate assets quickly and with minimal loss in value. The business plan should contain a discussion of how the bank plans to manage its liquidity risk.

The bank and its holding company may be required to enter into a binding written agreement setting forth the holding company's obligations to provide liquidity support to the bank, if and when necessary. If such a condition is imposed, the terms and provisions of any liquidity maintenance agreement must be acceptable to the bank and the OCC, and may include a provision for collateral to support those obligations. Required documents may include maintenance of a contingency funding plan that would be provided to the OCC periodically on request.

Contingency Funding Plan

As part of a comprehensive liquidity risk management program, Internet banks should develop and maintain a contingency funding plan (CFP). The degree and sophistication of a CFP should be commensurate with the bank's complexity and risk exposure, activities, products, and organizational structure.

A CFP is a cash flow projection and comprehensive funding plan that forecasts funding needs and funding sources under market scenarios, including rapid asset growth or liability erosion. The CFP should represent management's best estimate of balance sheet changes that may result from a liquidity or credit event. The CFP can help control day-to-day liquidity risk by showing that the bank, even if it is in financial trouble, could find sources of funds to cover its uses of funds.

If a bank relies on its holding company for contingency funding or liquidity support, the holding company should also prepare a CFP, which incorporates its potential support for the bank. This holding company CFP should then be incorporated into the bank's CFP to ensure appropriate coordination and documentation.

The CFP can be valuable for day-to-day liquidity risk management. Integrating liquidity scenario analysis into the day-to-day liquidity

management process will ensure that the bank is best prepared to respond to an unexpected problem. In this sense, a CFP is an extension of ongoing liquidity management and formalizes the objectives of liquidity management by ensuring:

- Maintenance of an appropriate amount of liquid assets.
- Measurement and projection of funding requirements during various scenarios.
- Management of access to funding sources.

Pursuant to 12 CFR 30, a national bank experiencing extraordinary asset growth may be required to file a safety and soundness plan with the OCC describing the sources and uses of liquid resources. A CFP that projects effective liquidity risk management under market scenarios of continuing asset growth or liability erosion substantively may satisfy the liquidity requirements of a safety and soundness plan.

Alternative Business Strategy

The organizers or investors must develop a comprehensive alternative business strategy and integrate it into the business and strategic plans and capital and funds management policies. The objective of the alternative business strategy is to ensure that the bank can manage potential scenarios prudently, efficiently, and effectively when the asset or deposit mixes, interest rates, operating expenses, marketing costs, and/or growth rates differ significantly from the original plans. This alternative plan should include realistic plans for how the board would access additional capital in the future, if situations dictate.

Management Selection

The organizers and board of directors are responsible for investigating thoroughly the background and qualifications of each proposed executive officer, using criteria no less stringent than those detailed in the Management Review Guidelines section of the "Background Investigations" booklet of the *Manual*. This responsibility cannot be delegated to counsel or consultants.

Senior management of an Internet bank must understand the technological basics behind electronic banking. Management and the board should be well balanced between bankers and technology persons. For example, a successful Internet business often uses traditional advertising techniques in addition to Web-based advertising and hyperlinks.

When a bank hires a CEO, the board of directors or a designated board committee should manage the selection process actively. The selection criteria should include integrity, technical competence, character, and experience in the financial services industry. The CEO should share the board's operating philosophy and vision for the bank to assure that mutual trust and a close working relationship are maintained. The CEO of an Internet bank should have expertise appropriate for the business lines in which the bank will engage. Although a background in technology is helpful, it is equally important that the CEO has the knowledge, skill, and experience to distinguish the customers the bank will serve, monitor the evolving marketplace, and implement a marketing plan to reach those customers.

It is crucial that the bank employ a Chief Technology Officer or equivalent. This person should have management expertise to oversee all aspects of bank information technology and understand the risks related to electronic banking. What once was considered back room operations is now the forefront of an Internet banking business. The management team should be able to evaluate innovations in technology and implement those appropriate to the bank's business lines.

Narrowly Focused Operations

Proposals that possess unique risks are those that call for narrowly focused banking services or those that anticipate serving a narrowly defined market niche through an Internet-only platform, such as lending portfolios that are heavily concentrated or target a restricted customer base. The risks that are exacerbated in narrowly focused banks include concentrations, funding/liquidity, capital, customer authentication, and strategic planning. Those unique risks require well-defined business strategies (including contingency plans, sound funding sources, and projected capital commensurate with the risks) and specialized management.

Because of the unusual supervisory risks associated with narrowly focused banks, the OCC will review the business plan to ensure that it adequately addresses the following risks:

- *Concentrations.* Diversified asset and liability portfolios, product selection, funding sources, and target markets help make a bank less vulnerable to a downturn in any one market that could significantly affect its income or liquidity. Narrowly focused banks, by their very nature, are not as diversified as traditional banks, and a bank's business plan should address how any concentration risk will be mitigated. The plan also should detail the source of required expertise to engage in a certain industry or lending type.

- *Funding and liquidity*. Some organizers have underestimated the marketing and operating expenses involved with an Internet delivery channel as they establish their product strategies. The organizers should clarify in the business plan how the bank's sources of funding are reasonably diverse, how it intends to maintain adequate liquidity, and how credit-sensitive funding risks will be managed.

- *Capital.* The business plan should identify sufficient capital to address uncertainties and provide a clear ability to raise capital, if needed. Except in rare circumstances, initial capitalization at a minimum must be sufficient to support the proposed bank until it achieves profitable operations, while maintaining adequate capital levels. Depending on the risk profile of a narrow-focused bank's business plan, higher capital levels may be required. This level of initial capital is particularly important if the bank relies on an Internet-only platform for distribution of products and services.

- *Customer authentication/security*. The business plan of a bank using the Internet as a significant means of product delivery must address authentication and security issues. The bank's method of customer authentication and fraud detection is critical because of the lack of physical contact with bank customers. Internet banking platforms allow bank customers to access information and systems directly, including those that enable funds transfers between banks (ACH). Also, pursuant to the Bank Secrecy Act, banks must report and record customer transactions

that exceed certain thresholds. In an Internet environment, a bank may need to modify its systems for monitoring customer transactions.

- *Strategic planning*. Narrowly focused banks often target a limited customer base and frequently have ill-defined contingency plans for redirecting efforts should the business plan not be successful. Organizers should define clearly in the business plan their targeted audience (*e.g.,* by product and geographies) and the strategic alternatives.

The OCC may require an independent third-party feasibility analysis or study be obtained to evaluate the likelihood of the success of the proposed business plan. This independent evaluation should address the bank's growth potential, competitor level, organizational and operational costs, financial implications, and the viability of the proposed bank's business plan.

Use of Vendors

A bank may rely on vendors to provide the delivery and technology expertise for its Internet banking services. The bank should perform due diligence before selecting a vendor to provide such services. It also should have a formal service agreement with the vendor that clearly addresses the duties and responsibilities of the parties involved and that meets the needs of the bank's business and strategic plans. (Organizers should enter into contracts contingent on preliminary approval of their application.)

If a bank contracts out to various vendors certain functions of its internal operations, the bank must notify the OCC of the relationship. The process of subcontracting activities that the bank would otherwise perform for itself triggers the requirements of the Bank Service Company Act, 12 USC 1861 *et seq.*[5] Pursuant to this statute, services performed for the bank by contract or otherwise, will be subject to the examination oversight of the OCC. A bank should notify potential vendors in writing of the OCC's examination and regulatory jurisdiction should they contract with the bank. This understanding regarding OCC jurisdiction should be included in all vendor contracts.

[5] In particular, see 12 USC 1867(c).

An application should outline with some detail and certainty what functions the bank will outsource and what it will do in-house. The application should include a list of the vendors being considered, including background information, the number of years in business, their financial condition (statements), and a copy of any contract. Also the application should include a description of the due diligence the applicant will conduct of each vendor's operation and how the applicant will evaluate the total cost pricing.

As an example, many bank customers use the telephone to conduct banking activities. Many banks have a telephone call center that operates 24 hours per day, 7 days per week. While outsourcing this call center to a vendor may be more efficient and economical, it may increase the bank's transaction, compliance, and reputation risks that customer calls may be mishandled. Accordingly, it is important that management conduct sufficient due diligence to evaluate the vendor's operation and provide ongoing monitoring of the vendor and the service level.

A bank is responsible for the security of its customer and bank records. When vendors are used, the bank also must ensure that the vendor secures those records properly.

Before the bank is granted final approval and allowed to open, it must develop a vendor management program, which will be reviewed at the preopening examination.

Verification and Authentication

As banks migrate to electronic commerce business models, effective processes must be in place to verify the identity of new customers at account opening and to authenticate existing customers when they initiate transactions. Customers will not be required to deal with bank staff in person. A national bank offering deposit-related products and services, including noninterest-bearing demand deposits, interest checking, money market accounts, certificates of deposit, and electronic bill payment, must ensure that it adequately verifies the identity of its customer.

The OCC expects national banks to exercise appropriate caution and due diligence when opening accounts using the Internet, mail, and other means. Customer verification is the process that a bank uses for new accounts to

corroborate the identity of new customers. A new account process involves requesting a variety of customer information items, including name, address, phone number, social security number, driver's license information, among other things. The bank then independently verifies the accuracy of this information.

Additionally, to establish a new customer account, the bank's process for granting the customer the authority to access the account via an electronic means is to use a predefined linkage between the customer and the account. Then the bank can use this predefined linkage to determine if the same person or an imposter is trying to access the account. This process is referred to as authentication. Authentication is a logical access control process that enables the bank to limit the computer system and account access to authorized parties. Logical access controls typically employ multiple attribute authentication including something the customer has (customer identification), something the customer knows (password), and as technology evolves something the customer is (biometric identity).

Internal systems and controls should address the risks associated with electronic accounts and include appropriate procedures to verify customer information as part of the account opening process and to monitor for fraud and suspicious activity after an account has been opened. A bank should monitor the verification and account authorization procedures continually to ensure a rigorous process for identifying, measuring, and managing the risk exposures. This process should include a regular audit function to test the controls and ensure they continue to meet the defined control objectives.

These procedures for access control also are essential for preventing fraud, money laundering, and other abuses. Whenever warranted, banks should consider restricting, or limiting, the type of customers or transactions for Internet banking. To limit the risk of money laundering, some banks restrict the type of business they will accept. For example, some banks do not accept, or they place additional controls over, accounts from foreign government officials, money service businesses, military equipment sales companies, and political or gambling organizations. Banks also may restrict account activity by prohibiting cash or monetary instrument deposits.

Business Resumption Contingency Plan

Management should ensure that the bank's business resumption plans tie in or harmonize with the vendors' plans so that in an event of a disaster (fire, power outage, computer problems, earthquake) backup procedures exist for transferring operations to an alternate site location or vendor. Adequate planning limits the financial and operational loss if a disaster occurs. This should be management's primary objective when preparing its business resumption plan.

The business resumption contingency plan should be written, approved by the board of directors, and validated annually by an independent source. Also the board should review the test results and review and approve the plan on an annual basis. This level of planning will provide for logical decisions, enhance employee responsiveness, and alleviate confusion during a crisis.[6] In an Internet bank, contingencies should include alternate delivery channels, such as the mail, telephone, call center, point-of-sale terminals, and ATMs.

Cross-border Operations

The Internet facilitates a bank's ability to conduct transactions with customers outside its normal marketplace, including cross borders. However, such transactions pose added risk management challenges, particularly if the bank plans to conduct business over the Internet in another country without any licensed physical presence there. In addition, banks conducting cross-border Internet banking must ensure compliance with regard to the Office of Foreign Assets Control's (OFAC) regulations, which restrict the processing of financial transactions involving countries under sanctions (see http://www.treas.gov/ofac).

Cross-border risks include adherence to the requirements of the Bank Secrecy Act. Internet banking that permits new accounts to be opened over the Internet with foreign customers must have rigorous account opening standards and controls to identify unusual or suspicious activity.

---

[6] See Interagency Policy on Business Resumption and Contingency Planning, SP-5, for more information.

Moreover, the potential global nature of Internet banking operations may subject a bank to foreign compliance and transactional risks because it must be knowledgeable about the laws and economic, social, and political climates of the foreign jurisdiction in which it is doing business. To mitigate this risk, some banks are using language on their Web sites to specify that the bank will accept deposits only from specified geographic areas and in U.S. dollars from persons residing in the U.S. This protects the bank from inadvertently becoming subject to another country's laws regarding Internet commerce or banking.

Stock Benefit Plans

Nonbanking companies, desiring to form a national bank, may have stock benefit plans that have existed for a period of time. These existing stock plans should be structured so they do not conflict with the OCC's policies. For example, if the plan does not include an "exercise or forfeit" provision should capital fall below minimum requirements, the plan would need to be amended.

Stock benefit plans, including stock options, stock warrants, and similar stock-based compensation plans, are a common form of compensation for Internet bank management. When structured properly, the OCC considers it acceptable compensation. The structure of stock benefit plans should encourage the continued involvement of the participants and the successful operation of the national bank. Plans should not contain features that would encourage speculative or high-risk activities, serve as an obstacle to the sale of additional stock, or convey control or provide preferential treatment to any bank insider. In reviewing stock benefit plans proposed for directors and officers, the OCC will consider certain features (see the "Corporate Organization" booklet of the *Manual* for specifics.)[7]

The OCC considers as unacceptable compensation proposals that allow insiders to purchase or acquire a separate class of bank or bank holding company stock with greater voting rights than other investors or to purchase stock at an original issue price lower than that paid by other investors. Such arrangements raise concerns about the bank's ability to raise additional capital, allow control without a proportionate financial investment, and make

[7] See note 4*, supra*.

it difficult for other shareholders to remove directors who hold such stock if they manage the bank in an unsafe manner.

Organization Costs

Normally, the OCC will allow expenses incurred by the organizing group in making application for and organizing a bank to be charged to the bank's capital. An organizing group funds the operations of a national bank through a loan or personal loans from individual organizers.

The cost of start-up activities, including all organizational costs, should be expensed as incurred. Detailed instructions for the definition of start-up activities and the inclusion of these costs in the bank's Report of Income are included in the Glossary instruction "Start-up Activities" to the Consolidated Reports of Condition and Income (Call Report). This guidance is consistent with AICPA Statement of Position 98-5, "Reporting on the Costs of Start-up Activities."[8]

The cost of purchasing and leasing bank premises should be capitalized in the cost of the asset. This would include interest costs incurred during the period the asset is under construction.

All fees and organization costs must be disclosed fully to prospective shareholders in the offering document. Sufficient information must be made available to assist in an evaluation of the reasonableness of such expenses. (See the "Corporate Organization" booklet of the *Manual* for additional information.)

Community Reinvestment Act (CRA)

Banks have a responsibility under the CRA to help meet the credit needs of their entire communities, consistent with the safe and sound operations of such institutions. The CRA regulations establish the framework and criteria by which examiners assess banks' records of helping to meet the credit needs of their communities (12 CFR 25).

[8] See OCC Bulletin 98-29, accounting for computer software costs.

The CRA uses a variety of terms to describe the institutions subject to its provisions, including "financial institutions," "regulated financial institutions," and "insured depository institutions." The statute defines a "regulated financial institution" as an "insured depository institution." Thus, the federal banking agencies apply the CRA, by its terms, to all insured depository institutions[9] whether they operate "traditionally" or through the Internet.

A purpose of the CRA was to require the federal financial regulatory agencies to use their supervisory authority to encourage insured depository institutions to help meet the credit needs "of the local communities in which they are chartered to do business." Consequently, the CRA sets forth the assessments that the agencies must conduct with respect to the record of all insured depository institutions within their respective jurisdictions in meeting community credit needs. These assessments generally relate to local communities in which the institution operates, in that the agencies must assess the institution's CRA record in its "entire community, including low- and moderate-income neighborhoods." The Interagency regulations implementing the CRA include requirements relating to the delineation of "assessment areas" for assessing the CRA record of covered institutions, which focus on activities conducted in the areas surrounding the institution's main office, branches, and deposit taking ATMs. Because Internet banking is not conducted in a conventional over-the-counter environment, but Internet banks are still insured depository institutions subject to the CRA, the agencies have faced a challenge in determining how to assess such institutions because the concept of "community" does not fit their operations easily.[10]

The CRA assessment area generally will consist of one or more metropolitan statistical areas or one or more contiguous political subdivisions (such as counties, cities, or towns), and it must include the geographic areas in which the bank has its main office, branches, and deposit-taking ATMs, if any. When an Internet bank is chartered, it designates a location for its charter. This site would be deemed to be the main office of the bank and would be included in its assessment area.

---

[9] The Interagency CRA regulations do not apply to certain special purpose banks, such as bankers banks (as defined in 12 USC 24(Seventh)), that do not perform commercial or retail banking services by granting credit to the public in the ordinary course of business.

[10] See Interagency Questions and Answers Regarding Community Reinvestment.

The CRA regulations (12 CFR 25) provide several evaluation methods for all national banks, including Internet banks:

- **Small banks**[11] are evaluated under the small bank test. This test focuses primarily on lending and lending-related activities in the bank's assessment area. In addition, small banks may elect to be evaluated under the large bank test, provided the bank collects, maintains, and reports the data required by the CRA regulations.

- **Large banks** (those that do not meet the definition of a small bank) are evaluated under the lending, investment, and service tests. As their names imply, these tests focus on the banks' performance in lending (home mortgage, small business, and small farm, and generally, at the bank's option, consumer lending), as well as community development lending, with a primary focus on the bank's assessment area; making investments (qualified investments that benefit the bank's assessment area or a broader statewide or regional area that includes the assessment area); and providing services (retail banking services, alternative delivery systems, including branches and community development services).

- **Community development test.** Some Internet banks (of any size) may be eligible for evaluation under the community development test. This test evaluates the bank's community development lending, qualified investments, and community development services — first in the bank's assessment areas or the broader statewide or regional area that includes its assessment areas, and, if the bank has adequately addressed credit needs in that area, nationwide. To be evaluated under this test, the bank must first be designated by the OCC as a limited purpose or wholesale bank. A limited purpose bank offers only a narrow product line (such as credit cards or motor vehicle loans) to a regional or broader market. A wholesale bank is not in the business of extending home mortgage, small business, small farm, or consumer loans to retail customers. The OCC has approved Internet banks that were designated limited-purpose and wholesale. For example, one bank limits its activities to credit card lending and deposit solicitations. Another bank focuses on deposit

[11] A bank that has total assets of less than $250 million as of December 31 of either of the prior two calendar years and independent or affiliated with a holding company that had total bank and thrift assets of less than $1 billion as of December 31 of either of the prior two calendar years.

products and payment-related services with no lending products offered to the public or to be purchased from other institutions.

A bank must request, in writing, to be designated as a limited purpose or wholesale bank. The request should be submitted at least three months prior to the proposed effective date of the designation and addressed to the Deputy Comptroller for Community and Consumer Policy.

- **Strategic plan.** A bank of any size or business strategy may elect to be evaluated under a strategic plan that it develops. A bank seeks informal and formal public comment during development of its plan. The plan is submitted to the OCC for approval. A plan, which may have a term of up to five years, must have annual interim measurable goals for helping to meet the credit needs of the bank's assessment area through various lending, investment, and service activities. Although a plan must address all three types of activities, emphasis may be placed on one or more of the activities, depending on the bank's capacity and constraints, product offerings, and business strategy. If a bank meets the goals specified in the plan for satisfactory performance, the bank will be rated satisfactory. (The bank may also include goals that represent outstanding performance.) The strategic plan option provides a more flexible alternative to a bank that is concerned that the requirements of the other tests are too rigid for the nature of its operations. Some Internet banks open under the small or large bank test but plan to develop a strategic plan after a period of transactional history.

The CRA requires the OCC and other federal regulators to provide written public evaluations of banks' records of performance under the law. The four ratings that may be assigned for a CRA evaluation are: outstanding, satisfactory, needs to improve, and substantial noncompliance. The OCC assigns those ratings, which are included in the public evaluation, on the basis of the bank's performance under its applicable assessment method.

CRA evaluations ordinarily are performed on a three-, four-, or five-year cycle, depending on size and overall CRA rating. However, the first CRA examination of a de novo bank will be conducted about 18-36 months after opening.

Field Investigation

The OCC will conduct a field investigation for an Internet bank application approximately 45 to 60 days after the application is filed. The OCC will tailor the scope of each onsite investigation, depending on the complexity of the application, with input from the supervisory office and other OCC divisions. The findings from such an investigation will influence the OCC's overall analysis and review of the application.

A national bank examiner, and other OCC personnel as necessary and appropriate, will review relevant materials; interview the organizers, board members, insiders, and other identified persons; explore matters related to the proposed bank's operations; and meet with the organizing group to discuss findings. Whenever possible, the OCC coordinates its investigation with the FDIC. (See "Procedures - Field Investigation" section for details.)

The cost for a field investigation is included in the filing fee.

Decisions

The OCC may approve or conditionally approve any filing after reviewing the application and considering the relevant factors. The OCC may impose conditions if it determines that they are necessary or appropriate to ensure that approval is consistent with applicable statutes, regulations, OCC policies, and safe and sound operation. (See the OCC's Web site for a summary of the Internet and electronic banking decisions for Internet banks.)

The OCC may deny a filing for reasons, including:

- The existence of significant supervisory, CRA (if applicable), or compliance concerns.

- Approval would be inconsistent with applicable law, regulations, OCC policy, and safe and sound practices.

- The applicant fails to provide in a timely manner information that the OCC requested to make an informed decision.

Preliminary Conditional Approval

Following the review of a new bank charter application or change in control notice, the OCC decides to grant preliminary conditional approval, raise no objection, or disapprove the request. Preliminary conditional approval indicates permission to proceed with the organization of the bank according to the plan set forth in the application but indicates that the applicant is subject to special conditions based on its unique proposal. Some of these conditions may have to be satisfied prior to opening.

The organizational steps of a new national bank generally include hiring management and staff; establishing premises; purchasing computers and other equipment; selecting vendors; developing and implementing policies, procedures, and controls; and raising capital. Preliminary conditional approval is not an assurance, however, that the OCC will grant final approval for a new national bank charter. Once the OCC grants preliminary conditional approval to a charter proposal, the organizing group must satisfy certain procedural and special requirements[12] before the OCC will grant final charter approval. In addition, the OCC sometimes imposes conditions that will remain in place after the bank opens.

In addition to the standard preopening requirements, the OCC may impose other special conditions related to the chartering of an Internet bank, such as:

- Submission, for review and approval, a complete description of the bank's final information systems and operations architecture and related control plans.

- Implementation of a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities.

- Executing a written agreement between the bank and its holding company that provides for capital maintenance and liquidity support to the bank. The terms and provisions of the agreement must be acceptable to the bank

[12] See the Standard Requirements listing in the Appendixes section of the "Charter" booklet of the *Manual*.

and the OCC, including a provision for collateral to support obligations, if required by the OCC.

- A higher amount of capital than originally proposed.

- Maintenance of an 8 percent Tier 1 capital leverage ratio for the first three years.

Final Conditional Approval

An Internet bank may not begin the business of banking until the OCC grants final approval. The OCC imposes the following standard conditions on each final approval of an Internet bank:

- During the bank's first three years of operation, the bank shall obtain prior written approval from the OCC's (appropriate supervisory office) before any significant deviation or change from the proposed operating or business plan occurs. The bank must notify the (appropriate supervisory office) at least sixty (60) days prior to any proposed significant deviation or change. The bank also must provide a copy of such notice to the FDIC's (appropriate regional supervisory office).

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

These conditions of approval are conditions "imposed in writing by the agency in connection with the granting of any application or other request" within the meaning of 12 USC 1818. As such, these conditions are enforceable under 12 USC 1818.

Regarding the first condition, the bank is not prohibited from deviating from its business plan. This condition requires that the bank obtain prior approval of deviations that are considered "significant."[13] Significant deviations or changes that have not been approved during the organization stage may be

[13] See OCC PPM 5400-9 for description.

grounds for delaying issuance of the charter or for withdrawing preliminary approval.

Preopening Examination

The preopening examination is the last major step of the national bank chartering process and will be performed within two weeks of the institution's scheduled opening date. The bank and OCC should be in continual contact as the preopening requirements are accomplished, including the board's drafting of the Minimum Policies and Procedures.

The organizers should submit a request to the OCC Licensing staff to schedule this examination at least 30 to 45 days before the proposed opening date. An interdisciplinary examination team, lead by the portfolio manager when practical, will visit the bank at least 14 days prior to the proposed opening date to determine whether the board of directors and management are prepared to begin operations and all preopening conditions have been met. The examination will be broad in scope and include an evaluation of the bank's final plans to identify, monitor, and control all relevant risks, especially transaction, strategic, and reputation risks stemming from the use of technology. Credit, interest rate, liquidity, strategic, reputation, and compliance risks also will be evaluated.

After the preopening examination, a meeting with the board of directors and management will be held to discuss examination findings. (See the "Corporate Organization" booklet of the *Comptroller's Corporate Manual* for specific procedures.)

Opening

Many Internet banks choose to conduct a so-called "soft opening" after receiving FDIC deposit insurance and OCC final charter authorization. Unlike a more traditional bank charter, the new Internet bank silently opens without marketing publicity, launching its Web site, usually under a hidden and temporary Web address. This soft opening permits the bank to test the completed and integrated systems in a live mode using real accounts with a small group of insider account holders. The bank can initiate and complete a variety of banking transactions outside its internal system, including with various servicers and participants, such as electronic bill payment provider,

core data processor, ATM switch, and interaction with the Federal Reserve System. The bank then can complete the remaining system and security testing and make any necessary adjustments before offering its services to the general public.

Thus, if the new bank finds it necessary, upon notifying the OCC and FDIC, to take the Web site "offline" for an extended period of time to make system changes, the bank's reputation is not damaged. When an Internet bank's delivery capabilities are concentrated in the Internet channel, the soft opening process helps the bank manage and control the reputation risk associated with an extended outage, as well as future transaction and other relevant risks. Banks have conducted a soft opening phase over a two- to four-week period. Once bank management is confident that the Web site is fully functional, it can proceed with a "hard opening" that implements its planned marketing efforts and notifies the public of the Web site address.

Supervision and Oversight

Overview

Internet banking creates new risks and challenges for national banks. From a supervisory perspective, risk is the potential that events, expected or unexpected, may have an adverse impact on the bank's earnings or capital.

Some Internet banking proposals center on narrowly focused lines of business or "niches." Although the OCC encourages innovation and the use of technology in the financial services industry, some nontraditional banking proposals contain high-risk strategies that must be controlled through well-considered risk management policies and practices and supported by strong capital and funding plans. If unprecedented or unusual banking services are proposed, the OCC will require detailed information and additional review.

Board of Directors' Oversight

The establishment of Internet banks enables many organizers and investors to become involved for the first time with a financial institution. Becoming a member of the board of directors for a national bank brings unique challenges of working in a supervised and regulated environment.

A national bank, as other corporate organizations, has shareholders that elect a board of directors. A bank's board of directors oversees the management of the bank's activities. Directors must exercise reasonable care when guiding the bank's affairs.

Although banks, as other corporations, use their capital to support their activities, most of the funds banks put at risk belong to others, primarily depositors. Banks lend and invest customers' deposits to earn a profit and a reasonable return to shareholders and to meet the credit needs of the community. Generating a return to shareholders from depositors' funds creates the framework for determining the risks that a bank can undertake prudently. The proper management of risk to serve those interests is a critical challenge faced by the board and bank management. As corporate directors, bank directors have duties of diligence and loyalty to the banking corporations they serve.

Directors of national banks are accountable, not only to their shareholders and depositors, but also to their regulators. The long-term health of a bank depends on a strong, independent, and attentive board. The board of directors does not guarantee the bank's success; however, it must oversee bank operations to ensure that the bank conducts business in a safe and sound manner and in compliance with laws and regulations.

The board must set policies with clear standards to guide the bank's operation, and it must monitor the bank's performance on an ongoing basis. When overseeing the bank's business performance, the directors should compare results to those of the business plan's financial projections and to its peer group. Monitoring the bank's key financial ratios and asset quality will keep the directors aware of the bank's business performance. It must keep informed about the bank's operating environment; hire and retain competent management; and ensure that the bank has a risk management structure and process suitable for the bank's size and activities.

The board should be involved in approving contracts,[14] and reviewing the analysis of vendor financials, security report summaries (e.g., intrusion attempts, vulnerabilities, internal security violations), and performance report

[14] For privacy considerations, see OCC Bulletin 2000-25, dated September 8, 2000, issuing "Privacy Laws and Regulations."

summaries (e.g., response times, system capacity, downtime). It also should oversee the bank's disaster recovery process, approving Internet-related policies and the business resumption plan, and set the strategic direction for the bank, including the Internet banking activities.

The board should be aware of certain red flags for electronic banking:

- Unresolved or repeat audit deficiencies.
- A system that does not have regular review and certifications by independent auditors, consultants, or technology experts.
- Management that is unable to provide a basic description of the system architecture, a comprehensive inventory of service providers, or effective vendor management.
- Systems, products, or services that are inconsistent with the bank's strategic plan.

More information about the role of a bank director is available in the OCC's *The Director's Book: The Role of the National Bank Director;* the OCC's *Red Flags in Board Reports -- A Guide for Directors*; and the FDIC's *Pocket Guide for Directors*.

Safety and Soundness Protections

Federal banking law includes certain restrictions on the business of banking to ensure the safety and soundness of the national banking system. For example, federal law limits:

- Certain transactions between a bank and its "affiliates."
- Loans to "insiders."
- Total lending exposure to any one customer.
- Capital distributions and management fees if the bank is undercapitalized.

Affiliate Transactions

Sections 23A and 23B of the Federal Reserve Act (FRA)[15] are designed to protect a bank from losses in transactions with its affiliates. Section 23A defines "affiliate" to include any "company" that controls a bank and any company that is under common control with the bank. Except in the case of a bank's financial subsidiary, bank subsidiaries generally are not considered to be affiliates of the bank.

Section 23A of the FRA

Section 23A protects banks by:

- Limiting "covered transactions" with any single affiliate to no more than 10 percent of the bank's capital and surplus,[16] and aggregate transactions with all affiliates to no more 20 percent of capital and surplus. Covered transactions include a bank's extensions of credit to its affiliates or purchases of assets from its affiliates; investments in securities issued by affiliates, and certain other transactions exposing the bank to risk.

- Requiring that all covered transactions between a bank and its affiliates be made on terms consistent with safe and sound banking practices. In particular, a bank may not purchase low-quality assets from its affiliates.

- Requiring that all extensions of credit to an affiliate be secured by a statutorily defined amount of collateral.[17]

Section 23B of the FRA

Section 23B requires a bank to engage in certain transactions with its affiliates only on terms and under circumstances that are substantially the same or at least as favorable to the bank as those prevailing at the time for comparable transactions with unaffiliated companies. This requirement

[15] See 12 USC 371c, 371c-1.
[16] The 10 percent limit is not applicable to a bank's transactions with a financial subsidiary (12 USC 371c(e)(3)(A)).
[17] A full or partial exemption from these restrictions may be available for certain statutorily prescribed types of transactions. See, for example, section 23A(d).

generally means that affiliate transactions must be conducted on an arm's-length basis. Thus, for example, pricing must reflect fair market value. Section 23B applies this restriction to any covered transaction, as defined by section 23A, and to other transactions, such as a sale of securities/assets and the payment of money or the furnishing of services to an affiliate.

Transactions with Insiders

Any financial or other business arrangement, direct or indirect, between the organizing group or other insiders (i.e., executive officers, directors, and principal shareholders) and the proposed bank must be made on terms no less favorable to the bank than market value or comparable standards. Although the bank may receive preferential treatment from the insider, the insider may not charge the bank a higher rate or require more onerous terms than those that would prevail in a comparable transaction between the bank and an unrelated third party.

Any contracts between the bank and any insider for services should include provisions addressing obligations of, and options available to, the parties should the OCC revoke its approval or object to a proposed executive officer.[18]

Under the FRB's Regulation O (12 CFR 215) and the OCC's part 31 (12 CFR 31), a bank (subject to a number of regulatory and statutory exceptions) may not make a loan to an insider in an amount that exceeds 15 percent of the bank's capital and surplus. In addition, a bank cannot extend preferential loans to insiders. Additional restrictions and requirements apply to loans to executive officers and other types of insider loans under those regulations.

Capital Distributions

Notwithstanding the permissibility of any particular dividend payment under 12 USC 60, national banks are subject to the safety and soundness protections provided by the prompt corrective action statute. Accordingly, under 12 USC 1831o(d)(1)(A), a national bank may not pay a dividend if the bank would be undercapitalized after the dividend payment is made.

---

[18] See the "Insider Activities" booklet of the *Comptroller's Handbook,* the OCC's *The Director's Book: The Role of the National Bank Director*, and 12 CFR 215.4(a).

Supervision by Risk

Traditional

The OCC has defined nine categories of risk for bank supervisory purposes. Those risks are credit, interest rate, liquidity, price, foreign currency translation, transaction, compliance, strategic, and reputation. It is essential that the board of directors become familiar with these nine risk categories as they apply to Internet banking. They are discussed thoroughly in the "Internet Banking" booklet of the *Comptroller's Handbook*, issued October 1999 (see Appendix C or http://www.occ.treas.gov/netbank/ebguide.htm).

Novel

Internet banking exposes a bank to a different mix of risks than traditional banking, because transaction, strategic, reputation, credit, and compliance risks are generally greater for an Internet bank. Internet banking creates new control challenges for risks for national banks. An Internet bank must be concerned with the escalating speed of transactions, the lack of direct control over an end user, and the verification and authentication of the user's identity.

An Internet bank that opens new accounts over the Internet must have rigorous opening standards and controls to identify and report suspicious activity (see Authentication section discussed previously).[19] The global nature of Internet operations may subject a bank to compliance, credit, and transactional risks, especially cross-border exposures (see Cross-border Operations section discussed previously).

Internet banking increases a bank's reliance on vendors and service providers to develop and maintain the technology systems, such as the Internet and the bank's internal systems. A bank must have adequate internal controls to manage and monitor such risks.

[19] 31 CFR 103.18 and 12 CFR 21.11 requirements.

Risk of Electronic Delivery

Fraud and money laundering risk considerations may require the use of more rigorous identification, authentication, and transaction verification methods than those used with traditional delivery channels. Liquidity, interest rate, price, reputation, and foreign currency translation risks may result from poor data integrity or unreliable systems. Electronic delivery risks should be managed as part of a bank's overall risk management process.

As described more fully in OCC Bulletin 98-3,"Technology Risk Management," banks should use a rigorous analytic process to identify, measure, monitor, and control risks. The quantity of risk assumed should be consistent with the bank's overall risk tolerance and must not exceed the bank's ability to manage and control its risks.

Risk Considerations

Outsourcing

A primary concern for bank management when the bank is outsourcing its functions is the need to maintain control over the services and products provided by third parties. For example, when negotiating contracts, management should confirm that responsibilities and accountability are defined clearly for each party. Management should ensure that the bank may exercise the control necessary to properly manage the products or services. Control items should include, but not be limited to, the bank's ability to perform audits and to obtain from the service provider independent internal control audits and summaries of test results. Bank management should establish controls that allow the bank to confirm third party recovery plans, review their financial condition, and establish data ownership with the third party. Management should establish its rights, to the extent possible, in the event a third party fails to perform under the contract. The contract also should permit modification to provide for regulatory compliance and for any change in applicable law. Management may wish to pursue a provision in the contract that provides for the service provider to notify the bank of a significant change in staffing or operating procedures.

The bank should consider the conditions under which it can terminate or change service providers or software vendors without incurring substantial liability in the event plans change or performance standards are not met.

Outsourcing to vendors does not relieve the bank from accountability for managing risk or assuring sound system controls. (See the Vendor Management section of the "Internet Banking" booklet of the *Comptroller's Handbook*.)

Information System Security

A bank's overall security program should include a risk-based protection strategy and risk management plan, a security policy, an awareness program, security controls, and testing activities. These elements are not unique to Internet banking, but rather are discussed to emphasize the importance of a sound program in managing risks that may arise from the use of electronic banking systems. A bank should use a combination of access, authentication, and other security controls to create a secure and confidential banking environment. These generally include passwords, firewalls, encryption, and intrusion detection and management.[20]

A bank should develop a description of its information systems architecture, including a discussion of the technologies used and key elements of the security policies, internal controls, and audit procedures.[21] A draft description should be submitted with the application or as soon as possible prior to the field investigation. The description should include a schematic drawing and discussion of the following items: Vendors and vendor contracts; Internet banking security policies; operating processes, including, but not limited to, vendor management, customer, vendor, and employee authentication; security mechanisms; business resumption plans; personnel; internal controls; and internal audit plans.

An Internet bank should have performed an independent security review and test of its Internet bank platform. The bank must have this review performed regardless of whether the platform is operated in-house or by one or more third-party service providers. This review must be conducted by an objective,

[20] For a more complete discussion of security, see OCC Bulletins 2000-14, 98-38, 98-31, BC 229, and the "Internet Banking" booklet of the *Comptroller's Handbook*.
[21] OCC Bulletin 98-1, Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing.

qualified internal or external source (Reviewer). The scope should cover the adequacy of physical and logical protection against unauthorized external access including individual penetration attempts, computer viruses, denial of service, and other forms of electronic access. In addition, the Reviewer must assess the adequacy of internal security. By written report, the Reviewer must confirm that the security measures, including the firewall, have been satisfactorily implemented and tested. The report must critique the effectiveness of security policies and controls and confirm, with reasonable certainty, that unauthorized internal or external data and network access or access attempts will be detected and recorded. As part of its decision to grant final charter approval, the OCC will consider the results of the report as well as any subsequent actions by the bank or service provider to implement any recommendations or to remedy any noted security or control deficiencies.[22]

Firewalls

Firewalls are used on Internet and electronic banking systems as security measures to protect internal systems. Firewalls provide a gateway to guard against unauthorized persons gaining access to the bank's network. The mere presence of a firewall does not assure logical security because firewalls can be penetrated.

Other controls work in tandem with firewalls. These controls include logical access controls and physical security. Access to systems, networks, and information should be on a "need-to-know" basis. A logical access control includes a user identification and a password. Each user should have a unique password composed of at least 6 to 8 alphanumeric characters. The use of passwords that are easily discerned must be avoided. (See "Appendix A, Firewalls and Associated Controls" of the "Internet Banking" booklet of the *Comptroller's Handbook,* for more detail.)

---

[22] Prior to the OCC's granting final approval to open, the bank will be required to have a security program in place that complies with the minimum security guidelines the Federal Banking Agencies publish under section 501(b) of the Gramm-Leach-Bliley Act (see 15 USC 6801, 6805(b)). Additionally, after opening, the bank should analyze security risks posed by new technology (and any needed program adjustments) before the bank adopts the technology to determine whether a security program remains adequate in light of the new risks presented.

Intrusion Detection and Management

Intrusions to networks may result in the misuse of funds through internal or external sources, destruction of customer and bank records or confidential information, or the denial of service. To address external attacks on a computer, bank management must create and implement a strong security strategy and program. Such a strategy and program should include intrusion risk assessment, risk mitigation controls, intrusion response policies and procedures, and testing processes.

Intrusion detection systems can be an integral part of the strategy. They review system logs and processes in near real time and alert management to known patterns of behavior that indicate an intrusion is occurring or is likely to take place soon. Although the systems are not infallible, their ability to scan voluminous logs for pattern identification and trends makes them a valuable supplement to manual reviews. Accordingly, management should consider real time intrusion detection systems when transaction activity cannot be monitored effectively by manual processes or systems.[23]

Encryption

Transactions on the Internet or any other telecommunication network must be secure to achieve a high level of public confidence. Customers, banks, and merchants need assurances that they will receive the service as ordered or the merchandise as requested, and they know the identity of the person with whom they are dealing. Encryption increases the security of transactions by providing confidentiality. Some forms of encryption may ensure that a transaction has not been tampered with.

Internet banking systems should employ a level of encryption that is appropriate to the level of risk present in the systems. The OCC does not mandate a particular strength or type of encryption. Rather, it expects management to evaluate security risks, review the cost and benefit of different encryption systems, and decide on an appropriate level of encryption as a business decision. Banks typically use symmetric (private key) encryption

[23] See OCC Bulletin 2000-14, "Infrastructure Threats: Intrusion Risks" (May 2000), OCC Alert 2000-1, "Internet Security: Distributed Denial of Service Attacks" (February 2000), OCC 99-9 and OCC Bulletin 98-38, "Technology Risk Management: PC Banking" (August 1998) for a more complete discussion.

technology to secure messages and asymmetric (public/private key) cryptography to authenticate parties.[24]

Backup and Recovery

A bank should assess the degree of customer reliance on the Internet and the potential risk to its reputation if its Internet banking operations are not accessible or functional. A bank must expand its backup provisions and recovery procedures as customer impact increases. Frequent downtime or a "hacked" site combined with weak backup can damage a bank's reputation and weaken strategic efforts to sustain Internet banking business.

Some suggested preventative and corrective controls include fault tolerant servers, backup battery power, diesel generator backup power, and offsite vaulting (offsite transmission and storage) of data. A bank that has only a small number of customers dependent on the Internet could redirect customers temporarily to other delivery channels (e.g., ATMs, telephone, or bank lobby). The OCC encourages frequent backup of the Web server and procedures to recover the Web server.

Customer Confusion

Hypertext Links to Third Parties

The bank may offer hypertext links to affiliate or third-party Web sites. However, the OCC expects that the bank will take reasonable steps to distinguish clearly between its products and services and those offered by an affiliate or a third party. Individuals who access the Web site should be able to tell when they are dealing with the bank and when they are not. This is especially important, for example, if the third party has different standards than the bank for security, privacy, etc., for information provided over the Internet. Technology offers multiple methods to provide such clarity to potential customers. Examples include simple text and dialogue boxes. These should use short explanatory sentences or bullet lists, a typeface and type size that are easy to read, boldface or italics for key words, and wide margins and ample spacing. Moreover, the bank should conspicuously

[24] See Appendix B, Cryptography, of the "Internet Banking" booklet of the *Comptroller's Handbook,* issued October 1999, for more detail.

disclose that it does not provide, endorse, or guaranty products or services available on third-party sites.

Trade Names

There are no federal laws or regulations that specifically require that all branches of an insured depository institution operate under a single name. Some national banks operate branded and identifiable Internet divisions separately under multiple trade names.

If customers believe they are dealing with two different institutions, they may inadvertently exceed FDIC insurance coverage. Accordingly, an insured depository institution that intends to use a different name for its Internet operations should take reasonable steps to ensure that customers will not become confused and believe that they are dealing with a separate institution or that their deposits are in different institutions and thus are insured separately.[25]

An Internet bank operation using multiple trade names should:

- Make clear on its homepage, and on any pages that allow a customer to initiate deposit account transactions, that the customer is dealing with one bank. For disclosures to be meaningful for bank customers, including those in electronic format, they should be clear, prominent, and easy to understand. Examples of how Internet disclosures may be made conspicuous include: large print easily viewable when a page is first opened; a dialog box that pops up whenever a customer accesses a Web page; or a simple graphic near the top of the page or in close proximity to the bank's logo. These examples are only some of the possibilities for conspicuous disclosures given the available technology.

- Use the legal name in all its legal documents, including certificates of deposit, signature cards, loan agreements, and other similar documents. Bank management should make clear to accountholders and other persons

[25] See OCC Interpretive Letter No. 881 (February 2000); OCC Bulletin 98-22 (Interagency Statement on Branch Names, May 1, 1998). Also see FTC issuance titled, "Dot Com Disclosures: Information about Online Advertising," May 2000, www.ftc.gov.

and businesses in its contracts and other such documents that the bank, not the division, is the legal entity with which they are contracting.

- Educate its staff so that customer confusion about deposit insurance is avoided. This means that it will be important for the staff who respond to questions from potential and current accountholders of both the bank and the division to clarify the status of the division in a way that is readily understood by customers. Thus call center employees, whether employees of the bank or those contracted through a third-party service provider, will need instruction about the possible customer confusion associated with multiple trade names.

- Obtain a signed statement from new accountholders that they are aware that the Internet-based operation is part of an insured institution and deposits held via the Internet channel are not separately insured.

To further address customer confusion[26] about FDIC insurance, the new deposit account customers of both the Internet operation and the traditional bank should sign a document indicating awareness of FDIC aggregation of deposits for the multiple identities. For example, Bank X could place the following disclosure on its Bank Y deposit application forms and deposit disclosure documents on the Bank Y's Web site.

> "Bank Y (Internet banking for Bank X), and Bank X, are the same FDIC-insured institution. Deposits held under each trade name are not separately insured but are combined to determine whether a depositor has exceeded the $100,000 federal deposit insurance limit."

Liability Insurance

A bank may wish to acquire liability insurance to mitigate any loss it might incur for inadequate or faulty systems. Some insurance companies are offering various specialty policies to businesses that assume the risk of the legal liability. Some specialty insurance policies offered are:

- Intellectual property, that usually covers patent, trademark, and copyright infringement suits.

[26] Also see OCC Alert No. 2000-09, Protecting Internet Addresses of National Banks.

- Breach of computer security, that protects from hacker threats, such as damage to or theft of data, extortion, and loss of income from attacks (called "cyber" insurance).

- Errors and omissions, that usually covers lawsuits from negligence and performance failure of the business' product or service.

Examination Frequency and Scope

By statute, every national bank must receive a full-scope, on-site (safety and soundness) examination not less than once every 12 months. The OCC may extend the 12-month interval to 18 months for institutions meeting certain criteria for size and condition. The first examination will be performed no later than 12 months after the institution opens for business.

The OCC conducts specialized examinations for other aspects of bank operations. Bank Information Technology (BIT) examinations usually are conducted on the same cycle as safety and soundness examinations; i.e., once in each 12- or 18-month cycle) and normally are conducted concurrently with other parts of the safety and soundness examination. Compliance with CRA will be reviewed via management reports to determine if the institution is making satisfactory progress in this area.

Internet banks, particularly Internet-only or limited facility banks, are exposed to greater risks than the traditional brick and mortar bank. There is generally less diversification among products offered. The newness of the industry exposes the bank to greater credit, compliance, reputation, strategic and transactions risk. The result is that, with few exceptions, Internet banks will be subject to more frequent examinations and reviews than the traditional brick and mortar bank. The specific level of supervision that each bank receives will be determined on a case-by-case basis, after review of each bank's risk profile through the quarterly monitoring program.[27]

[27] For details on the quarterly monitoring, see PPM 5400-9.

The Evaluation Process

Because banking is essentially a business of accepting risks, the OCC's supervisory process is centered on evaluating those risks. The OCC does this through its supervision by risk program, using a risk assessment system. Examiners evaluate the quantity of risks and the quality of risk management systems in each bank and assign each risk an aggregate assessment (low, moderate, or high) and an expected direction of change (increasing, stable, or decreasing). Risk assessments are used to develop supervisory strategies that guide examination activities throughout the supervisory cycle.

Additionally, all financial institutions are evaluated and rated under the Federal Financial Institutions Examination Council's Uniform Financial Institutions Rating System. This system, which is referred to as the CAMELS rating, assesses six components of a bank's performance: Capital adequacy, Asset quality, Management administration, Earnings, Liquidity, and Sensitivity to market risk. Evaluations of the components take into consideration the institution's size and sophistication, the nature and complexity of its activities, and its risk profile.

Composite and component ratings range from **1** to **5**. A **1** is the highest rating, indicating the strongest performance and risk management practices relative to the institution's size, complexity, and risk profile, and the level of least supervisory concern. A **5** rating is the lowest rating, indicating the most critically deficient level of performance, inadequate risk management practices relative to the institution's size, complexity, and risk profile, and the greatest supervisory concern. (For a more detailed discussion, see the *Comptroller's Handbook*, "Bank Supervision Process.")

Some common problems associated with new Internet banks are:

— Slower than anticipated growth (ineffective marketing plan).

— Rapid growth rate.

— Impatience for growth/profitability.

— Aggressive industry deposit pricing.

— Difficulties in hiring qualified personnel.

— Excessive salary/occupancy expense.

— Management/board incompatibility.

— Consumer compliance weaknesses.

— Initial high overhead expense compared with projections.

— Poor asset/liability management.

— Inability to generate quality loans.

At the conclusion of each full scope examination, examiners discuss their findings with bank management and the bank's board of directors and summarize those findings in a report of examination. These meetings allow an opportunity to discuss the objectives of the OCC's supervision; strategic issues that may be confronting the bank; any major concerns, risks, or issues that may need to be addressed; and other matters of mutual interest.

Compliance Supervision

An Internet bank must comply with all consumer protection laws and regulations that apply to its operations**.** OCC Bulletin 98-31, entitled "Guidance on Electronic Financial Services and Consumer Compliance," provides answers to many of the basic compliance questions that Internet banks ask, along with examples. It provides basic information and suggested guidance pertaining to federal consumer protection laws and regulations and their application to electronic financial service operations. This guidance is divided into two sections: (1) The Compliance Regulatory Environment, and (2) The Role of Consumer Compliance in Developing and Implementing Electronic Services.

All national banks are subject to a number of statutes and regulations administered or enforced by the OCC. In addition to banking laws, national banks may be subject to various other federal or state laws and regulations, including securities, insurance, fiduciary, consumer protection, and

disclosure laws and regulations. Summaries of the regulations that have posed particular challenges for Internet banks follow.

Privacy

National banks are subject to a number of federal statutes and regulations that govern the disclosure of consumer information. The most comprehensive of these provisions is Title V of the Gramm-Leach-Bliley Act that requires banks and other financial institutions to provide consumers of their financial products or services with privacy notices and an opportunity to opt out of certain information sharing with nonaffiliated third parties. Banks also are subject to the Fair Credit Reporting Act (FCRA), which governs the use and disclosure of consumer reporting information. Additionally, banks should be aware of the Electronic Fund Transfer Act, the Right to Financial Privacy Act, the Children's Online Privacy Protection Act, and the Federal Trade Commission Act.

Gramm-Leach-Bliley Act Privacy Provisions — The Gramm-Leach-Bliley Act (GLBA)[28] enacted new privacy-related provisions applicable to financial institutions. The federal banking regulatory agencies promulgated final rules (see 12 CFR 40) to implement these provisions that become effective November 13, 2000. Compliance with these regulatory requirements is mandatory as of July 1, 2001.

In general, the regulations require banks to provide their customers with notices that accurately describe their privacy policies and practices, including their policies for the disclosure of nonpublic personal information[29] to their affiliates and to nonaffiliated third parties. The notices must be provided at the time the customer relationship is established and annually thereafter. Notices must be clear and conspicuous and provided so that each intended recipient can reasonably be expected to receive actual notice. The notices must be in writing or may be delivered electronically if the consumer agrees.

---

[28] Pub. L. 106-102; 15 USC 6801 *et seq*., effective November 13, 2000.

[29] Generally this means any information that is provided by a consumer to a bank to obtain a financial product or service, that results from a transaction between a bank and a consumer involving a financial product or service, or that is otherwise obtained by a bank in connection with providing a financial product or service to a consumer. If a bank obtains information about its consumers from a publicly available source, that information will not be protected (i.e., subject to notice and opt out) unless the information is disclosed as part of a list, description, or other grouping of a bank's consumers.

Subject to specified exceptions that permit banks to share information in the ordinary course of business, banks may not disclose nonpublic personal information about consumers to any nonaffiliated third party unless consumers are given a reasonable opportunity to direct that their information not be shared (opt out). Thus, before a bank may disclose nonpublic personal information about a consumer (even if not a "customer") to a nonaffiliated third party, the bank must provide the consumer with an initial privacy notice and an opt-out notice (which may be included in the privacy notice).

The GLBA regulations also provide that a bank generally may not disclose an account number or similar form of access number or code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in marketing. A bank may, however, disclose its customer account numbers to third party agents or servicers in order to market the bank's own products or services, provided the bank does not authorize the third party to initiate charges to customer accounts. The regulations also limit the redisclosure and reuse of nonpublic personal information obtained from other nonaffiliated financial institutions.

FCRA Information Sharing Provisions—The FCRA sets standards for the collection, communication, and use of information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. The communication of this type of information may be a "consumer report" subject to the FCRA's requirements. However, the FCRA specifically excepts from the definition of "consumer report": (1) the disclosure of a bank's own transaction and experience information to any third party; and, (2) the disclosure of consumer reporting information to a bank's affiliates if the bank first notifies its consumers that it intends to share such information and provides them with an opportunity to opt out of this information sharing (affiliate information sharing).[30]

As a general matter, a bank will not be subject to the FCRA's substantial requirements that apply to consumer reporting agencies[31] if the bank

[30] The GLBA directed the OCC and the other federal banking regulatory agencies to adopt regulations to carry out the purposes of the FCRA. On October 20, 2000 the agencies published for comment joint proposed regulations regarding the affiliate information sharing provisions of the FCRA.
[31] These requirements related to furnishing consumer reports only for permissible purposes,

communicates information only in a manner consistent with the two exceptions described previously.

Banks' information disclosures may be subject to both the GLBA and the FCRA. Therefore, it is critical that banks understand the differences between the GLBA and the FCRA provisions to reduce compliance risks in this area. The statutes differ in the scope of their coverage, as well as in their requirements for a bank's treatment of consumer information. As a result, what may be a permissible disclosure under one statute may be prohibited or subject to different conditions under the other statute. Because compliance with one statute will not entail compliance with the other, banks are strongly advised to evaluate the requirements of both laws in connection with their disclosures of consumer information. (For a more detailed discussion, see OCC Bulletin 2000-25, "Privacy Laws and Regulations,"[32] issued September 8, 2000.)

Other Provisions—Banks and their subsidiaries should be aware of the following federal laws that may affect their consumer financial information practices:

- The Electronic Fund Transfer Act and Regulation E require that banks make certain disclosures when a consumer contracts for an electronic transfer service or before the first electronic fund transfer is made involving the consumer's account.

- The Right to Financial Privacy Act prohibits a bank from disclosing a customer's financial record to the federal government, except in limited circumstances, such as pursuant to the customer's authorization, an administrative subpoena or summons, a search warrant, a judicial subpoena, or a formal written request in connection with a legitimate law enforcement inquiry, or to a supervisory agency in connection with its supervisory, regulatory, or monetary functions.

- The Children's Online Privacy Protection Act (COPPA) establishes requirements applicable to the collection, use, and/or disclosure of personal information about children that is collected through the Internet

---

maintaining high standards for ensuring the accuracy of information in consumer reports, resolving consumer disputes, and other matters.

[32] Specific guidance located at www.occ.treas.gov/ftp/bulletin/2000-25a.pdf.

or another online service. Banks are subject to COPPA if they operate a web site or online service (or portion thereof) directed to children, or have actual knowledge that they are collecting or maintaining personal information from a child online.

- The Federal Trade Commission Act prohibits unfair or deceptive acts or practices in or affecting commerce, and provides a basis for government enforcement actions against deception resulting from misleading statements concerning a company's privacy practices or policies, or failures to abide by a stated policy.

Advertising

Advertisements on Internet Web sites must meet the advertising requirements of Regulation M (Consumer Leasing), Regulation Z (Truth in Lending), and Regulation DD (Truth in Savings). Although final regulatory interpretations have not been published, guidance is available, and banks should structure their advertisements to minimize compliance risk. Issues that banks should consider when posting electronic advertisements are the clear and conspicuous standard, multi-page advertisements and triggering terms.

To meet the clear and conspicuous standard, banks must be aware of the regulatory requirements regarding the prominence of certain disclosures in their advertisements. Banks also must consider the requirements of Regulations M and Z that permit creditors and lessors to provide required advertising disclosures on more than one page, if certain conditions are met. Banks should monitor carefully amendments to these regulations to ensure compliance with multi-page advertising in the context of electronic advertisements. Banks must comply with the triggering term requirements of Regulations M, Z, and DD ensuring that the terms are disclosed appropriately and are set forth clearly and conspicuously.

Real Estate Settlement Procedures Act

The Real Estate Settlement Procedures Act (RESPA) is a consumer protection statute that requires mortgage brokers and/or lenders to give a borrower pertinent and timely disclosures regarding the nature and cost of real estate settlements. RESPA also prohibits kickbacks and unearned fees, and it places

limitations on the use of escrow accounts. Penalties are provided for violating the prohibitions against kickbacks and unearned fees.

Web linking arrangements and alliances and compensation arrangements with mortgage firms can be structured in a variety of ways. However, banks must ensure that they do not violate the anti-kickback requirements of RESPA. The Department of Housing and Urban Development (HUD) has rulemaking and interpretative authority under RESPA. HUD is developing guidance on this issue.

Fair Lending Statutes

The federal fair lending statutes are the Equal Credit Opportunity Act (ECOA) and the Fair Housing Act (FHAct). The ECOA prohibits discrimination in any part of a credit transaction. The ECOA applies to any extension of credit, including extensions of credit to persons, small businesses, corporations, partnerships, and trusts. The FHAct applies to residential real estate-related transactions. Both of these acts prohibit discrimination based on race, color, religion, sex, or national origin. The ECOA also prohibits discrimination based on age, marital status, receipt of public assistance, or the exercise of a right under the Consumer Protection Act. The FHAct also prohibits discrimination based on handicap or familial status.

The business plan should indicate that the bank understands its obligations under these statutes. Additionally, the charter application should affirm that the bank has designed its marketing efforts to be consistent with these laws. Internet banks focusing on niche markets must be particularly aware of this issue.

Bank Secrecy Act and Anti-Money Laundering Provisions

The Bank Secrecy Act (BSA) and its implementing regulations require financial institutions to file certain currency, monetary instrument, and suspicious activity reports and to maintain certain records for possible use in criminal, tax, and regulatory proceedings (31 USC 5311 et seq., 31 CFR 103, 12 CFR 21.21). Congress enacted the BSA to prevent financial institutions from being used as intermediaries for the movement of criminally derived funds to conceal the true source, ownership, or use of the funds, i.e., money laundering. Although attempts to launder money through a legitimate

financial institution can emanate from many different sources, certain kinds of businesses, transactions, or geographic locations may lend themselves more readily to potential criminal activity than others.

All national banks must establish and maintain procedures reasonably designed to ensure and monitor their compliance with the BSA and its implementing regulations. Failure to comply with these mandates, including the timely reporting of suspicious activity for Internet-related activity, could subject a bank to possible civil and criminal fines and other supervisory action. This requires national banks to establish a compliance program that includes, at a minimum, adequate BSA policies and procedures, designation of a compliance officer, and BSA training and audits. In addition, national banks should be aware of various criminal statutes prohibiting money laundering and structuring of deposits to evade the BSA reporting requirements. (See 18 USC 1956, 1957 and 31 USC 5324.)

Procedures: Establishing a National Bank

Exploratory Inquiry, Conference Call, or Meeting

Licensing Staff

1. Ensures that the inquirer and/or organizers have reviewed the information available on Internet banking on the OCC's Web site (OCC.treas.gov), including this booklet and other applicable booklets of the *Comptroller's Corporate Manual* (*Manual*) for guidance about the OCC's policies and procedures to establish or acquire a national bank. Forwards any requested information about these processes to the inquirer.

2. Notifies headquarters Licensing (HQ LIC) E-banking senior advisor about an inquiry, providing names, sponsor, proposed location (city/state), business line, and any issues raised.

Inquirer

3. Reviews the written guidance and information about the process and begins to develop and document the proposal by preparing the bank's business plan (see Appendix A for sample plan).

4. When key ideas are framed, requests an exploratory conference call or meeting to clarify any questions or concerns. Mails or faxes a copy of any written documents that describes the proposal to the district Licensing staff for distribution to other OCC staff for review *prior* to the call or meeting. Allows adequate time for OCC staff to review the material.

Licensing Staff

5. Schedules an exploratory conference call or meeting with proposed organizers, counsel, and consultants, along with the appropriate district supervisory, legal, and licensing staff, and the E-banking team in Washington, D.C.

The E-banking team is composed of:

- LIC staff—senior advisor or designee.

- Bank Supervision Operations (BSOP) and Bank Supervisory Policy (BKSP) staffs—a national bank examiner/coordinator as each Senior Deputy Comptroller designates and any BSOP and BKSP specialty area staff as included by the BSOP/BKSP coordinators and the appropriate field supervisory and examiner staffs.

- Bank Activities and Structure and Community and Consumer Law attorneys, and the Assistant Chief Counsel for Electronic Banking.

- Economic and Policy Analysis specialists.

6. Sends a copy of any written material to the HQ LIC senior advisor for distribution to the E-banking team for review prior to the conference call or meeting. HQ LIC will coordinate and inform the appropriate team members.

7. Conducts conference call or meeting with all appropriate parties.

Prefiling Meeting

Inquirer

8. When the filing materials are near completion, requests that a prefiling meeting be scheduled to review the filing materials and to discuss the process. This meeting includes all the organizers for a charter, including the chief executive officer (CEO), if possible (collectively, the organizing group), or the acquirers. Sends a copy of the draft filing and business plan at the time of the request to the Licensing staff for distribution to other OCC staff for review, allowing for adequate time (at least two weeks) to review the drafts.

Licensing Staff

9. Schedules a prefiling meeting to review the requirements and procedures for organizing or acquiring a national bank.

    - Invites the FDIC staff to participate in the prefiling meeting.

    - Invites E-banking team, district Assistant Deputy Comptroller (ADC) and Deputy Comptroller (DC) or their staff, as appropriate.

    - Sends a copy of any written material to the ADC or supervisory analyst and to the HQ LIC senior advisor for review prior to the conference call or meeting.

    - HQ LIC senior advisor coordinates and informs the appropriate E-banking team members of the prefiling meeting. Distributes copies of the draft filing and business plan as soon as they are received to all E-banking team members and to any other interested parties for review and comment prior to the meeting.

10. At the prefiling meeting, Licensing staff discusses the following subjects, as appropriate, with the group:

    - How the group came together and the factors that led to the decision to file.

    - The key policies and specific requirements affecting the chartering or acquisition process. For example, capital, funding and liquidity, management selection, CRA plan, Internet technology, vendor selection.

    - An overview of the proposal with particular emphasis on any unique aspects or novel policy or legal issues.

    - The OCC Licensing and supervisory interactions for filings, and, as applicable, those of the FDIC and the Federal Reserve.

- The importance of a comprehensive, well-developed business plan, including the markets the proposed bank will serve and the products and services to be offered.

- The importance of incorporating a multi-scenario alternative business strategy into the business plan. If a bank holding company is organizing, discuss how it will be expected to provide liquidity support and how it should demonstrate that support in the alternative business strategy.

- How to file the charter application or change in control notice and follow the procedures outlined in the appropriate manuals, including the time involved after submission.

- Information about the organizers' or acquirers' qualifications, both individually and collectively.

11. If any prefiling discussion or meeting reveals significant policy, legal, compliance, or supervisory issues, the Licensing staff ensures that specific issues are brought to the attention of the appropriate OCC staff for a decision.

12. Prepares a memo of the meeting and holds it in a pending file. If there was no district supervisory representative at the prefiling meeting, Licensing will e-mail the summary to the appropriate ADC.

13. If necessary, takes steps for the appropriate official to make a decision on any request for a streamlined submission and/or waiver.

14. Sends an OCC response on any request for a streamlined submission and/or waiver to the organizing group and retains a copy, with the original request and any documentation, in a pending file.

Procedures: Filing

Organizers or Acquirers

1. Submit a complete application or notice and filing fee to the licensing manager in the appropriate district office, or if so instructed, directly to HQ LIC.

2. Publish a notice on the date of filing or as soon as practicable before or after the date of filing (see the "Public Involvement" booklet).

Review

Licensing Staff

3. Initiates and enters appropriate information into the Corporate Activities Information System (CAIS). Licensing manager assigns licensing analyst to process the filing.

4. Immediately notifies the HQ LIC senior advisor of receipt (i.e., by telephone or E-mail, which may include the Executive Summary Comments or Application Comments from CAIS). Senior advisor notifies Director, Licensing Operations, who assigns the case coordinator to process the filing.

5. Establishes the official file to maintain all original documents and initiates background checks, as appropriate (see the "Background Investigations" booklet).

6. Forwards the filing fee and the deposit memorandum (Form 6043-01) to the Comptroller of the Currency, P.O. Box 73150, Chicago, Illinois 60673-7150. Retains a copy of the memorandum. Contacts the spokesperson, if the filing fee is not received or is inaccurate.

7. Reviews the filing, relevant information about proposed affiliates and ownership, and biographical and financial information filed to determine if the filing contains all information necessary to reach a

decision. If not, requests any additional information from the spokesperson to be provided by a specific due date.

8. If the application is submitted by a sponsor, consults with the HQ LIC senior advisor or case coordinator to determine if the sponsor's lead depository institution meets the necessary criteria and is eligible for expedited review of the charter application; and

   - If the lead depository institution is not an eligible bank, prepares and sends a letter to the spokesperson providing notice of standard review within five business days of receipt.

   - (If appropriate) If the lead depository institution is an eligible bank, acknowledges filing within five business days of receipt.

9. Within five business days of receipt, after reviewing the filing, notifies the ADC and supervisory analyst of receipt and indicates that a field investigation tentatively should be planned in 45 to 60 days. At the same time, forwards the filing and solicits comments from appropriate OCC staff, including the ADC and the E-banking team, asking for a preliminary response within 15 days of receipt. Consults with the senior advisor or case coordinator for names of E-banking staff assigned to process the application.

10. If filing does not contain all information needed to reach a decision, requests necessary information in writing and establishes a specific due date to provide the information. E-mails a copy of a request for additional information to the ADC and supervisory analyst.

11. After the filing is reviewed for sufficiency, requests a field investigation from the appropriate supervisory office (see Procedures: Field Investigation).

Review and Decision

Licensing Staff

12. Receives and reviews the Field Investigation Report. Forwards a copy to HQ senior advisor or the case coordinator.

13. Prepares confidential memorandum and decision letter, recommending a decision to the delegated official.

14. Forwards the official file to HQ LIC for decision and makes appropriate CAIS entries.

HQ LIC

15. Makes appropriate CAIS entries.

16. Reviews the district's documents for unresolved issues or concerns. Case coordinator conducts meetings with E-banking team to discuss any unresolved policy, legal, or supervisory issues. Prior to decision, schedules and conducts meeting on any filing issues with senior deputy comptrollers. Makes a recommendation; and forwards the official file to the appropriate official for decision.

17. Notifies the spokesperson, interested parties, ADC, and the licensing manager of the decision.

18. Sends the spokesperson a decision letter.

19. Makes appropriate CAIS entries.

20. Completes applicable sections of the New Bank Handoff Checklist, forwarding electronic copies of the following documents, at a minimum, to the supervisory office: the confidential memorandum, preliminary conditional approval letter (including enclosures), updated CAIS comments, and additional material highlighting any supervisory or licensing concerns.

21. For conditionally approved or no objection filings, returns the official file to the licensing manager for additional processing. The case coordinator makes the entry for the condition for significant deviations or changes from the proposed operating/business plan in the "Enforcement Actions" section of the OCC's electronic information system as Type "Regulatory Condition in Writing."

22. To ensure that the special condition is published, submits a copy with signature and an electronic copy of the preliminary conditional approval letter to the secretary to the director of Licensing Operations.

Organizers or Acquirers

23. Receive conditional approval or no objection. Proceed to organize the bank (see the "Corporate Organization" booklet) or acquire control.

24. If the field investigation required corrections or procedures, verifies that deficiencies identified have been corrected or procedures established.

25. Identifies any material change to the filing and provides notice of such change to the Licensing staff.

26. Submits a letter to the Licensing staff attesting to the satisfactory resolution of any conditions imposed in the conditional approval letter.

Close Out

HQ LIC

27. For conditionally approved applications, coordinates with Licensing staff and supervisory office on the status of bank's organizational efforts and compliance with any conditions or special preopening requirements, including possible HQ E-banking team participation in the preopening examination.

28. For denied applications or disapproved change in control notices, reviews the file for completeness and forwards it to Central Records.

29. Makes appropriate CAIS entries.

Procedures: Field Investigation

Assignment and Preplanning

Licensing Staff

1. Requests that the appropriate supervisory office assign the portfolio manager (EIC), Bank Information Technology (BIT) expert, compliance specialist, and additional examiners for the field investigation. Notifies the assigned HQ LIC case coordinator to determine if any members of the E-banking team will participate.

2. Develops the scope of the investigation with input from the supervisory office and other divisions, as appropriate. At least two weeks prior to the investigation, provides a field investigation request to the EIC along with relevant materials (i.e., charter number, application and any amendments, biographical and financial information, scope memorandum describing areas that warrant particular attention).

EIC

3. Notifies the Licensing staff of the possible start dates.

Licensing Staff

4. Notifies the assigned HQ LIC case coordinator of the possible start dates and coordinates the best time for all to participate.

5. Notifies the EIC of all E-banking staff participating and the date preferred for the investigation. With the EIC, determines the date for submission of the memorandum summarizing the results of the field investigation.

EIC

6. Makes arrangements with the applicant and the FDIC:

- Contacts the FDIC to coordinate onsite activities. If desired, Licensing is available to coordinate with the FDIC. The EIC arranges the actual date of the investigation with the charter applicant and the FDIC. The EIC should contact Licensing staff if the timing cannot be coordinated with the appropriate FDIC office. A simultaneous investigation with the FDIC is desirable, but not mandatory.

- Contacts the spokesperson to schedule the investigation.

7. Prior to conducting the investigation:

   - Schedules time to prepare for the onsite investigation by reviewing the charter application, scope memorandum, E-banking team input, any special instructions.

   - Uses judgment to determine and assign the areas to be reviewed.

   - Through the spokesperson, schedules interviews with all directors and senior executive officers identified in the filing.

On Site

8. Interviews the organizers and directors to determine each person's:

   - Familiarity with national banking laws and regulations.

   - Management and business experience.

   - Competency to perform the proposed role (e.g., how he or she will help the bank, what services he or she will use, what attributes he or she brings that will be good for the bank).

   - Knowledge of the business plan, i.e., customers, products and services, market area, competition, and reasonableness of financial projections, and involvement in its development.

9. Determines the feasibility of the business plan, including:

   - The adequacy of projected capital levels.

     (The business plan should present thorough arguments and justification to support proposed capital, including any off-balance-sheet activities contemplated. Special purpose institutions should address factors unique to the risks characteristic of those limited purpose institutions and explain how the capital structure meets such risk concerns. If novel banking products or services are planned, discuss the purpose and need for specific capital levels, including industry comparison, as appropriate.)

   - The reasonableness of the capital budgeting/overhead expense projections for any related hardware, software, data processing, or personnel costs.

   - Whether the market analysis, including economic and competitive components and any independent analysis, and the marketing strategy are reasonable and realistic.

   - Whether earnings and growth are reasonably attainable.

   - The reasonableness of the bank's liquidity structure and its alternative business strategy.

   - Whether management and the board will operate the bank in a safe and sound manner.

   - The level of expertise and technical knowledge of the Chief Technology Officer.

10. Reviews the CRA assessment area and discusses management's plan to serve the identified banking needs of its community.

11. If loan products will be offered, assesses the lending program (may be reviewed at the preopening exam, if appropriate).

- Determines the "Quantity of Risk" (pages 48-52) and the "Quality of Risk Management" (pages 54-59), using the applicable procedures in the *Comptroller's Handbook, "*Loan Portfolio Management" booklet.

- If the bank anticipates lending on-line, describes the process, including customer verification and authentication, on-line credit decisions, and credit-decision modeling information being used.

- If credit scoring will be used, reviews the scoring model using OCC Bulletin 97-24 as a guide.

12. Determines the "Quantity of Risk" (pages 26-29) and the "Quality of Risk Management" (pages 30-47), using the applicable procedures *Comptroller's Handbook*, "Internet Banking" as a guide.

    - Reviews the proposed security measures to assure that the bank's data systems are adequately protected from inside and outside manipulation and fraud.

    - Determines if the planned information systems technology architecture is feasible and will result in safe and sound operations.

    - Determines if the infrastructure, systems, and procedures are capable of expansion to accommodate the proposed business plan.

    - Assesses the adequacy of the disaster recovery and business resumption plans (if not available, reviews at the preopening examination).

    - Reviews any completed Information Systems External Audits and vendor management programs.

13. Reviews any hyperlinks to affiliates or third parties to ensure that customers know with whom they are dealing; i.e., bank or third party.

14. Reviews and assesses any proposed transactions with affiliates or third parties, e.g., fees, referrals, sharing space and employees, and shared salaries.

15. Contacts Licensing staff with any questions during the field investigation or if anything unusual or significant is found.

16. Discusses findings with the ADC and Licensing staff prior to meeting with proposed management and the board of directors.

17. Meets with the proposed management and board of directors at the conclusion of the visit to discuss findings.

    - Discusses major concerns or issues, including risks, impact of failing to correct deficiencies, and suggestions for improvement with proposed management and the board of directors. (See the "Meeting with Boards of Directors" (pages 40-41), "Bank Supervision Process" booklet of *Comptroller's Handbook*, for other applicable meeting discussion items.)

    - Under no circumstances are any conclusions, preliminary or otherwise, conveyed during the investigation or at this meeting. Neither the conclusions nor the likelihood of charter approval should be discussed with the applicant; that is, *no statements should be made that suggest an opinion about whether the charter should or should not be approved*.

18. Prepares a memorandum summarizing the field investigation results.

    - Summarizes findings, specifically addressing any deficiencies, recommendations, and areas of concern. Draws conclusions (e.g., favorable or unfavorable, satisfactory or unsatisfactory) on each matter reviewed and provides supporting information.

    - Because additional information may often be available with which the EIC or ADC are not familiar, the final evaluation or recommendation on the application is reserved for Licensing.

    - Discusses conclusions and reviews draft memorandum findings with the ADC. The ADC must concur with the findings prior to approval of the investigation. If any significant differences arise, every effort should be made to resolve such differences concerning major findings and conclusions.

If differences cannot be resolved, the matters should be referred to the appropriate supervisory office official within five business days of identification.

19. After EIC and ADC approval, records it as a targeted examination (type 99) into the OCC's electronic information system. Accesses the OCC's electronic information system by the bank's charter number; however, the bank is still inactive.

20. Signs the memorandum and forwards it to the Licensing staff. Also sends an e-mail to Licensing advising that the investigation results have been recorded and approved and attaches an electronic copy of the memorandum.

21. Retains the charter file, including the application, all investigation workpapers, and a copy of the written report.

Licensing Staff

22. Communicates formally with the organizing group any significant issues, questions, or concerns remaining from the field investigation and chartering process.

23. Sends copies of all major correspondence and E-mails regarding the bank to the BSOP Internet Banking Coordinator, Washington, DC, the appropriate ADC, supervisory analyst, and portfolio manager.

Appendix A: Sample Business Plan Guidelines

Preparation and Use

The business or operating plan (business plan) should be an integral part of the management and oversight of a financial institution. It should establish the institution's goals and objectives. It is a written summary of how the business will organize its resources to meet its goals and how the financial institution will measure progress.

The business plan should be comprehensive and well developed, demonstrating the result of in-depth planning by the institution's organizers and management. The forecasts of market demand, customer base, competition, and economic conditions should be realistic. The plan must reflect sound banking principles and demonstrate realistic assessment of risk in light of economic and competitive conditions in the market to be served. An institution with a special purpose or focus should address this special or unique feature in detail in the appropriate sections of the plan. In particular, sections of the plan that discuss concentrations, liquidity and funding, capital, customer authentication, and security will be reviewed to ensure that these risks are addressed adequately.

The business plan should be a three-year plan, which provides detailed explanations of actions that are proposed to accomplish the primary functions of the financial institution. The description should provide enough detail to determine that the institution has a reasonable chance for success, will operate in a safe and sound manner, and will have capital that is adequate to support the risk profile.

For an institution with an Internet or alternative delivery channel, the plan should contain a clear and detailed definition of the market that the institution will serve and the products and services it will provide. An Internet operation has a potential global market of anyone with Internet access. The selected population information is essential to understand the risks associated with a global market. The marketing plan should explain how the institution would achieve brand recognition.

Confidentiality

In general, requests for confidential treatment of specific portions of the application and exhibits must be submitted in writing concurrently with the submission of the application and must discuss the justification for the requested treatment. An applicant's reasons for requesting confidentiality should specifically demonstrate the harm (e.g., to its competitive position, invasion of privacy) that would result from public release of information (5 USC 552). Information for which confidential treatment is requested should be: (1) specifically identified in the public portion of the application (by reference to the confidential section); (2) separately bound; and (3) labeled "Confidential." An applicant should follow the same procedure regarding a request for confidential treatment with regard to the subsequent filing of supplemental information to the application.

An applicant should contact the OCC for specific instructions regarding requests for confidential treatment. The OCC will determine whether the information submitted as confidential will be so regarded and will advise the applicant of any decision to make available to the public information labeled as "Confidential."

BUSINESS PLAN (Sample Plan)

I. Table of Contents

II. Executive Summary (Describe the highlights of the plan)

III. Description of Business

A. Provide a detailed description of your business, including the products, market, and services as well as a thorough description of the market niche (what makes your business unique).

B. Discuss the legal form and stock ownership, and any investment in subsidiaries or service corporations.

C. Describe the location, office quarters, and any branch structure. Include any temporary quarters.

D. If applicable, describe the institution's present financial condition and current resources; such as branch network, staff, and customer base. Specifically include a discussion of the institution's strengths and weaknesses.

IV. Marketing Plan

A marketing plan should include a market analysis, including an economic and competitive component. The plan should contain a detailed discussion that provides factual support that the institution has reasonable prospects to achieve the revenue projections, customer volume, and key marketing and income targets.

A. Product Strategy

1) List the planned products and services (include activities of any subsidiaries). Generally discuss how the institution will offer products over the three years, indicating any variation in the different market areas, and include the time frame for the introduction and the anticipated cost associated with each.

2) Briefly describe the primary sources of loans and deposits and the major methods used to solicit them. If using brokers or agents, provide full details on the nature and extent of all such activities, including sources, amounts, fees, and any intended tie-in of compensatory arrangements with the broker or agent.

3) Outline in detail the functions that will be outsourced and those the institution will do in-house. Describe the due diligence conducted of the vendors' operation and how the institution evaluated the total cost pricing.

4) Describe any arrangements with other E-commerce businesses.

B. Market Analysis

NOTE: The analysis should be based on the most current data available, and the sources of information should be referenced. This section should contain a detailed, in-depth discussion of the major planning assumptions for the market analysis that were used to develop the plans and objectives and the basis for the assumptions.

1) Describe the intended target market and the geographical market area(s). Provide a map that specifically identifies each market area. Collectively, the maps should delineate areas from which the organizing group expects the proposed bank to draw approximately 75 percent of its business.

2) Describe the demographics of the target market population (age, education, and occupation.)

3) Economic Component[33]

(i) Describe the economic forecast for the first three years of operation. The plan should cover the most likely and worse case scenarios.

(ii) Indicate any national, regional, or local economic factors that may affect the operations of the financial institution. Include an analysis of any anticipated changes in the market, the factors influencing those changes, and the effect they will have on the institution.

(iii) Describe the current economic characteristics of the proposed market(s), for example, size, income, and industry and housing patterns.

(iv) Discuss the economic factors that influence the products and services to be offered. A more in-depth discussion is warranted where different types of products and services are identified for different market areas in the Description of Business section.

4) Competitive Analysis

(i) List any and all potential competitors inside and outside the proposed market area(s).

(ii) Discuss the product strategy for the proposed institution that compares and contrasts that strategy with the organizing group's perception of those of its competitors. Include expected results in terms of relative strength, market share, and pricing.

(iii) Discuss the overall marketing/advertising strategy, including approaches to reach the target market through marketing of brand, products, and services.

[33] If obtained, discuss any independent economic survey or market feasibility study.

Outline the specific medium that will be used, including timing and level of advertising efforts.

V. Management Plan

A. Directors and Officers

1) Provide the number of organizers and/or directors, salary and other forms of compensation, if any, and the number and percentage of shares each will purchase.

2) Describe the organizational structure and provide an organizational chart, indicating the number of officers and employees. Describe the duties and responsibilities of the board of directors and senior executive officers. Describe any committees that will be established.

3) Discuss the qualifications and experience of the proposed directors and senior executive officers to implement the proposed business plan and manage the operations of the institution. Describe the extent, if any, to which directors or major stockholders are or will be involved in the day-to-day management of the institution.

4) Provide the expected compensation of the senior executive officers and the aggregate compensation of all officers.

5) Discuss the qualities desired in any remaining prospective executive officers.

6) Discuss any plans to address management succession, including any management training program or other available resources.

7) Describe any plans to provide director education or training to inexperienced bank directors.

B. Conflicts of Interest and Management Interlocks[34]

1) Describe the extent, if any, that there will be transactions with affiliated entities or individuals.

2) Describe any potential conflict of interest or management interlock that could occur with the establishment of the institution.

VI. Community Service and Community Reinvestment Act

Note: This section should be bound separately. It does not apply to certain special focus institutions, such as uninsured trust banks, cash management banks, and bankers' banks. Special features of other institutions may affect their CRA descriptions. If an institution will offer only a narrow product line, such as credit card or motor vehicle loans, to a regional or broader market, this discussion should be focused as appropriate for that limited type of operation, and a formal request for designation as a limited purpose institution should be included in the charter application.

A. Summarize the evaluation of each proposed assessment area's financial needs, including its consumer, business, nonprofit, civic, and government sectors.

B. Describe the programs, products, and activities to be offered that respond to the identified banking needs of the areas, including low- and moderate-income, and that are consistent with safe and sound operation.

C. Describe how the institution helps and/or will help to meet the existing or anticipated credit needs of its CRA[35] assessment area(s).

D. Discuss how the institution will attract and maintain community support for its long-term success.

[34] See 12 CFR 26.
[35] See 12 CFR 25.

E. Discuss the evaluation method under which the institution's performance will be assessed.

VII. Records, Systems, and Controls

A. Describe the institution's current and/or proposed accounting and internal control systems, indicating any use of electronic processing systems.

B. Discuss management's proposed independent, risk monitoring systems, including internal and external audit activities, loan review program, and compliance management program.

C. State plans for an annual audit by independent public accountants.

D. Discuss the Internet systems and security.

1) Information systems. Outline the proposed or existing information systems architecture and any proposed changes or upgrades. This plan need not include a description of the institution's entire data architecture, but it should include a detailed outline of the systems or system alternatives (or proposed vendor or vendor alternatives). The information should be sufficient to convince the OCC that:

- The operation will work within existing technology.
- The operation is suitable to the type of business in which the institution will engage.
- The security software and procedures will be sufficient to protect the institution from unauthorized tampering or access.
- The organizers and directors have given sufficient thought to the entire technology plan.

2) Provide lists or descriptions of the primary systems and flowcharts of the general processes. The level of detail in these system descriptions should be sufficient to enable verification of the cost projections in the pro formas with respect to reasonable practices and market prices.

3) Security—physical and logical components. Describe the system's internal and external access, discuss the technologies used, and the key elements for the security controls, internal controls, and audit procedures.

4) Describe the process and controls that will be followed to verify and authenticate electronic banking customers.

Note: Prior to opening, the examiners will need a more detailed description of the institution's information system architecture when the exam team reviews its implementation. In addition, before implementation, the institution must undergo a successful comprehensive security review by an objective and qualified source, including adequacy of protection against unauthorized external access. The exam team's review will include an evaluation of internal system policies and procedures as well as a review of any testing conducted on the system, e.g., penetration testing or other such tests of system vulnerability to unauthorized access. Independent tests should cover general and environmental controls as well as audit, monitoring, and balancing controls. Independent testing will provide an objective opinion on the adequacy of these controls.[36]

[36] Prior to final approval, the bank should have a security program in place that complies with the minimum security guidelines the federal banking agencies published pursuant to 15 USC 6801, 6805(b). After opening, 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 exposure. The bank should then adjust the security program as necessary before introducing the new technology-intensive product, service, or other activity.

VIII. Financial Management Plan

A. Capital Adequacy

1) Discuss capital goals and the means to achieve these goals. Discuss the formula or basis used to arrive at the proposed capital structure.

2) Discuss the adequacy of the proposed capital structure relative to internal and external risks, planned operational and financial assumptions, and projected organization and operating expenses. Present thorough justification to support proposed capital, including any off-balance-sheet activities contemplated.

3) Discuss the plan for raising capital initially and for financing growth, with particular emphasis on conformance with regulatory capital requirements.

4) Describe any plans for the payment of dividends.

B. Liquidity

Discuss the institution's plan to manage its liquidity risk, including funding sources (deposits, borrowings, securitizations). Include holding company support, if any.

C. Interest Rate Risk Management

1) Discuss the advantages and disadvantages of the proposed asset/liability mix, including a net interest margin analysis and any actions that will be taken to reduce major risks through appropriate funds management techniques and systems.

2) Discuss the institution's current and/or proposed asset and liability portfolio in terms of sensitivity to interest rate changes and the impact of earnings, capital, and net portfolio value. When available, compare this with the exposure limits that management set.

3) Describe any plans to use hedging activities (futures, options, interest rate swaps, derivative instruments, etc.)

D. Borrowings

1) Describe any plans to borrow funds from other financial institutions or sources, including the amount, composition, interest rate, maturity, and purpose.

2) Describe the debt service requirements for any debt that will be issued at the holding company level to capitalize the institution.

E. Other

1) Discuss the use of options, warrants, and/or other benefits associated with the proposed capital.

2) If applicable, discuss any plans to grow through merger or acquisition activity, including, at a minimum, the effect on staffing, physical space needs, capital, operating systems capability and compatibility, and management.

IX. Monitoring and Revising Plan

A. Describe how the board of directors will monitor adherence to the business plan.

B. Describe how the board of directors will adjust and amend the plan to accommodate significant or material economic changes.

X. Alternative Business Strategy

The institution must develop a comprehensive alternative business strategy detailing how it will operate under scenarios in which market conditions differ significantly from those projected in this business

plan. This alternative business strategy should be realistic about the business risks and incorporate sound management of such risks. This alternative strategy must consider potential adverse scenarios relating to the asset or liability mixes, interest rates, operating expenses, marketing costs, and growth rates. This discussion should include realistic plans for how the bank would access additional capital, if needed, in the future and, if applicable, contingency funding plans that address strategies for managing potential liquidity fluctuations. This plan also should discuss any financial safeguards to offset unexpected costs and to remain well capitalized.

Periodically, the institution should update this section, especially as the institution becomes more complex and as the industry conditions change.

XI. Financial Projections

A. Provide financial information for opening day pro forma and quarterly projections for the first three years of operations following the anticipated opening of the institution. The line items in the financial statements should be consistent with the Consolidated Reports of Condition and Income (Call Report),[37] so projected items may be compared conveniently with actual performance. However, Call Report items may be grouped into categories. The financial statements should be presented in two ways: (1) showing the dollar amounts, and (2) as a percentage of total assets.

1) Describe in detail all the assumptions used to prepare the projected statements, including the assumed interest rate scenario for each interest earning asset and interest costing liability over the term of the business plan.

2) Provide the basis for the assumptions used for noninterest income and noninterest expense.

[37] See FDIC's Web site, http://www.fdic.gov/regulations/resources/call/crinst/callinst.html.

3) Indicate the amount of lease expense, capital improvements, and furniture, fixtures, and equipment, including systems and equipment upgrades.

4) Describe the assumptions for the start-up costs, volumes, expected returns, and expected time frame to introduce each new product and service.

5) Describe the methodology used to determine allowance for loan and lease losses.

B. Discuss how marketing studies or surveys were used to support the projected growth of the institution. In addition, discuss the level of marketing expenses necessary to achieve the level of projected market share for both loan and deposit products. Assumptions should be consistent with those experienced by other institutions in the target market. Significant variances between the assumptions in the target market should be explained.

C. Using the Alternative Business Strategy, provide a sensitivity analysis on the financial projections. For example, if the strategy indicates that interest rates will rise and the asset/liability mix will be changed, detail the effects of the adverse scenarios in the interest rate environment or asset/liability mix. Provide the following financial statements:

Projected Balance Sheet (Schedule RC)

Projected Income Statement (Schedule RI)

Regulatory Capital Schedule (Schedule RI-A)

Appendix B: OCC Contacts

General Information

Office of the Comptroller of the Currency
250 E Street, SW
Washington, DC 20219-0001

Telephone	(202) 874-5060
Internet site	http://www.occ.treas.gov

Licensing Department

Telephone	(202) 874-5060
Fax Number	(202) 874-5293
Internet	HQ.Licensing@occ.treas.gov

Processes corporate applications from all national bank subsidiaries of certain holding companies assigned to the Washington, DC, licensing unit, and applications involving novel, complex, or precedent-setting issues. Also responsible for oversight of district Licensing staff and development and implementation of licensing policies.

Bank Activities and Structure Division

Telephone	(202) 874-5300
FAX	(202) 874-5322

Responsible for legal issues, including chartering of new banks, change in control, activities of banks and their subsidiaries, and branching.

Communications Division

Telephone	(202) 874-4700
Subscriptions	(202) 874-4960
Fax Number	(202) 874-5263
Fax-on-demand	(202) 479-0141

Provides publications support and information services. Includes responding to inquiries from the public about the agency's mission and activities, operating and overseeing the Public Information Room, which offers access to OCC public documents, and processing all initial requests filed under the Freedom of Information and Privacy Acts.

Community and Consumer Law Division

Telephone (202) 874-5750
Fax Number (202) 874-5322

Responsible for community and consumer legal issues, including community reinvestment and community development (CD) matters.

Community and Consumer Policy Department

Telephone (202) 874-4428
Fax Number (202) 874-5221

Responsible for community and consumer policy issues, including CRA and designation of limited purpose banks under 12 CFR 25.

Assistant Chief Counsel (Electronic Banking Law)

Telephone (202)874-5200
Fax Number (202)874-5374

Responsible for electronic banking legal issues.

Securities and Corporate Practices Division

Telephone (202) 874-5210
Fax Number (202) 874-5279

Responsible for securities, fiduciary, and insurance legal issues, as well as corporate governance and shareholder rights.

OCC District Offices

Northeastern

Licensing Manager
1114 Avenue of the Americas, Suite 3900
New York, New York 10036-7780

Telephone	(212) 790-4055
Fax Number	(212) 790-4098

Supervises most national banks headquartered in Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Puerto Rico, Rhode Island, Vermont, and the Virgin Islands.

Southeastern

Licensing Manager
Marquis One Tower, Suite 600
245 Peachtree Center Ave., NE
Atlanta, Georgia 30303-1223

Telephone	(404) 588-4525
Fax Number	(404) 588-4532

Supervises most national banks headquartered in Alabama, Florida, Georgia, Mississippi, North Carolina, South Carolina, Tennessee, Virginia, and West Virginia.

Central

Licensing Manager
One Financial Place, Suite 2700
440 South LaSalle Street
Chicago, Illinois 60605-1073

Telephone	(312) 663-8084
Fax Number	(312) 435-0951

Supervises most national banks headquartered in Illinois, Indiana, Kentucky, Michigan, Ohio, and Wisconsin.

Midwestern

Licensing Manager
2345 Grand Boulevard, Suite 700
Kansas City, Missouri 64108-2683

Telephone	(816) 556-1860
Fax Number	(816) 556-1892

Supervises most national banks headquartered in Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, and South Dakota.

Southwestern

Licensing Manager
1600 Lincoln Plaza
500 North Akard Street
Dallas, Texas 75201-3342

Telephone	(214) 720-7052
Fax Number	(214) 720-7068

Supervises most national banks headquartered in Arkansas, Louisiana, Oklahoma, and Texas.

Western

Licensing Manager
50 Fremont Street, Suite 3900
San Francisco, California 94105-2292

Telephone	(415) 545-5916
Fax Number	(415) 545-5925

Supervises most national banks headquartered in Alaska, Arizona, California, Colorado, Guam, Hawaii, Idaho, Montana, New Mexico, Nevada, Northern Mariana Islands, Oregon, Washington, Wyoming, and Utah.

Appendix C: Internet Banking Risks[38]

Internet banking creates new risk control challenges for national banks. From a supervisory perspective, risk is the potential that events, expected or unexpected, may have an adverse impact on the bank's earnings or capital. The OCC has defined nine categories of risk for bank supervision purposes. The risks are credit, interest rate, liquidity, price, foreign exchange, transaction, compliance, strategic, and reputation. These categories are not mutually exclusive and all of these risks are associated with Internet banking.

Credit Risk

Credit risk is the risk to earnings or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise to perform as agreed. Credit risk is found in all activities where success depends on counterparty, issuer, or borrower performance. It arises any time bank funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether on or off the banks balance sheet.

Internet banking provides the opportunity for banks to expand their geographic range. Customers can reach a given institution from literally anywhere in the world. In dealing with customers over the Internet, absent any personal contact, it is challenging for institutions to verify the bonafides of their customers, which is an important element in making sound credit decisions. Verifying collateral and perfecting security agreements also can be challenging with out-of-area borrowers. Unless properly managed, Internet banking could lead to a concentration in out-of-area credits or credits within a single industry. Moreover, the question of which state's or country's laws control an Internet relationship is still developing.

Effective management of a portfolio of loans obtained through the Internet requires that the board and management understand and control the bank's lending risk profile and credit culture. They must assure that effective policies, processes, and practices are in place to control the risk associated

[38] Excerpt from the *Comptroller's Handbook,* Internet Banking, pages 5-13.

with such loans. *See* the "Loan Portfolio Management," booklet of the *Comptroller's Handbook* for a more complete discussion of credit risk.

Interest Rate Risk

Interest rate risk is the risk to earnings or capital arising from movements in interest rates. From an economic perspective, a bank focuses on the sensitivity of the value of its assets, liabilities and revenues to changes in interest rates. Interest rate risk arises from differences between the timing of rate changes and the timing of cash flows (repricing risk); from changing rate relationships among different yield curves affecting bank activities (basis risk); from changing rate relationships across the spectrum of maturities (yield curve risk); and from interest-related options embedded in bank products (options risk). Evaluation of interest rate risk must consider the impact of complex, illiquid hedging strategies or products, and also the potential impact that changes in interest rates will have on fee income. In those situations where trading is separately managed, this refers to structural positions and not trading portfolios.

Internet banking can attract deposits, loans, and other relationships from a larger pool of possible customers than other forms of marketing. Greater access to customers who primarily seek the best rate or term reinforces the need for managers to maintain appropriate asset/liability management systems, including the ability to react quickly to changing market conditions.

Liquidity Risk

Liquidity risk is the risk to earnings or capital arising from a bank's inability to meet its obligations when they come due, without incurring unacceptable losses. Liquidity risk includes the inability to manage unplanned changes in funding sources. Liquidity risk also arises from the failure to recognize or address changes in market conditions affecting the ability of the bank to liquidate assets quickly and with minimal loss in value.

Internet banking can increase deposit volatility from customers who maintain accounts solely on the basis of rate or terms. Asset/liability and loan portfolio management systems should be appropriate for products offered through Internet banking. Increased monitoring of liquidity and changes in deposits and loans may be warranted depending on the volume and nature of Internet account activities.

Price Risk

Price risk is the risk to earnings or capital arising from changes in the value of traded portfolios of financial instruments. This risk arises from market making, dealing, and position taking in interest rate, foreign exchange, equity, and commodities markets.

Banks may be exposed to price risk if they create or expand deposit brokering, loan sales, or securitization programs as a result of Internet banking activities. Appropriate management systems should be maintained to monitor, measure, and manage price risk if assets are actively traded.

Foreign Exchange Risk

Foreign exchange risk is present when a loan or portfolio of loans is denominated in a foreign currency or is funded by borrowings in another currency. In some cases, banks will enter into multi-currency credit commitments that permit borrowers to select the currency they prefer to use in each rollover period. Foreign exchange risk can be intensified by political, social, or economic developments. The consequences can be unfavorable if one of the currencies involved becomes subject to stringent exchange controls or is subject to wide exchange-rate fluctuations. Foreign exchange risk is discussed in more detail in the "Foreign Exchange," booklet of the *Comptroller's Handbook*.

Banks may be exposed to foreign exchange risk if they accept deposits from non-U.S. residents or create accounts denominated in currencies other than U.S. dollars. Appropriate systems should be developed if banks engage in these activities.

Transaction Risk

Transaction risk is the current and prospective risk to earnings and capital arising from fraud, error, and the inability to deliver products or services, maintain a competitive position, and manage information. Transaction risk is evident in each product and service offered and encompasses product

development and delivery, transaction processing, systems development, computing systems, complexity of products and services, and the internal control environment.

A high level of transaction risk may exist with Internet banking products, particularly if those lines of business are not adequately planned, implemented, and monitored. Banks that offer financial products and services through the Internet must be able to meet their customers' expectations. Banks must also ensure they have the right product mix and capacity to deliver accurate, timely, and reliable services to develop a high level of confidence in their brand name. Customers who do business over the Internet are likely to have little tolerance for errors or omissions from financial institutions that do not have sophisticated internal controls to manage their Internet banking business. Likewise, customers will expect continuous availability of the product and Web pages that are easy to navigate.

Software to support various Internet banking functions is provided to the customer from a variety of sources. Banks may support customers using customer-acquired or bank-supplied browsers or personal financial manager (PFM) software. Good communications between banks and their customers will help manage expectations on the compatibility of various PFM software products.

Attacks or intrusion attempts on banks' computer and network systems are a major concern. Studies show that systems are more vulnerable to internal attacks than external, because internal system users have knowledge of the system and access. Banks should have sound preventive and detective controls to protect their Internet banking systems from exploitation both internally and externally. *See* OCC Bulletin 99-9, "Infrastructure Threats from Cyber-Terrorists" for additional information.

Contingency and business resumption planning is necessary for banks to be sure that they can deliver products and services in the event of adverse circumstances. Internet banking products connected to a robust network may actually make this easier because back up capabilities can be spread over a wide geographic area. For example, if the main server is inoperable, the network could automatically reroute traffic to a back up server in a different geographical location. Security issues should be considered when the

institution develops its contingency and business resumption plans. In such situations, security and internal controls at the back-up location should be as sophisticated as those at the primary processing site. High levels of system availability will be a key expectation of customers and will likely differentiate success levels among financial institutions on the Internet.

National banks that offer bill presentment and payment will need a process to settle transactions between the bank, its customers, and external parties. In addition to transaction risk, settlement failures could adversely affect reputation, liquidity, and credit risk.

Compliance Risk

Compliance risk is the risk to earnings or capital arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, or ethical standards. Compliance risk also arises in situations where the laws or rules governing certain bank products or activities of the bank's clients may be ambiguous or untested. Compliance risk exposes the institution to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance risk can lead to a diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential, and lack of contract enforceability.

Most Internet banking customers will continue to use other bank delivery channels. Accordingly, national banks will need to make certain that their disclosures on Internet banking channels, including Web sites, remain synchronized with other delivery channels to ensure the delivery of a consistent and accurate message to customers.

Federal consumer protection laws and regulations, including CRA and Fair Lending, are applicable to electronic financial services operations including Internet banking. Moreover, it is important for national banks to be familiar with the regulations that permit electronic delivery of disclosures/notices versus those that require traditional hard copy notification. National banks should carefully review and monitor all requirements applicable to electronic products and services and ensure they comply with evolving statutory and regulatory requirements.

Advertising and record-keeping requirements also apply to banks' Web sites and to the products and services offered. Advertisements should clearly and conspicuously display the FDIC insurance notice, where applicable, so customers can readily determine whether a product or service is insured. Regular monitoring of bank Web sites will help ensure compliance with applicable laws, rules, and regulations. *See* the "Consumer Compliance Examination" booklet of the *Comptroller's Handbook*, OCC Bulletin 94-13, "Nondeposit Investment Sales Examination Procedures," and OCC Bulletin 98-31, "Guidance on Electronic Financial Services and Consumer Compliance" for more information.

Application of Bank Secrecy Act (BSA) requirements to cyberbanking products and services is critical. The anonymity of banking over the Internet poses a challenge in adhering to BSA standards. Banks planning to allow the establishment of new accounts over the Internet should have rigorous account opening standards. Also, the bank should set up a control system to identify unusual or suspicious activities and, when appropriate, file suspicious activity reports (SARs).

The BSA funds transfer rules also apply to funds transfers or transmittals performed over the Internet when transactions exceed $3,000 and do not meet one of the exceptions. The rules require banks to ensure that customers provide all the required information before accepting transfer instructions. The record keeping requirements imposed by the rules allow banks to retain written or electronic records of the information.

The Office of Foreign Asset Control (OFAC) administers laws that impose economic sanctions against foreign nations and individuals. This includes blocking accounts and other assets and prohibiting financial transactions. Internet banking businesses must comply with OFAC requirements. A bank needs to collect enough information to identify customers and determine whether a particular transaction is prohibited under OFAC rules. *See* the *FFIEC Information Systems Examination Handbook* (*IS Handbook*) for a discussion of OFAC.

Strategic Risk

Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of

decisions, or lack of responsiveness to industry changes. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities. The organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental changes.

Management must understand the risks associated with Internet banking before they make a decision to develop a particular class of business. In some cases, banks may offer new products and services via the Internet. It is important that management understand the risks and ramifications of these decisions. Sufficient levels of technology and MIS are necessary to support such a business venture. Because many banks will compete with financial institutions beyond their existing trade area, those engaging in Internet banking must have a strong link between the technology employed and the bank's strategic planning process.

Before introducing a Internet banking product, management should consider whether the product and technology are consistent with tangible business objectives in the bank's strategic plan. The bank also should consider whether adequate expertise and resources are available to identify, monitor, and control risk in the Internet banking business. The planning and decision making process should focus on how a specific business need is met by the Internet banking product, rather than focusing on the product as an independent objective. The bank's technology experts, along with its marketing and operational executives, should contribute to the decision making and planning process. They should ensure that the plan is consistent with the overall business objectives of the bank and is within the bank's risk tolerance. New technologies, especially the Internet, could bring about rapid changes in competitive forces. Accordingly, the strategic vision should determine the way the Internet banking product line is designed, implemented, and monitored.

Reputation Risk

Reputation risk is the current and prospective impact on earnings and capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services or continue servicing existing relationships. This risk may expose the institution to litigation, financial loss, or a decline in its customer base. Reputation risk exposure is present throughout the organization and includes the responsibility to exercise an abundance of caution in dealing with customers and the community.

A bank's reputation can suffer if it fails to deliver on marketing claims or to provide accurate, timely services. This can include failing to adequately meet customer credit needs, providing unreliable or inefficient delivery systems, untimely responses to customer inquiries, or violations of customer privacy expectations.

A bank's reputation can be damaged by Internet banking services that are poorly executed or otherwise alienate customers and the public. Well designed marketing, including disclosures, is one way to educate potential customers and help limit reputation risk. Customers must understand what they can reasonably expect from a product or service and what special risks and benefits they incur when using the system. As such, marketing concepts need to be coordinated closely with adequate disclosure statements. A national bank should not market the bank's Internet banking system based on features or attributes the system does not have. The marketing program must present the product fairly and accurately.

National banks should carefully consider how connections to third parties are presented on their Web sites. Hypertext links are often used to enable a customer to link to a third party. Such links may reflect an endorsement of the third party's products or services in the eyes of the customer. It should be clear to the customer when they have left the bank's Web site so that there is no confusion about the provider of the specific products and services offered or the security and privacy standards that apply. Similarly, adequate disclosures must be made so that customers can distinguish between insured and non-insured products.

National banks need to be sure that their business continuity plans include the Internet banking business. Regular testing of the business continuity plan,

including communications strategies with the press and public, will help the bank ensure it can respond effectively and promptly to any adverse customer or media reactions.

Glossary

Authentication — The process that assures the receiver of a digital message of the identity of the sender. It is used to validate the integrity of the message. Secondly, it is the process of proving the claimed identity of an individual user, machine, software component, or any other entity.

Business Resumption Contingency Plan — A plan that addresses all critical services and operations that are provided by internal departments and external sources. The process that reviews the various departments, units, or functions and assesses each area's importance for the viability of the organization and providing customer services. Plans are developed to cover restoring critical areas should they be affected by physical disasters, such as fires or flooding; environmental disasters, such as power or telecommunication failure; or other disasters.

Browser — A computer program that enables the user to retrieve information that has been made publicly available on the Internet; also that permits multimedia (graphics) applications on the World Wide Web.

Consumer — One who obtains products or services from a financial institution to be used primarily for personal, family, or household purposes.

Co-operative content — Placing information from and/or interactivity with the bank and at least one other business in the same page view. Does not include interactivity that consists solely of links to another entity (changing the entire page view to present a page view from another entity).

Disaster Recovery Plan — This plan is a part of the business resumption plan. It includes protection against physical disasters and other disruptions to operations; backup considerations related to hardware, software, applications, documentation, procedures, data files, and telecommunication; and insurance policies regardless of the type of computer equipment and software, and size of the information systems facilities within the organization.

Due diligence — The process of investigation by a potential buyer of a product's or service's claimed and actual financial value and operational performance.

Electronic purse or wallet — A stored value device that can be used to make purchases from more than one vendor.

Feasibility analysis — The process of determining the likelihood that a proposal will fulfill specified objectives.

Financial subsidiary — Any company controlled by one or more insured depository institutions, other than a subsidiary that engages solely in activities that a national bank may engage in directly (i.e., operating subsidiary or bank service company). A financial subsidiary may engage in specified activities that are financial in nature or incidental to financial activities if the bank and the subsidiary meet certain requirements and comply with stated safeguards.

Firewall — A system or combination of hardware and software solutions that enforces a boundary between two or more networks.

Hypertext — Electronic documents that present information that is not sequential but is organized so that related items of information are connected.

Internet — A worldwide network of computer networks (commonly referred to as the information superhighway).

Internet banking — Systems that enable bank customers to access accounts and general information on bank products and services through a personal computer (PC) or other intelligent device.

Internet service provider — An entity that provides access and/or service related to the Internet, generally for a fee.

Linking — Creation of a place on the page view (text, graphic, hot spot, etc.) where clicking or otherwise activating the place changes the entire page view.

Organization costs — The direct costs incurred to incorporate and charter a bank. Such direct costs include, but are not limited to, professional (e.g., legal, accounting, and consulting) fees and printing costs related directly to the chartering or incorporation process, filing fees paid to chartering authorities, and the cost of economic impact studies.

Organizers — The persons who filed and signed the charter application. Organizing directors may be added during the organization phase, if their Interagency Biographical and Financial Reports are filed with the OCC and receive no objection. Those directors also become "organizers."

Organizing group — Five or more persons acting on their own behalf, or serving as representatives of a sponsoring holding company, who apply to the OCC for a national bank charter.

Page view — What is seen in the browser.

PC banking — Computer hardware, software, and telecommunication systems that enable retail customers to access both specific account and general bank information on bank products and services through a personal computer (PC). The bank's network design and telecommunication links may include the use of private networks (e.g., direct dial-in using leased or dedicated telephone lines) or public networks (e.g., the Internet).

Penetration testing — Using automated tools to determine a network's vulnerability to unauthorized access.

Portal — Page views that consistently identify the bank as the provider or sponsor of the page view, and provide a navigation system to change all or part of the page view's content while maintaining an identification with the provider/sponsor. An example is a virtual mall.

Private labeling — Creation of page views that present, by implication or otherwise, that the content and interactivity is with the bank and not some other entity, or that the service or product is provided by or on behalf of the bank. A portal can be, but is not necessarily, private labeling.

Server — 1) A computer dedicated to servicing requests for resources from other computers on a network. Servers typically run network operating

systems. 2) A computer that provides services to another computer (the client).

Small bank — A bank that has total assets of less than $250 million as of December 31 of either of the prior two calendar years and independent or affiliated with a holding company that had total bank and thrift assets of less than $1 billion as of December 31 of either of the prior two calendar years.

Sponsor — Persons currently affiliated with other depository institutions; persons who are collectively experienced in banking and have demonstrated the ability to work together, or a proposed or existing bank holding company applying to form a *de novo* national bank.

Start-up activities — Start-up activities are defined broadly as those one-time activities related to opening a new facility, introducing a new product or service, conducting business in a new territory, conducting business with a new class of customer, or commencing some new operation. Start-up activities include activities related to organizing a new entity, such as a new bank, the costs of which are commonly referred to as organization costs.

Stored value cards — Cards that store prepaid value by magnetic strip or computer chip that can be spent or transferred to persons and/or merchants similar to spending currency or coins.

Web page — Information presented through a Web browser in a single view.

Web site — A Web page or set of Web pages designed, presented, and linked together to form a logical information resource and/or transaction initiation function.

References

Affiliate Transactions

Laws	12 USC 371c (Section 23A), 371c-1 (Section 23B)
Regulation	12 CFR 31, 250.250
Other	Interpretive Letter No. 667, October 12, 1994; OCC Conditional Approval Letters No. 202, April 25, 1996; No. 383, April 13, 2000

Bank Enterprise Act

Law	12 USC 1834a
Regulation	12 CFR 1806

Bank Holding Company Act

Laws	12 USC 1841 et seq.
Regulation	12 CFR 225

Bank Secrecy/Anti-Money Laundering Act

Laws	18 USC 1818(s), 1829(b), 1951, 1959 31 USC 5311 et seq.
Regulations	31 CFR 103 12 CFR 21
Issuance	AL 2000-8, 2000-3, 98-4 Comptroller's Handbook, Bank Secrecy Act

Branches

Law	12 USC 36
Regulations	12 CFR 5.30, 7.1003
Issuance	OCC 98-2

Business Resumption

Issuance	OCC 97-23, BC 177

Capital Adequacy

Regulation	12 CFR 3

Certification Authority Systems

Issuance	OCC 99-20

Change in Bank Control Act

Law	12 USC 1817(j)
Regulation	12 CFR 5.50

Community Development Financial Institutions

Laws	12 USC 4701 et seq.
Regulation	12 CFR 1805

Community Development Investments

Law	12 USC 24(11)
Regulation	12 CFR 24

Community Reinvestment Act

Laws	12 USC 2901 et seq.
Regulation	12 CFR 25
Issuance	OCC 2000-15; Comptroller's Handbook, Community Reinvestment Act Examination Procedures

Conflicts of Interest

Issuance	Comptroller's Handbook, "Conflicts of Interest"

Corporate Decisions

Laws	12 USC 27, 93a, 1818(b), 12 USC 1831o(e)(4)
Regulation	12 CFR 5.13

Corporate Practices

Regulations	12 CFR 7.2000 et al.

Dividends

Law	12 USC 60

Regulations	12 CFR 5.63, 5.64, 5.65, 5.66
Issuance	OCC 94-41

Electronic Delivery

Regulation	12 CFR 7.1019
Issuances	FFIEC IS Examination Handbook, Volume 1 OCC Alert 2000-09

Electronic Disclosures

Issuance	OCC 99-35

Electronic Financial Services and Consumer Compliance, Guidance on

Issuance	OCC 98-31
Other	FTC paper, "Dot Com Disclosures: Information about Online Advertising"

Electronic Signatures

Law	Public Law 106-229

Equal Credit Opportunity Act

Laws	15 USC 1691 et seq.
Regulation	12 CFR 202
Issuance	Comptroller's Handbook, Fair Lending

Examination Guidance

Issuance	PPM 5400-9 OCC 99-3 FFIEC Information Systems Examination Handbook, 1996

Fair Credit Reporting

Issuance	Comptroller's Handbook, Fair Credit Reporting
Advisory Letter	AL 99-3

Fair Housing Act

Laws	42 USC 3601 et seq.
Regulation	24 CFR 100
Issuance	Comptroller's Handbook, Fair Lending

Federal Deposit Insurance Act

Laws	12 USC 1811 et seq.
Regulation	12 CFR 303

Federal Reserve Act

Laws	12 USC 221 et seq.

Finder Authority

Regulation	12 CFR 7.1002

Fraud, Computer-related

Law	18 USC 1030
Issuance	AL 97-9

Gramm-Leach-Bliley Act

Laws	Public Law 106-102, 15 USC 6801, 12 USC 24a
Regulation	12 CFR 5.39

Insider Activities

Laws	12 USC 375, 375a, 375b, 376
Regulations	12 CFR 31, 215
Issuances	*Comptroller's Corporate Manual*, "Investment in Bank Premises" *Comptroller's Handbook*, "Insider Activities"

Interest Rate Risk

Issuances	OCC 96-36, *Comptroller's Handbook*, "Capital and Dividends," "Interest Rate Risk"

Internal and External Audit

Regulations	12 CFR 9, 30, 363, 17 CFR 210, 228, 229, 240
Issuance	OCC 98-1, *Comptroller's Handbook*, *"Internal and External Audits"*

Interstate Branching

Law	12 USC 36
Regulation	12 CFR 5.30

Misrepresentations or Omissions

Law	18 USC 1001

National Bank Act

Laws	12 USC 1 et seq.

Personal Identification Number

Advisory Letter	AL 91-4

Privacy

Law	15 USC 6801
Regulation	12 CFR 40
Issuance	OCC 2000-25
Advisory Letter	AL 99-6

Privacy, Children's Online

Law	15 USC 6501
Regulation	16 CFR 312
Issuance	OCC 2000-25

Public File Availability

Regulation	12 CFR 5.9

Publication Requirement and Comment

Regulations	12 CFR 5.8, 5.10

Real Estate Settlement Procedures

Law	12 USC 2601 et seq.
Regulation	24 CFR 3500
Issuance	Comptroller's Handbook, Real Estate Settlement Procedures

Safety and Soundness Standards (Security)

Regulation	12 CFR 30

Securities

Regulations	12 CFR 11, 16

Sharing Space and Employees

Regulation	12 CFR 7.3001

Small Business Investment Companies (SBICs)

Laws	15 USC 681 et seq.

Software Accounting

Issuance	OCC 98-29

Stock Ownership of Director

Law	12 USC 72
Regulation	12 CFR 7.2005

Stored Value Card Systems

Law	12 USC 24(Seventh)
Issuance	OCC 96-48

Supervisory Policies and Procedures

Issuance	PPM 5400-9

Technology Risk Management

Issuances	OCC 98-3, OCC 98-31, OCC 98-38, OCC 99-9, OCC 2000-14, Banking Circular 226, Banking Circular 229, *Comptroller's Handbook,* "Internet Banking"