2000

Cyberbanking: Legal and Regulatory Considerations for Banking Organizations

John L. Douglas

Follow this and additional works at: http://scholarship.law.unc.edu/ncbi

Part of the Banking and Finance Law Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/ncbi/vol4/iss1/6

This Article is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Banking Institute by an authorized administrator of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
CYBERBANKING: LEGAL AND REGULATORY
CONSIDERATIONS FOR BANKING
ORGANIZATIONS

JOHN L. DOUGLAS†

TABLE OF CONTENTS

I. Introduction ........................................................................ 59
II. Offering Electronic Banking Services ..................................... 60
   A. Basic Authority .............................................................. 60
      1. National Banks ..................................................... 60
      2. State Banks ............................................................ 61
      3. Federal Reserve ..................................................... 62
   B. Supervisory Concerns ..................................................... 63
      1. No Specific Prior Approval Requirements, but Prior
         Discussion Advised .................................................. 63
      2. Identification of Risks .............................................. 64
         a. OCC Technology Risk Guidance ............................. 64
         b. FRB SR 98-9 ....................................................... 67
      3. FDIC Electronic Banking Safety and
         Soundness Procedures ............................................ 69
      4. OCC's Comptroller's Handbook on Internet Banking .............. 73
      5. Security ................................................................. 75
         a. Cyber-Terrorists vs. Infrastructure .......................... 75
         b. Information Security for Networks .......................... 77
         c. FDIC FIL 68-9 ..................................................... 78

† Partner, Alston & Bird LLP, Atlanta, GA/Washington DC; B.A., 1972, Davidson
College; J.D., 1977, University of Georgia.
C. Compliance................................................................. 79
   1. Compliance Issues for Advertising and
      Information Only Systems................................. 80
   2. Compliance Issue for On-Line
      Depository Services........................................ 81
         a. Disclosures Generally.............................. 81
         b. Need for an Account Agreement............ 82
         c. Need to Know Your Customer .............. 83
         d. Electronic Funds Transfers ................ 84
         e. Truth in Savings................................. 85
         f. Expedited Funds Availability.............. 86
         g. Regulation D Reserve
            Requirements........................................ 87
   3. Compliance Issues for Lending and
      Leasing Services........................................ 87
         a. Truth in Lending.................................. 88
         b. Equal Credit Opportunity Act ......... 89
         c. Fair Housing Act................................. 90
         d. Home Mortgage Disclosure Act....... 90
         e. Fair Credit Reporting Act................. 91
   4. Compliance Issues for Non-Deposit
      Investment Products.................................... 92

   A. Electronic Money............................................... 94
      1. Deposit Insurance................................... 96
      2. Electronic Funds Transfers...................... 97
      3. Reserve Requirements.............................. 97
      4. Escheat Statutes..................................... 98
   B. Bill Payment and Presentment............................... 98
   C. Digital Signatures and Certificate Authority............ 99
   D. Internet Service Provider.................................. 100
   E. Software Design and Development.......................... 101
   F. Information Processing...................................... 102
   G. The Problem of the Impermissible Incidental
      Activity..................................................... 102
      1. OCC..................................................... 103
         a. Excess Capacity................................. 103
         b. Insignificant Part of Permissible
I. INTRODUCTION

There is no doubt that technology has transformed the banking industry. It has allowed the development of an incredible array of new products and services. It has permitted gathering, sorting and using information in novel ways. It has radically modified the cost equation of providing products and services. It
allows a new form of convenience, as customers can access banking information, products and services, as well as a multitude of other items, from the convenience of their homes or businesses, without ever having to enter the bank's premises.

This discussion will address the issue of electronic banking – the business of allowing individual consumers to access and use banking information, products and services via personal computer. It will do so from the perspective of the banking organization itself: the regulatory, legal and structural considerations that affect how the bank engages in these activities. It will explore the permissible limits of cyberbanking – the extent to which the banking organization may involve itself in technology-related activities as part of its banking business. The primary focus will be on the banking agencies – the OCC, the Federal Reserve and the FDIC, rather than the OTS.

This discussion is, of course, a work in progress. The regulatory and legal environment changes as rapidly as the Internet changes. Just as it transforms the business of selling books or cars or music, it has transformed the business of selling loans, deposit services and the like. It presents special challenges and special opportunities. One of those challenges, however, is dealing with the impact of a legal and regulatory environment that was designed for a world of paper documents and pen and ink signatures, a world where there were branches on corners and loan officers sitting in offices. These are not part of the world of cyberbanking.

II. THE BASICS: THE ABILITY TO OFFER BANKING PRODUCTS AND SERVICES ELECTRONICALLY

A. Basic Authority

1. National Banks.

The National Bank Act permits national banks to exercise "all such incidental powers as shall be necessary to carry on the
business of banking." As defined over the years, the powers of national banks have been broadly construed to allow a huge range of banking, financial and related activities.

In its revision to its regulatory interpretations in 1997, the OCC added specific authority to engage in electronic banking activities. The revision provides as follows:

**Furnishing of products and services by electronic means and facilities.** A national bank may perform, provide, or deliver through electronic means and facilities any activity, function, product, or service that it is otherwise authorized to perform, provide, or deliver. A national bank may also, in order to optimize the use of the bank's resources, market and sell to third parties electronic capacities acquired or developed by the bank in good faith for banking purposes.²

While there would appear to be little remarkable about the declaration, it should eliminate a substantial amount of interplay and interaction with the OCC about the permissibility of various electronic banking activities. The OCC has issued a significant number of letters to financial institutions in which it has confirmed this basic power. For example, the OCC has allowed twelve national banks to create Integrion Financial Network, a venture designed to offer home banking and related services over the Internet and through the use of other electronic devices.³

2. State Banks - FDIC's Section 24 Authority

State bank powers generally derive from state law, subject

---

to the overlay of federal statutes that can provide important constraints. Of particular importance is Section 24 of the Federal Deposit Insurance Act,\(^4\) which was added in 1991 as part of the Federal Deposit Insurance Corporation Improvement Act. It permits state-chartered banks to engage in any activity that is permissible for national banks as principal, unless the FDIC determines that the activity would pose a threat to the insurance fund. Accordingly, in the electronic banking arena, the OCC precedents on bank-permissible activities generally define the parameters of permissible state bank activities.

Many states also have so-called "wild card" statutes, pursuant to which state chartered banks may exercise powers granted national banks, even where no specific statutory authority is contained in the state statute.

From time to time there may be no particular OCC precedent with respect to a particular activity. The OCC has entertained requests for interpretive rulings from state chartered banks as to whether an activity would be permissible for a national bank. As an example, a state chartered bank went to the OCC to obtain a ruling that acting as an Internet service provider was a permissible adjunct to a home banking service.\(^5\)

3. Federal Reserve

The Federal Reserve has no chartering authority, and its statutes generally do not provide enabling powers to the banks it regulates. Such powers are derived from the statutes of the state chartering authority. The Federal Reserve, however, has in other circumstances approved electronic banking activities for financial institutions. These precedents provide broad comfort that the performance of traditional banking activities through electronic means is permissible.\(^6\) The Federal Reserve supervisory releases

---

discussed below demonstrate the Federal Reserve's general support for electronic banking as a permissible activity.

B. Supervisory Concerns

Just because the activity is permissible does not mean that the regulatory bodies are not concerned about how the activity is conducted. The regulators have gone to great lengths to provide guidance and direction to financial institutions seeking to offer banking products and services over the Internet.

1. No Specific Prior Approval Requirements, But Prior Discussion Advised

Unless an institution is engaging in an activity that would otherwise require approval, none of the agencies will require prior approval for an existing bank to commence electronic banking activities. This is in contrast to the OTS requirement that before a savings and loan association commences a "transactional" banking service over the Internet, thirty days' prior notice to the agency is required. However, even though no prior notice or approval is required by the banking agencies, banks are advised to notify and consult with their primary federal regulator prior to commencing significant activities. Not only will the regulators be appreciative of the prior notice, they often have useful information and experience to impart. Of particular usefulness will be the agencies' perspectives on risks and pitfalls.

Prior approval will be required to establish a new bank that will engage in electronic banking, to establish an operating subsidiary to participate in a technology venture or for a bank holding company to acquire more than five percent of a company engaged in permissible technology or electronic banking activities. These approval requirements are driven, however, not by the technology or electronic banking nature of the activity, but rather by the general statutory and regulatory requirements ap-

---

applicable to new bank charters, operating subsidiaries or holding company investments.

2. Identification of Risks

The explosion of technology in the financial services industry has resulted in a wealth of new services and efficiencies. Unfortunately, along with these opportunities have come a variety of new risks. Identifying and managing these new risks has become the newest challenge for financial institutions and their regulators.

a. OCC Technology Risk Guidance

OCC Bulletin 98-3, Technology Risk Management Guidance for Bankers and Examiners, was intended to provide guidance for national banks concerning how they should identify, measure, monitor and control the risks associated with the use of technology. For purposes of this Bulletin, the OCC defines technology as "the tools and systems that are used to store, receive, transmit, process and recover information" including, but not limited to, computer hardware and software, and telecommunications links.

Bulletin 98-3 addresses two main issues. First, it outlines the primary risks related to the use of technology by banks. Second, the Bulletin describes a risk management process designed to minimize these risks.

With respect to technology-related risks, the OCC stated that although banks using technology-related products, services, delivery channels and processes could potentially be exposed to all of the nine categories of risk discussed in the OCC's "supervision by risk" framework, they should be particularly concerned with transaction, strategic, reputation, and compliance risks.

Transaction risk is the risk to a financial institution's earn-
ings or capital arising from problems with the institution’s delivery of services. There are countless ways in which technology may result in transaction risk. For instance, incompatible internal and external systems may prevent delivery of services and, therefore, create transaction risk for the financial institution. Transaction risk may be magnified if banks use outside vendors to perform services such as loan underwriting or credit scoring as the bank may not have the ability to adequately monitor the third-party’s use of technology. Insufficient internal controls, security measures, contingency planning or auditing policies may also lead to transaction risk.

Strategic risk is the risk to a financial institution’s earnings or capital caused by ineffective planning or decision making related to future business goals. Strategic risk may arise when management deploys technology without adequate knowledge and skills, when the technology does not suit customer needs, or when the technology is unreliable.

Reputation risk is, as the name suggests, risk to a financial institution’s earnings or capital stemming from negative public opinion. Reputation problems are not only detrimental to the financial institution in the present but will likely injure the institution’s ability to establish future relationships or successfully offer new services. Technology may contribute to an institution’s reputation risk in a variety of ways. For example, security breaches revealing confidential customer information, disruption of services, or even simple consumer fear (such as that surrounding the Year 2000) can potentially turn public opinion against an institution.

The final risk that directly relates to a financial institution’s use of technology is compliance risk. Compliance risk is risk to a financial institution’s earnings or capital resulting from non-compliance with legal and regulatory requirements. Non-compliance may subject an institution to fines, civil money penalties, damages, and the voiding of contracts. In terms of technology, compliance risk may arise from the fact that banking laws were largely designed for paper-based transactions and have not entirely evolved to address electronic transactions.

The OCC has recognized the risks that confront banks to-
day, particularly in relation to their use of technology. In this re-
spect, the OCC has explained that along with banks' increased
reliance on technology comes an increased responsibility for un-
derstanding how specific technologies operate and how their use
or failure may expose banks to risk. The OCC has stated that it
will review a bank's technology-related risks together with its
other risks in order to determine the bank's overall risk profile
within the context of the OCC's "supervision by risk" frame-
work.

A bank that is implementing new technology should, ac-
cording to the OCC, "engage in a rigorous analytic process" to
identify and quantify technology-related risks and, to the extent
possible, establish controls to manage risk exposure. Simply put,
banks need to develop risk management programs. With this
goal in mind, OCC Bulletin 98-3 proposes a technology-related
risk management process. The three-step process requires a bank
to: (1) plan for its use of technology; (2) decide how it will imple-
ment the technology; and (3) measure and monitor its risk taking.
These three elements should be the foundation of any technol-
ogy-related risk management process, regardless of the size of
the institution.

The first element of the risk management process is plan-
ing. According to the OCC, effective planning includes: (1) in-
volving the board of directors and senior management in
decision-making throughout the planning process; (2) gathering
and analyzing relevant information regarding new and existing
technologies; and (3) assessing needs and reviewing relevant op-
tions.

The second consideration in the risk management process
concerns the implementation of new technology. Proper imple-
mentation includes bank use of appropriate internal controls
such as clear and measurable goals, and the allocation of specific
responsibilities to specific personnel. Additionally, proper im-
plementation includes having policies and procedures to manage
risk related to the bank's use of technology, to ensure that key
employees and vendors have the expertise and training to handle
new technology, and to thoroughly test new technology systems
and products. Finally, proper implementation includes contin-
gency planning designed to reduce bank vulnerability to system failures, unauthorized intrusions, and other problems.

The third step in the OCC's suggested risk management process requires the bank to ensure that its measurement and monitoring efforts effectively identify ways to manage risk exposure. The OCC will evaluate the bank's auditing and quality assurance programs to determine whether the institution's measurement and monitoring policies are sufficient.

b. FRB SR 98-9

In April 1998, the Federal Reserve published SR 98-9 in order to provide its examiners with guidance in evaluating the effectiveness of a financial institution's ability to manage the risks associated with information technology. Information technology refers to a combination of computer hardware and software telecommunications, and information. Much like OCC Bulletin 98-3, SR 98-9 recognized the increasing role that technology played in all levels of a financial institution's operations and information processing. The increasing role of technology also created a source of new risk, as evidenced by the concerns surrounding the Year 2000. The goal of the Federal Reserve was essentially to adapt its risk-focused supervisory process to the changing role of information technology.

Unlike OCC Bulletin 98-3, which proposed a specific risk management process, the Federal Reserve in SR 98-9 set forth five "information technology elements" to be evaluated in terms of the overall business risks of the financial institution. Essentially, examiners were to consider the effect that the five elements would have on the risks (including credit, market, liquidity, operational, legal, and reputational risks) confronting a particular financial institution.

The five information technology elements to be considered by Federal Reserve examiners were management processes, architec-
ture, integrity, security, and availability. The first element, management processes, broadly encompasses planning, investment, development, execution, and staffing of information technology programs. Examples of management processes include strategic planning, management succession policies, and regular independent audits. With regard to this first element, Federal Reserve examiners are to consider not only whether the information technology strategies of the organization are consistent with the organization’s mission and business objectives, but also whether the organization has the appropriate management processes in place to execute those information technology strategies.

Architecture, the second information technology element, refers to the underlying design of the automated information system and its component parts such as network communications, hardware, and software. Effective architecture meets both the current and long-term business objectives and capacity requirements of the organization. Additionally, the architecture must provide solutions to compatibility and integration problems with other systems and sources of data.

The third element is integrity. This refers to the reliability, accuracy, and completeness of the information delivered to the end-user. Integrity may become a concern, for instance, in the situation where a bank’s loan division mistakenly inputs erroneous entries into its general ledger system resulting in billing errors and similar problems. Organizations may consider implementing information system audits and independent application reviews to safeguard the integrity of its information.

Security, the fourth information technology element, essentially refers to an organization’s ability to prevent unauthorized access, modification, destruction, or disclosure of information assets during their creation, transmission, processing, maintenance, or storage. Examiners are to evaluate whether the organization’s operating procedures and controls are commensurate with the potential for and risk associated with such security breaches.

The final information technology element discussed by the Federal Reserve in SR 98-9 is availability. Availability relates to the delivery of information to end-users. Information technology has effective availability when information is regularly delivered
to the end user on a timely basis. A secondary aspect of availability concerns whether an organization has contingency plans in place to limit disruptions caused by human error or intervention, natural disaster, or utility or communications failures. The five somewhat ill-defined elements set forth in SR 98-9 are intended to be flexible tools to facilitate consideration of the risks associated with information technology. To be most useful, these elements need to be incorporated into an effective risk management process.

3. FDIC's Electronic Banking Safety and Soundness Examination Procedures

Historically, banks and other financial institutions have provided limited electronic capabilities in the form of phone banking, ATMs, and automated clearing-house systems. New technology, however, has resulted in a vast array of electronic capabilities ranging from elaborate computer networks to informational and transactional web sites to electronic bill payment systems.

The FDIC has segregated these new electronic capabilities, particularly bank web sites, into three categories based on their degree of functionality and interactivity.11 Level I systems are those "Information-Only Systems" which allow access to basic marketing and publicly available information, as well as the transmission of non-sensitive electronic mail. In Level I systems, the publisher, usually the bank, is communicating information that historically would have been made available through print or similar media. These systems present the least risk to financial institutions with respect to security breaches and other failures and are, therefore, subject to the least stringent FDIC examinations.

Level II systems, "Electronic Information Transfer Systems," are interactive in that they allow the transmission of sensi-

tive messages, documents, or files between financial institutions and their clients. This category includes systems that allow sensitive or confidential electronic mail between banks and customers, data or files to be downloaded by customers from a bank’s network, and bank web sites that permit customers to submit online loan or deposit account applications. Level II systems are subject to more significant examinations than are Level I systems.

Level III systems, “Fully Transactional Information Systems,” are those that allow Level I and Level II activities as well as online account information, fund transfers between accounts, and electronic bill payment among other things. Level III systems are subject to the most thorough FDIC examination procedures.

Clearly, developing technology has improved the opportunities available to financial institutions. Unfortunately, along with these opportunities have come a variety of new risks. Some risks are obvious such as the possibility of newly deployed technology quickly becoming obsolete. By contrast, technology-related risks may also be unexpected such as the risk that new technology will not suit the demands of consumers. Some technology-related incidents may be particularly dangerous for financial institutions given their highly interconnected computer systems. For instance, system attacks, either internal or external, may be undertaken to disrupt services, access databases and information resources, or for purposes of financial gain. These attacks may even be motivated simply by the challenge of overcoming a bank’s security systems. Another technology-related problem facing financial institutions is the possible failure of one or more participants in a payment system or outsourcing arrangement. The consequences of such a failure could quickly extend beyond the failing party resulting in reputation damage and lost confidence on a much broader scale.

In response to these technology-related risks, the FDIC has emphasized the need to develop effective risk management programs. Risk management is the ongoing process of identifying, measuring, monitoring, and managing potential risk exposure. In particular, the FDIC has identified three general areas where financial institutions should focus their risk management efforts.
First, they should undertake *general supervision* including planning and analysis, policies and procedures, accountability and authority, regulatory and legal compliance, human resources, and auditing. Second, financial institutions need to consider *transaction processing* matters such as authentication, information integrity, and data confidentiality. Finally, financial institutions need to generally consider *system administration* such as resource requirements, system security, system reliability, outsourcing policies, and contingency planning.

Even beyond these general risk management considerations, there are several risk management techniques that have specific relevance to electronic banking. Management should incorporate these techniques into its overall risk management program. They include *strategic planning and feasibility analysis, incident response and preparedness, and internal routines and controls*.

The importance of strategic planning and feasibility analysis cannot be overstated as they relate to electronic banking. Strategic planning is the ongoing process of evolving and adapting an organization’s mission and business objectives. Feasibility analysis, although similar, involves decisions concerning specific proposals as opposed to overall organizational goals. Feasibility analysis entails the determination of whether a specific proposal will satisfy a given business objective. When completing a feasibility study, a particular proposal or opportunity should be considered in three stages: (1) *study*, during which needs and objectives are analyzed, and alternatives are developed based on performance specifications; (2) *design and development*, during which the best solution is identified based on technical specifications, the system is installed, policies and procedures are developed, and documentation is completed; and (3) *operation*, during which the system is operated and maintained. With respect to the electronic capabilities of financial institutions, these strategic planning and feasibility analysis decisions are of particular importance because of the significant investment and risks that may accompany the deployment of a new technology. Consequently, it is imperative that management, including the board of directors and other senior officers, is fully informed of the opportunities and risks related to the deployment of new technology.
Once a new technology has been set up, ongoing reviews will be necessary to evaluate the performance of the technology against strategic and operational objectives.

Beyond preventing problems through strategic planning and feasibility analysis, a second function of an effective risk management program is to respond to situations promptly in order to limit their negative effects. Quick response is of even greater importance in an era of high-speed technology and interdependent computer systems where a small problem has potential to balloon quickly. Development of an effective incident response policy should begin by assessing the risks posed to each system; it should determine the importance and sensitivity of all systems, applications and data sources. Additionally, the incident response policy should identify and prepare key personnel whose expertise will be necessary to respond quickly and decisively to a situation. These individuals should then be empowered with the authority to respond during an incident. Another component of an effective incident response policy is an institution's backup systems. Ideally, these backups will limit the effects of any disruption on essential systems or information resources.

The final essential element of any technology-related risk management program is an effective system of internal routines and controls. Because financial institutions are especially vulnerable to failures of and attacks on their computer systems, an effective risk management program must incorporate a system of internal controls to protect hardware, software, information resources, and electronic transmissions. One key internal control is an effective security program including physical and system access controls such as on-site security, system passwords, firewalls, encryption, and intrusion detection systems. Audit procedures are also vital to any internal control system. The final component of the internal control system involves educating personnel as to the importance of adhering to this system of controls.
In October 1999, the OCC published a specialized booklet as part of its Comptroller’s Handbook that deals solely with Internet Banking. This booklet is, in some respects, very similar to earlier FDIC and OCC publications in that it categorizes the various types of Internet banking, discusses the nine varieties of risk confronting banks in relation to their Internet banking activities, and sets forth a three step risk management process. In other respects, however, the Internet Banking booklet differs from earlier publications in the level of detail with which it addresses internal control systems, in-house development versus outsourcing of Internet services, and other issues concerning public confidence in Internet banking.

The Comptroller’s Handbook defines “Internet Banking” as the systems that enable bank customers to access accounts and general information on bank products and services through a personal computer or other intelligent device. Internet banking services include everything from wholesale wire transfers and automated clearinghouse transactions to retail services such as balance inquiry, funds transfer, and bill presentment and payment. As with many other areas of society, the Internet has brought about revolutionary changes in the business of banking.

Several factors are driving the enormous growth of Internet banking. In particular, the chief factor pushing the increasing use of Internet technology has been competitive pressure. Banks must offer Internet services or lose their customers to the competition. Another factor that has spurred the growth of Internet banking has been the significant cost efficiencies of this new technology. While the cost of delivering the average manual banking transaction is more than one dollar, the cost of the average Internet transaction is about a penny. An additional driving factor has been the geographic reach of the Internet.

As mentioned above, the Comptroller's Handbook breaks down Internet banking into three categories, similar to those discussed in the FDIC's *Electronic Banking Safety and Soundness Examination Procedures*. The Handbook classifies banks Internet service offerings as informational, communicative, or transactional based on their level of functionality and interactivity. As the level of interactivity increases so does the risk of security breaches and the need for internal control systems.

The *Internet Banking* booklet also discusses the risks facing banks offering Internet services. It generally defines risk as the potential that events, either expected or unexpected, may have an adverse impact on the earnings or capital of a bank. The OCC advises that all nine categories of risk (credit, compliance, foreign exchange, interest rate, liquidity, price, reputation, transaction, and strategic) are associated with Internet banking activities. To minimize these risks, the OCC refers banks to the three step risk management process discussed in Bulletin 98-3, *Technology Risk Management*.

Inextricably tied to risk management processes are internal controls. Internal control systems related to Internet banking services should be commensurate with the level of risk presented by the services. The required internal controls will depend on the objectives of the bank and the types of Internet services offered. It is the duty of bank management to determine the bank's goals and objectives with respect to its Internet banking offerings and then to establish a system of internal controls sufficient to ensure that the goals and objectives are met.

The *Internet Banking* booklet also addressed the decision whether banks should offer in-house or outsourced Internet banking services. This decision depends on several considerations. Of particular importance are the size and resources of the bank. Larger banks with substantial resources may choose to purchase the necessary hardware and software to offer Internet banking. This will allow those banks the greatest ability to customize their product offerings. On the other hand, it may be more cost effective for smaller institutions to simply have someone else offer these services on their behalf. It is important to remember, however, that even if the service is handled by an
outside vendor, the bank is still responsible for monitoring the security, reliability and general performance of the service vendor. Therefore, should a bank choose to outsource its Internet services, it should enter into a formal service agreement with the vendor that clearly establishes all of the rights and responsibilities of the parties.

The final segment of the OCC's Internet Banking booklet discusses several issues relating to consumer and business confidence in Internet banking. Public confidence is, obviously, essential to the success of Internet banking. With this in mind, banks must employ policies, procedures and technology directed at easing consumer apprehension. Specifically, banks need to address consumer concerns including: security, authentication, trust, non-repudiation, privacy, and availability.

5. Security

A primary fear in electronic commerce is the underlying security of the system. In the cyberworld, there are no originals. Duplicates are generally an identical match of the electronic impulses or 0's and 1's that constitute the original. Data and information, stored in such form, is subject to manipulation or destruction, either intentionally or unintentionally. Where banks and money are concerned, the importance of security is even greater. The regulators recognize the risk and not only strongly encourage banks to address the risk, but also focus on it strongly during the examination and evaluation process.

a. Cyber-Terrorists vs. Infrastructure

OCC Bulletin 99-9, Infrastructure Threats from Cyber-Terrorists, discusses the threat to financial institutions and the general infrastructure of our society (including telecommunications, energy, banking and finance, transportation, utilities, and emergency services) presented by Cyber-terrorists. The Bulletin

13. See OCC 99-9, Infrastructure Threats from Cyber-Terrorists (March 5, 1999),
defines Cyber-terrorism as “the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.” It can take a variety of forms including commercial espionage or employee sabotage. Cyber-terrorism can be a single catastrophic attack or a series of coordinated but seemingly independent attacks.

Historically, the most significant threats to the computer security of financial institutions came from internal attacks by disgruntled employees. Today, however, the threat has become far broader with the advent of the Internet and our more highly automated society. While technological advances have resulted in increased efficiency and improved service, they have also made our infrastructures increasingly automated and interdependent. Consequently, the destruction or debilitation of public utilities, for instance, could result in the cascading destruction of our banking and finance systems. It is these types of problems which the OCC intended to address in Bulletin 99-9.

With respect to external attacks, the OCC emphasizes the need for banks to install strong intrusion detection systems capable of detecting and recording attempts to break into their computer systems. Additionally, the OCC stresses the importance of reporting suspected cyber-crimes and computer intrusions to the FBI Computer Crimes unit and to the Suspicious Activity Reporting System in order to allow the detection of patterns or related incidents.

Regarding internal attacks, the OCC suggests that banks implement a physical security program that limits access to computing and information resources. As an additional layer of protection, the OCC recommends the use of user IDs, passwords, anti-virus programs, and monitoring of computer and Internet usage.

The OCC’s final advice relates to indirect damage to banks resulting from attacks on other parts of the infrastructure. In particular, the OCC advises the use of back-up plans and contingency plans to reduce disruptions caused by failures in other
areas of the infrastructure.

b. *Information Security for Networks*

In 1996, the Federal Reserve, after interviewing a cross-section of financial institutions, securities firms, CPA firms, and other industry related firms, published SR 97-32 outlining what it considered to be prudent and effective security measures related to computer networks. These measures were designed to protect information and ensure its integrity, availability, and confidentiality.

SR 97–32 emphasized several key points. First, the Federal Reserve stressed the need for a strong information security program establishing the necessary structure and accountability to manage risks and foster awareness of the importance of information security. An effective information security program should involve active board and management oversight, established policies and procedures, measurement and monitoring systems, and a system of internal controls.

Like OCC Bulletin 99-9, the Federal Reserve's SR 97-32 also discussed the vulnerability of internal network systems. The paper suggested that internal attacks could potentially be the most damaging to a financial institution as the institution's own personnel, including consultants as well as employees, may have authorized access to critical information and computer resources. To limits these problems, the Federal Reserve suggested the use of background checks of information technology personnel such as system administrators, telecommunications support staff, system programmers and any other personnel with access to sensitive information.

The Federal Reserve also suggested that organizations should encrypt confidential information, particularly data intended to be transmitted over public networks. The paper warned that even "dedicated" or "leased" lines may not provide

adequate privacy as they still use the same infrastructure as the public networks and are, therefore, still subject to the same attacks. Additionally, SR 97-32 warned institutions against having Internet sites which contain a link directly into the institution’s own internal network. Such a path may provide unauthorized individuals with a way to attack the institution’s internal network and information assets.

Finally, the paper pointed out, quite practically, that security programs designed to protect networks from security breaches may require dedication of significant resources. It is the responsibility of senior management to evaluate the costs and benefits of such programs in deciding how to best allocate the institution’s resources.

c. FDIC FIL 68-99

In July 1999, the FDIC published FIL 68-99 in an effort to provide financial institutions and examiners with background information and guidance on various risk-assessment tools and practices related to information security. The paper described the steps for establishing a sound information security policy starting with a thorough and proactive risk assessment and concluding with the creation of an ongoing security program incorporating prevention, detection, and response components.

According to the paper, an effective policy begins with an assessment of the risks confronting the organization’s information and technology resources. This process involves evaluating the threats presented by serious hackers, interested computer novices, dishonest vendors and competitors, disgruntled current or former employees, and even agents of espionage. As the FDIC pointed out, the Internet has provided a wealth of information to both banks and hackers, allowing the average Internet user to quickly find information describing how to break into an institution’s systems using known security flaws and/or software bugs. FIL 68-99 describes various mechanisms which hackers may use

to attack an institution's computer systems. Systems have been attacked using everything from stolen passwords to simple computer viruses to Trojan horse programs to Internet Protocol spoofing.

According to the FDIC, the first step in addressing these threats is to evaluate where an institution is vulnerable and then to develop a program that addresses these weaknesses. Such a program should involve three components: prevention, detection, and response. Regarding prevention, the FDIC suggests that institutions use a combination of vulnerability assessment tools that scan networks, servers, firewalls, routers, and applications for known security flaws and software bugs as well as penetration analysis tests in which independent or internal personnel attempt to break into the institution's systems. The FDIC also suggested using intrusion detection systems that essentially act as burglar alarms reporting potential attacks or intrusions to the appropriate personnel. The final requirement of a sound information security program is an incident response strategy that identifies what constitutes a break-in or system misuse, establishes procedures for reporting incidents to management, the board of directors, legal counsel, and law enforcement agents, and empowers personnel to respond to such incidents.

C. Compliance

The laws governing consumer compliance generally have not changed in recognition of the delivery of banking services over the Internet. Accordingly, banks must determine an appropriate method of dealing with consumer compliance issues when there are no paper-based documents and there is no face-to-face interaction with the customer.

It is useful to think about compliance depending upon the level of electronic activities the institution engages in. There is one set of issues when a financial institution is simply distributing information about itself or its products. There is another set if the customer is able to engage in banking transactions. There is yet a third set if the customer is able to engage in non-banking transactions, such as securities or insurance transactions. Finally,
there are additional issues if the bank merely provides "links" or access to the sites of third-parties where an array of products or services may be purchased.

1. Compliance Issues for Advertising and Information Only Systems

As a preliminary matter, it is probably appropriate to use the working assumption that virtually all web page data is advertising. It is thus proper to consider web sites that provide information as being equivalent to a pamphlet or similar product, with the advertising requirements being applicable to the entire document.

As a general matter, under both state and federal law it is illegal to engage in unfair or deceptive advertising. Accordingly, as a preliminary matter, web page data should be accurate. As an example, both the FTC and the bank regulatory agencies are concerned that privacy statements and policies accurately reflect the practices of the institution.

The home page of the bank's web site must display the official advertising statement, unless one of the exceptions to the requirement is available.\textsuperscript{16} Subsidiary web pages should also generally be thought of as advertisements, unless one of the exceptions applies. Accordingly, the words "Member FDIC" or the FDIC symbol should appear on the top level web page, and on other pages that can reasonably be considered to be advertisements. Institutions may want to consider whether the symbol should appear on other pages if there is a reasonably likelihood that parties will be entering the site through other pages, whether or not they could be considered advertising. The official bank or savings association signs\textsuperscript{17} are not required to be displayed.

The "Equal Housing Lender" logo or legend, or other permissible disclosure of non-discrimination policy, should also appear if the institution is advertising credit products that are

\textsuperscript{16} See 12 C.F.R. § 328.3 (1999).
\textsuperscript{17} See id. at § 328.2.
subject to the Fair Housing Act.\textsuperscript{18}

If there are materials describing rates on deposit accounts or loan products, the bank will need to comply with Truth in Savings and Truth in Lending obligations.

2. Compliance Issues for On-Line Depository Services

An additional layer of complexity is added when the bank begins to provide access to deposit account information and permits the customer to initiate transactions in those accounts. There are four major statutory and regulatory requirements to be addressed, the EFT Act (Reg. E), the Expedited Funds Availability Act (Reg. CC), the Truth in Savings Act (Reg. DD) and Federal Reserve requirements (Reg. D). The general focus of these regulations is on disclosures, delivery of required statements, accuracy of interest rates, notices, and error resolution.

\textit{a. Disclosures Generally}

Disclosures must be "clear and conspicuous." As this requirement is adapted to the Internet, banks must be sensitive to what a customer actually sees and how the customer sees it. Pointers and hot links may be useful methods of assuring that the customer actually views required disclosures.

The regulators are rapidly moving to the point where disclosures can be made electronically rather than in writing on physical paper so long as the customer agrees to electronic delivery. To satisfy the disclosure obligation, the disclosure must generally be capable of being viewed, downloaded and printed by

\textsuperscript{18} See id. at § 338.3(a) which states:

Any bank which directly or through third parties engages in any form of advertising of any loan for the purpose of purchasing, constructing, improving, repairing, or maintaining a dwelling or any loan secured by a dwelling shall prominently indicate in such advertisement, in a manner appropriate to the advertising medium and format utilized, that the bank makes loans without regard to race, color, religion, national origin, sex, handicap or familial status.
the customer. To assure that customers using media where printing is not possible, banks should provide a mechanism where the written disclosures can be mailed to the customer at an address to be designated by the customer.

Because the regulations on occasion require that certain disclosures be delivered at a specific time (e.g., at the time an application is delivered), the institution should assure that there is a mechanism to satisfy this requirement through mandatory links or other methods that will assure automatic presentation of required disclosures.

b. Need for an Account Agreement

As a preliminary matter, banks must assure that the customer has provided appropriate authorization to engage in online banking activities. Most banks are requiring a separate "online banking" agreement, that may be a written document maintained by the bank, or an electronic document posted on the site that the customer must "click through" and accept in order to commence the online banking activities. Whatever method is used must be sufficient to bind the customer, for online banking typically depends upon user identification numbers and passwords, and the bank must be in a position to rely upon the user of those identifiers in fulfilling transactions and requests.

The bank may also use this online account agreement to provide many of the disclosures called for under the various regulations discussed below where appropriate.¹⁹

Part of the account agreement may address the consent to the electronic delivery of notices and disclosures. It may be appropriate for the agreement to provide a mechanism for the customer to "opt out" of electronic delivery and receive paper disclosures in person or by mail.

¹⁹. As an example of an extensive account agreement and disclosure format, see Wells Fargo's online banking agreement at: <https://banking.wellsfargo.com/common/html/wibdisc.html> (visited March, 2000).
c. Need to Know Your Customer

Although the banking agencies dropped their proposed "Know Your Customer" rule in mid-1999, the underlying statutory requirements that led to the proposal are still present. The proposed rule was promulgated on December 7, 1998\textsuperscript{20} and was withdrawn on March 29, 1999,\textsuperscript{21} after the agency received over 250,000 comments in opposition to the proposed rule.

First, banks have an obligation to file Suspicious Activity Reports whenever it detects known or suspected criminal violations of federal law or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act. The reports must be filed with the appropriate law enforcement agencies and the Department of the Treasury.\textsuperscript{22}

Second, banks have an obligation to comply with the Bank Secrecy Act, which imposes strict record keeping and reporting requirements with respect to transactions in currency and monetary instruments.\textsuperscript{23}

Third, banks have a requirement not to engage in business, directly or indirectly, in property in which any person in a country embargoed by the Treasury Department's Office of Foreign Assets Control (OFAC), such as Cuba, North Korea, Iran, Iraq, Libya and Sudan, as well as any of the 2000-plus Specially Designated Nationals, has an interest. The Internet is international, almost by definition, and the bank must be sensitive regarding with whom it is doing business. Enforcement in this area is quite robust, with high civil and criminal penalties.\textsuperscript{24}

\textsuperscript{22} See, e.g., 12 C.F.R. § 353 (1999).
\textsuperscript{24} See 31 C.F.R. Chapter V (1999). For example, 31 C.F.R. 500.201(a) provides as follows:

All of the following transactions are prohibited, except as specifically authorized by the Secretary of the Treasury (or any person, agency, or instrumentality designated by him) by means of regulations, rulings, instructions, licenses, or otherwise, if either such transactions are by, or on behalf of, or pursuant to the direction of
The recent money laundering hearings involving the Bank of New York and accounts with Russian correspondent banks and companies highlight the critical need to know basic information about customers. Failure to establish systems and controls in this area could be particularly damaging to the institution.

d. Electronic Funds Transfers (Regulation E)

The Electronic Funds Transfer Act and the Federal Reserve Board's Regulation E apply whenever online banking systems provide for transactions that will debit or credit a consumer's account.

In general, Regulation E requires disclosures to be clear and readily understandable, in a form that the consumer may keep. Depository institutions may satisfy this requirement by the electronic delivery of these disclosures so long as the consumer agrees to such delivery.

When a customer signs up for new banking services, the customer must be provided with the Regulation E disclosures if the services are subject to terms and conditions different from those that have previously been properly disclosed to the customer. Accordingly, many institutions are including the Regulation E disclosures in their online account agreements or are separately providing the disclosures when the customer initiates online banking services.

27. See id. at § 205.4.
28. See id. at § 205.4(c)(2).
29. See C.F.R. Official Staff Commentary § 205.7(a)-4.
Regulation E generally provides for a receipt requirement whenever a customer initiates an electronic funds transfer at an electronic terminal. However, there are certain exceptions. As an analogous device to a telephone, receipts should not be necessary for transactions initiated by a consumer from a personal computer.

Important in connection with bill payment systems is the requirement that there be written authorization for pre-authorized transfers from a consumer's account, or that the writing be "similarly authenticated." The Official Staff Commentary specifically permits authentication through a home banking system. "To satisfy this requirements of this section, there must be some means to identify the consumer (such as a security code) and to make available a paper copy of the authorization (automatically or upon request)."

Importantly, 12 C.F.R. § 205.6 governs the limitations of the consumer's liability in connection with unauthorized transactions or loss or theft of an access device (which would include the user identification information and password). Notwithstanding the general desire to allow the bank to rely upon all transactions and instructions initiated with the consumer's identifying information, Federal law will impose limits on the customer's liability. Where customers are using online systems, the bank should be aware that notices of loss, theft or unauthorized access may occur electronically, and the bank should have systems in place to receive and act promptly upon such notices.

**e. Truth in Savings (Regulation DD)**

The Truth in Savings Act and the Federal Reserve Board's Regulation DD require financial institutions to make

---

31. See C.F.R. Official Staff Commentary § 205.2(h)-1.
32. 12 C.F.R. § 205.10(b) (1999).
33. C.F.R. Official Staff Commentary § 205.10(b)-5.
35. 12 C.F.R. § 230 (1999)
meaningful disclosures to consumers regarding the costs and interest rates paid on deposit accounts. If information about deposit products is made available, proper advertising disclosures must be made in accordance with each of the requirements of the Regulation. There is no exemption for information made available over the institution's web site.

Regulation DD contains important requirements as to the timing of certain disclosures. For example, account disclosures must be provided before an account is opened.\(^{36}\) Further, disclosures must be made "clearly and conspicuously in writing, and in a form the consumer may keep."\(^{37}\) The Federal Reserve has issued a proposed rule that would allow electronic delivery of these disclosures.\(^{38}\) The proposal contains extensive details regarding how to satisfy the timing and other requirements of Regulation DD. Until the proposal is adopted, however, the electronic disclosures will have to be supplemented by paper disclosures. A possible alternative would be electronic delivery to an email address if the recipient confirms that the email has been received and printed out. Alternatively, fax delivery should be sufficient if the recipient confirms that the fax has been received in paper form. In any event, the account should not be opened until the receipt of the written disclosure is assured.

If the web site contains account information, it should be monitored for recency, accuracy and compliance. Information should be clearly dated, and appropriate disclaimers should be placed on web site material indicating that rates may have changed, and indicating how the customer may obtain updated information.

\(f.\) Expedited Funds Availability

The Expedited Funds Availability Act and the Federal Reserve Board's Regulation CC\(^{39}\) require financial institutions to

\(^{36}\) See id. at § 230.4(a).
\(^{37}\) Id. at § 230.3(a).
comply with certain requirements with respect to the availability of funds and to make specific disclosures regarding their policies. These requirements still apply, even though the customer may be dealing with the institution electronically. As a general matter, the disclosures required by 12 C.F.R. § 229.16 as to funds availability policies must be made prior to the opening of a new account. The Federal Reserve will permit these disclosures to be made electronically if the customer agrees. The disclosure must be in textual form and must be in a form the customer may keep. Generally this requires that the disclosure be capable of being downloaded or printed. Accordingly, the institution should periodically test its site to assure that disclosures meet the requirements of this section.

g.  Regulation D (Reserve Requirements)

Regulation D\textsuperscript{41} imposes reserve requirements on accounts maintained at the institution. The actual reserve requirement depends upon the type of account. For savings and MMDA accounts which are subject to the six transaction limit, electronic withdrawals, electronic transfers or payments to third parties initiated by the depositor count against the limit.

3. Compliance Issues for Lending and Leasing Services

Providing online lending and leasing services brings into play another layer of complex regulation, and accordingly requires strict attention to the various compliance issues. Again, the most serious issues relate to disclosures. There are a series of statutes to be addressed, including the Equal Credit Opportunity Act (Reg. B),\textsuperscript{42} the Home Mortgage Disclosure Act (Reg. C),\textsuperscript{43} the Consumer Leasing Act (Reg. M),\textsuperscript{44} the Truth in Lending Act (Reg.

\textsuperscript{40} See C.F.R. Official Staff Commentary § 229.15(a)-1.
\textsuperscript{41} 12 C.F.R. § 204 (1999).
\textsuperscript{42} Id. at § 202.
\textsuperscript{43} Id. at § 203.
\textsuperscript{44} Id. at § 213.
The Truth in Lending Act\textsuperscript{50} and the Federal Reserve Board’s Regulation Z\textsuperscript{51} are designed to promote the informed use of consumer credit by requiring disclosures about the terms and costs of such credit. There are specific disclosure and related requirements for both open-end and closed end credit, all of which will come into play if the bank offers credit over the Internet. Disclosures are required in connection with advertisements\textsuperscript{52} and whenever there is a solicitation or application to provide credit.\textsuperscript{53} Importantly, advertisements include any commercial message in any medium that promotes, directly or indirectly, a credit transaction.\textsuperscript{54} “Messages inviting, offering, or otherwise announcing generally to prospective customers the availability of credit transactions whether in visual, oral, or print media, are covered by Regulation Z.”\textsuperscript{55} Web pages would clearly fall within the ambit of this description.

Disclosures are required to be provided “clearly and conspicuously in writing in a form that the consumer may keep.”\textsuperscript{56} There are important exceptions to this requirement, including certain specific disclosures for credit and charge card applications, home equity disclosures, alternative summary billing

\textsuperscript{50} The Truth in Lending Act is part of the Consumer Credit Protection Act, 15 U.S.C. 1601 (1994).

\textsuperscript{51} 12 C.F.R. § 226 (1999).

\textsuperscript{52} See id. at §§ 226.16, 226.29.

\textsuperscript{53} See id. at §§ 226.5, 226.5a, 226.5b.

\textsuperscript{54} See id. at § 226.2(a)(2).

\textsuperscript{55} C.F.R. Official Staff Commentary § 226.2(2)(a)(2)-1.

rights statements, credit and charge card renewal disclosures, and disclosures about payment requirements. These specific disclosures, while they must be clear and conspicuous and in writing, need not be in a form the consumer can keep, opening the way for their electronic disclosure. The Federal Reserve has proposed allowing electronic delivery of essentially all of the Regulation Z disclosures. The proposal contains extensive details regarding how to satisfy the timing and other requirements of Regulation Z. Until the proposal is adopted, however, the electronic disclosures (other than the exceptions noted above) will have to be supplemented by paper disclosures.

Interestingly, Regulation Z does allow electronic delivery of periodic statements if the customer agrees.

b. Equal Credit Opportunity Act
(Regulation B)

The Equal Credit Opportunity Act and the Federal Reserve Board's Regulation B are designed to promote the availability of credit for all creditworthy applicants regardless of race, color, religion, national origin, sex, marital status, or age, or certain other factors. It prohibits credit practices that discriminate on the basis of any of these factors, and imposes certain other requirements.

To the extent the online system relates to extending credit, all of the Regulation B requirements would be applicable. Of particular importance are two specific items. First, if a credit application is taken online, it constitutes a written application under 12 C.F.R. § 202.5(e), and second, if the application relates to the purchase or refinancing of a dwelling, the institution must request the specific information provided in 12 C.F.R. § 202.13 (race or national origin, sex, marital status and age). In general,

57. See 12 C.F.R. 226.5(a)(1), n.8.
online credit applications must satisfy the requirements of 12 C.F.R. § 202.5.

If the application is taken online with video capability, the application will be treated as if it were in person for the purposes of 12 C.F.R. § 202.13(b). That is, if the customer elects not to complete the requested information regarding race or national origin, the institution is to note on the form such information to the extent it is able to do so. Without video capacity, the application will be treated as if it were received by mail.

c. Fair Housing Act

As noted above, an institution that advertises online credit products that are subject to the Fair Housing Act\(^2\) must display the Equal Housing Lender logotype and legend or other permissible disclosure of its non-discrimination policy.\(^3\)

d. Home Mortgage Disclosure Act
(Regulation C)

The Home Mortgage Disclosure Act\(^4\) and the Federal Reserve Board's Regulation C\(^5\) impose data collection requirements on financial institutions designed to help determine whether institutions are serving the needs of their communities, to identify possible discriminatory lending patterns and enforce anti-discrimination statutes, and to assist public officials in distributing public-sector investments.

---

63. See 12 C.F.R. § 338.3(a) which provides as follows:

Any bank which directly or through third parties engages in any form of advertising of any loan for the purpose of purchasing, constructing, improving, repairing, or maintaining a dwelling or any loan secured by a dwelling shall prominently indicate in such advertisement, in a manner appropriate to the advertising medium and format utilized, that the bank makes loans without regard to race, color, religion, national origin, sex, handicap or familial status.

Institutions are required to collect data regarding applications for and, originations or purchases of home purchase and home improvement loans. Among other things, required data includes the type and purpose of the loan, the location of the property, the race or national origin and sex of the borrower, the gross annual income of the borrower, and the type of action taken with respect to the loan.66 Similar to the Equal Credit Opportunity Act, if applications are taken online with video capability, the applications will be treated as if they were in person for the purposes of 12 C.F.R. § 203.4(b). That is, if the customer elects not to complete the requested information regarding race or national origin, the institution is to note on the form such information to the extent it is able to do so. Without video capacity, the application will be treated as if it were received by mail.

e. The Fair Credit Reporting Act

12 U.S.C. 1681 imposes strict requirements on entities that collect, transmit and use information on consumers for the purpose of making (or allowing others to make) credit and certain other decisions. The definitional sections in the Act are of extreme importance as they define consumer report, consumer reporting agency, and the various other entities that can be brought within the scope of the act by virtue of their collection, transmission or use of consumer information.

The Fair Credit Reporting Act allows banks to gather and use their own experiential information in making credit decisions, and allows them to share certain of that information with credit reporting agencies. It also allows banks to use information from credit reporting agencies in making credit and certain other decisions, but imposes certain obligations on banks when they deny credit or access to other services or opportunities on the basis of information contained in the credit report. A bank can become a credit reporting agency and, thus, become subject to the requirements associated with maintaining accurate information

66. See id. at § 203.4.
and allowing consumers to correct erroneous information.

Recently the OCC has expressed some concern about banks withholding information from credit reporting agencies. While there is no statutory obligation for banks to share the information they may have obtained based upon direct transactions with the customer, the OCC has indicated that as accurate credit information is of benefit to the overall credit industry, it would look unfavorably upon a lender that refused to share basic information with the credit reporting agencies.

The FCRA obligations must be considered by banks when developing privacy statements for their customers. Banks will clearly want to reserve the right to share permissible experiential information with the credit reporting agencies, even though they might be willing to commit to their customers not to share information with third-party marketers.

4. Compliance Issues for Non-Deposit Investment Products

The law on the sale and delivery of non-deposit investment products is beyond the scope of this outline. However, from a banking law perspective, there are two primary requirements that should be considered whenever a bank is involved in providing information regarding non-deposit investment products through its web site.

First, there must be full disclosure of the uninsured nature of these products. The February 15, 1994, Interagency Statement on Retail Sales of Nondeposit Investment Products provides important guidance to banks with respect to offering and selling insurance and securities products to their customers. While the Statement was not drafted with the Internet offering of such products in mind, the principles contained in the Statement should properly be adapted to online advertisement and offerings.

According to the Statement:

67. (visited on March 7, 2000)
Sales activities for nondeposit investment products should ensure that customers for these products are clearly and fully informed of the nature and risks associated with these products. In particular, where nondeposit investment products are recommended or sold to retail customers, depository institutions should ensure that customers are fully informed that the products:

- are not insured by the FDIC;

- are not deposits or other obligations of the institution and are not guaranteed by the institution; and,

- are subject to investment risks, including possible loss of the principal invested.

Moreover, sales activities involving these investment products should be designed to minimize the possibility of customer confusion and to safeguard the institution from liability under the applicable anti-fraud provisions of the federal securities laws, which, among other things, prohibit materially misleading or inaccurate representations in connection with the sale of securities.

Accordingly, the notice of “not FDIC-insured, not guaranteed, possible loss of principal” should appropriately appear when the customer enters the online pages where non-insured products are discussed, and the message should be appropriately repeated when the customer reaches points at the site where “buy” or “invest” decisions are made.

Further, in order to comply with the general intent of the Statement, the pages dealing with non-insured products should be segregated from those dealing with insured deposit products. “Segregation” in this light means some appropriate separation
from the deposit pages, forcing the user to exit those pages where
deposit products are discussed and entering a new area where it
is clear that there is an entirely new subject matter. Again, the
disclosures of "not FDIC-insured, not guaranteed, possible loss of
principal" help enforce the segregation concept if delivered upon
entry into this new area.

III. BEYOND BASIC BANKING: WHAT ELSE IS PERMISSIBLE?

The OCC has been quite aggressive in defining permissible
incidents to banking. While the general OCC rule on allowing
banks to conduct any activity electronically that it could other-
wise permissibly engage in is quite broad, on a series of occa-
sions the OCC has provided specific amplification to permissible
banking activities. Many of these appear in the OCC rulings on
permissible minority investments by banks, where one of the re-
quirements is that the entity must engage only in activities per-
missible for the bank itself.

A. Electronic Money

Nothing seems quite as central to the business of banking
as handling and dealing with money. While banks have not been
in a position to issue their own currency for many years, the OCC
has exhibited a willingness to let banks create electronic money
and create and participate in various payment systems involving
such electronic money.

In general, electronic money refers to the information that
represents value that can be used for the purchase of goods or
services. A party will exchange some form of "real" money (be it
in the form of cash, check or credit card purchase) for the elec-
tronic value. At some point, the holder of the electronic value
can surrender the value for "real" money. There are a variety of
types of electronic money systems.

69. See infra discussion in Part III.A.
In an Order dated August 19, 1996, the OCC allowed Huntington Bank to invest in a stored-value/smart card system for universities, hospitals and other self-contained geographic locations. Among other things, the bank contemplated receiving and holding the funds paid for the value associated with the cards, and standing behind the obligation to redeem the cards or assure payment to parties accepting the value in transactions.

In another Order, dated December 2, 1996, the OCC allowed several banks to invest in Mondex, the electronic money product developed primarily by National Westminster Bank in England. This particular order involved the investment by four U.S. banks in Mondex, U.S.A. The proposal contemplated that the electronic money created under the system could circulate among participants until surrendered for redemption. The product hearkens back, in some ways, to the early days in this country where banks issued their own notes and such notes circulated as currency.

A more recent letter confirms that a bank may directly acquire a non-controlling, minority interest in a Delaware corporation and thereby acquire, indirectly, a non-controlling minority interest in the corporation's sole subsidiary engaged in providing stored value systems. Apparently, the request involved a bank that wished to obtain a minority interest in the Huntington stored value/smart card program mentioned above. The recent OCC letter indicated that the venture had established stored value/smart card systems for fourteen customers, including twelve universities.

On May 10, 1996, the OCC approved an investment by a bank in an entity engaged in the design, development, marketing and maintenance of a network for electronic funds transfers and electronic data interchange. The purpose, among other things,
was to facilitate and transact electronic commerce and marketing software products. Part of the activities would involve the transfer and settlement of financial obligations.\textsuperscript{73}

In a novel order, the OCC approved an application for a bank to design, build and operate and electronic toll booth. According to the OCC, the bank would serve as a focal point in transactions where money was paid and received, something within the core powers of banks.\textsuperscript{74}

The issuance of electronic money creates a series of issues under other statutes. These include issues under laws and regulations affecting deposit insurance, electronic funds transfers and Regulation E, reserve requirements and state escheat laws.

1. Deposit Insurance

In General Counsel Opinion No. 8,\textsuperscript{75} the FDIC issued a lengthy opinion discussing whether stored value card arrangements constituted accounts for which federal deposit insurance would be required. Although the technical descriptions of the various stored value card and electronic money systems is somewhat strained, the Opinion generally provides that unless the bank is creating a separate account for the customer with the intent and the ability to track the funds in that account, an insured deposit relationship is created. Systems that provide such capacity may be somewhat unusual; however, the FDIC clearly provides the flexibility to create an insured deposit relationship if desired.

If the relationship between the bank as issuer of the electronic money and the individual or entity holding the electronic money is not an insured account relationship, the holder of the electronic money would be a general unsecured creditor of the issuer. This means that if the issuer were a bank, and the bank failed, the creditor would fall behind depositors in the priority

\textsuperscript{73} OCC Interpretive Letter 732 (May 10, 1996), available in 1996 WL 413710.
\textsuperscript{74} OCC Interpretive Letter 731 (July 1, 1996), available in 1996 WL 413705.
\textsuperscript{75} FDIC, General Counsel opinion No. 8 (July 16, 1996).
scheme, and perhaps would receive less than full payment with respect to the claim.

2. Electronic Funds Transfers

Stored value systems and electronic money arrangements create issues under the Electronic Funds Transfer Act\(^6\) and Regulation E of the Federal Reserve.\(^7\) The basic issue is whether there is a consumer account created that may be accessed through electronic funds transfers. If so, there is a series of disclosure requirements, dispute resolution procedures, limitations on liability and other matters that must be dealt with.

The Federal Reserve has attempted to address how the EFT and Regulation E requirements would apply to stored value cards and electronic money systems, and until now has been unable to adopt final regulations providing guidance. In 1996, the Federal Reserve issued proposed regulations\(^8\) that would have exempted small denomination systems and imposed minimal disclosure obligations on systems dealing with larger values. The Federal Reserve has apparently recognized that applying all of the Regulation E requirements makes little sense to many of these systems, due not only to technical problems but also the realization that the provisions provide little meaningful benefit. In general, making appropriate disclosures will be of key importance.

3. Reserve Requirements

Banks should recognize that in the event they participate in electronic money systems where they will be holding funds, they will be required to deal with the reserve requirements contained in Regulation D.\(^9\) While it might theoretically be possible to structure the funds so that they are held in a time deposit or

\(^7\) 12 C.F.R. § 205 (1999).
other form of account with less than full reserve requirements, care should be taken in recognizing and dealing with the issue.

4. Escheat Statutes

Virtually every state has some form of statute requiring that unclaimed property be turned over to the state. With electronic money and stored value systems, there will inevitably be funds remaining that have not been used and have not been redeemed.

Institutions have adopted various approaches for handling the escheat issue. Certain systems impose a monthly fee, similar to an "inactive account" charge. Many electronic money systems have a security feature that provides that the funds must be used by a date certain. Certain of the issuers in such programs take the position that the electronic money system is simply the right to participate in a payment system. Accordingly, when that right "expires" there is no right to reclaim unused funds, therefore, there is nothing to be escheated to the state. It is too soon to have definitive answers on the viability of these approaches.

B. Bill Payment and Presentment

The OCC has been very supportive of banks providing bill payment and bill presentment services. In Conditional Approval 221 (December 4, 1996), the OCC allowed a group of banks to form a limited liability company that would develop and operate a platform for home banking services over the Internet. One component of the proposal was to offer bill payment services.

More recently, this same consortium entered into an arrangement with CheckFree Corporation to develop and operate a bill payment service. As part of this request, the consortium took warrants in CheckFree that, upon exercise, could permit the entity to own up to 15% of CheckFree's common stock. CheckFree, among other things, is the largest non-bank owned bill payment system.

80. OCC Conditional Approval 221, supra note 3.
services provider. The OCC has had little problem determining that bill payment services are within the permissible ambits of the business of banking.

More recently, Citibank sought approval from the OCC to invest in Transpoint, a venture with First Data Corporation and Microsoft, to provide bill payment services. The OCC approved the request in Conditional Approval 304 (March 5, 1999).82 Each of these ventures has commenced providing bill presentment services as well, where a customer may receive bills in electronic form over the Internet. The OCC approvals that have approved bill payment services are broad enough to encompass the bill presentment services as well.

C. Digital Signatures and Certificate Authority

Digital signatures are a cryptographic method of assuring the identity of parties transmitting information across the Internet and the integrity of the message transmitted. Digital signatures are designed to address two of the key problems with Internet messages, that of assuring that the party purporting to send a message is actually the party sending the message, and of assuring that the message received is actually the message sent. Digital signatures rely upon public key/private key cryptography, whereby key pairs provide the necessary assurance.

A digital certificate is like the cryptographic assurance provided by a third party that the key pairs "belong" to the designated owner, and that they have not been compromised. A certificate authority, then, is a third party that stands behind the cryptographic assurance. Banks, given their knowledge of and relationships with customers, are natural parties to provide the types of assurances.

In Conditional Approval 267 (January 12, 1998),83 the OCC

83. Conditional Approval 267, Application by Zions First National Bank, Salt
approved a request by Zions First National Bank, Salt Lake City, Utah, to establish an operating subsidiary that would act as a certification authority and repository for certificates used to verify digital signatures. The OCC easily determined that the type of service was similar to many services traditionally provided by banks on behalf of customers (signature guarantees, notary services, etc.), and determined that the services were a permissible incident to the business of banking. The OCC devoted a significant part of the letter to discussing the types of risks inherent in the proposed business and outlining its safety and soundness concerns.

More recently, Bank of America and Citibank sought approval to invest in a limited liability company through existing operating subsidiaries that would explore the creation of an operating company that would issue digital certificates, act as a signature authority, and assume some of the liability risks associated with the activity. Part of the proposal included creating operating rules, liability limits and other conditions associated with the activity. The approval did not specifically provide approval to engage in the activity, providing some indication that the OCC might like to review the overall proposal, including the liability risks, before the business became operational.84

D. Internet Service Provider

In August, 1996, the OCC indicated that acting as an Internet Service Provider ("ISP") in its community would be a permissible activity for a national bank as an incident to providing home banking services to its customers.85 The OCC relied in part upon its excess capacity interpretation,86 indicating that as the bank would need to invest and use Internet service technol-

Lake City, Utah, to Establish an Operating Subsidiary that Will Act as a Certification Authority and Repository for Certificates Used to Verify Digital Signatures (January 12, 1998), available in 1998 WL 41538.

84. See OCC Conditional Approval 301 (January 15, 1999), available in 1999 WL 74106.


ogy as part of its home banking service to its customers, it could sell that capacity to non-customers as well. Interestingly, the request, from Apollo Trust Company, was from a state bank that needed assurance that such an activity was permissible for a national bank so that it could engage in that activity as a state bank.

Similarly, in the Integrion order, the OCC allowed the venture to act as an ISP as part of the banking services that would be provided.87

In a somewhat related vein, the OCC has allowed national banks to provide Web hosting services. In Interpretive Letter 856 (March 5, 1999),88 the OCC indicated that the business of banking includes offering to merchant customers a commercially enabled retail Web site hosting service so that participating merchants can receive and process credit card orders over the Internet. While the bank is not acting as the ISP, the bank is hosting the web site of the merchant, with the intent of both allowing the bank’s customers to access the merchant, presumably from the bank’s own web pages, and allowing the merchant to access the bank’s customer base.

E. Software Design and Development

Within the permissible ambit of banking business is the design and development of software to conduct the banking activities. In OCC Interpretive Letter 756 (November 5, 1996),89 the OCC allowed a bank to purchase a minority interest in a limited liability company to be formed with an unaffiliated corporation to engage in the development, distribution and maintenance of computer software for cash management applications.

Similarly, in OCC Interpretive Letter 677 (June 28, 1995),90

87. See OCC Conditional Approval Letter 221, supra note 3.
88. Interpretive Letter 856 (March 5, 1999), available in 1999 WL 183558.
90. OCC Interpretive Letter 677, The Establishment of Operating Subsidiaries by Two National Banks to Engage Through a Joint Venture in the Development and
the OCC approved the acquisition by a group of bank of MECA, the developer of the *Managing Your Money* personal financial software.

**F. Information Processing**

Walter Wriston once described the business of banking as the business of dealing with information. The OCC has authorized banks to engage in a variety of ventures devoted to assembling, processing and transmitting information. A common thread of all of these approvals is that the predominant activity of the venture relates to financial, economic or banking information. For example, in OCC Conditional Approval 282 (July 31, 1998),\(^9\) the OCC permitted NationsBank, National Association to establish an operating subsidiary, NationsBanc Health Services, Inc., that would acquire a one-half, non-controlling equity interest in Electronic Health Services, L.L.C. The venture would capture, process and distribute information on medical reimbursements and payments and participate in the related payments flow. The venture would also make available a variety of banking products, and might under certain circumstances provide related and necessary hardware.\(^9\)

**G. The Problem of the Impermissible Incidental Activity**

Technology activities rarely fit into neat boxes, and investments and acquisitions often bring into play potentially difficult issues regarding activities that are not permissible for the bank or bank holding company. Whether the issue involves electronic games (a common problem) or some other non-financial activity,

---


92. See OCC Interpretive Letter 419, Joint Venture to Facilitate Settlement and Payment of Health Insurance Claims Through the Use of Shred EFT Technology (February 16, 1988), *available in 1988 WL 508734* (authorizing formation of a limited partnership to “develop a data processing system linking health care providers, health care insurers, health care recipients, and their respective depository institutions”).
the bank or bank holding company often needs to address whether and how to bring the activities into compliance.

1. OCC

The OCC has developed a number of theories pursuant to which incidental impermissible activities might be retained.

a. Excess Capacity

The OCC expanded a concept it had previously applied in the real estate area, pursuant to which a bank could lease excess office space to third parties. By extending the concept to the electronic arena, banks are able to market and sell excess computer capacity to third parties, regardless of the nature or type of user. The interpretive ruling reads as follows: "A national bank may also, in order to optimize the use of the bank's resources, market and sell to third parties electronic capacities acquired or developed by the bank in good faith for banking purposes."93

This concept was utilized by the OCC in approving a request of a bank to participate in a venture to market electronic imaging services. The primary targets of the venture were imaging services for banks and other financial institutions and imaging of financial data for non-financial services companies. The OCC allowed the venture to market imaging services to non-financial entities for use with non-financial data.94

b. Insignificant Part of Permissible Product Offering

The OCC has on occasion adopted another approach to impermissible activities, focusing upon the overall relationship


94. See OCC Interpretive Letter 805, Letter Concludes that the "Business of Banking" Includes 1) Electronic Imaging Services for Other Banks and Financial Institutions and 2) Electronic Imaging Services for Non-Banks if Limited to Financial Data and Documents (October 9, 1997), available in 1997 WL 751157.
between the permissible and impermissible activities. This is particularly true where the products have broader applicability than simply the permissible banking activities. For example, in OCC Conditional Approval Letter 221 (December 4, 1996), the OCC address the permissibility of providing Internet access as part of a home banking program. It noted:

Finally, the Internet access feature will be only a minor part of the entire package offered by the LLC (less than 10% of total net income) and will entail little additional expense for the LLC. Under these circumstances, we find the Internet access feature to be validly incidental to the other LLC Services.

The OCC further stated:

Full function products provided as an incidental part of a package of banking services cannot dominate the banking services being provided. See OCC Interpretive Letter No. 737, supra; OCC Interpretive Letter No. 516, supra; Letter from Michael J. O'Keefe, District Counsel, Midwestern District (July 13, 1987) (unpublished); OCC Interpretive Letter No. 345, [1986-1987 Transfer Binder] Fed. Banking L. Rep. (CCH) ¶ 77,799 (July 9, 1986). The OCC has two alternative tests for determining when sale of full function products as part of a package of banking services is "incidental" to those services. The older OCC test is whether the cost of the full function product is less than 30% of the cost of the entire package. OCC Interpretive Letter No. 742, supra. As an alternative to the cost test, a recent letter adopted a test based on the percentage of "gross profits" (sales less cost of goods sold) that is derived from the sale of the hardware. OCC Interpretive Letter No. 754, supra.

95. OCC Conditional Approval Letter 221, supra note 3.
Specifically, this letter held that where the gross profits generated by a full function product provided in connection with a banking service do not exceed thirty percent of the total gross profits from that service, the sale of the full function product is incidental to the permitted banking service.

c. *De-minimis Exceptions*

In a couple of letters the OCC has indicated that a minor amount of impermissible activities might not necessarily be fatal to the overall activity, regardless of whether it is connected to the permissible activities. For example, in OCC Interpretive Letter 677 (June 28, 1995), involving the acquisition by a group of bank of MECA, the developer of the *Managing Your Money* personal financial software. MECA had also developed gaming software. The OCC noted that it was not a significant part of the overall business of MECA, that MECA did not intend to devote further resources to it, and that it would naturally dissipate over time.

In the Integrion/CheckFree letter, the OCC indicated that there might be a "basket" available for impermissible activities. The Integrion banks sought approval to hold a non-controlling equity interest in CheckFree Corporation, and sought some assurance that if CheckFree commenced to engage in impermissible activities, immediate divestiture would not be required. The OCC gave the banks two years to accomplish divestiture were CheckFree to engage in impermissible activities, but indicated that it would consider whether immaterial impermissible activities might be allowed without requiring divestiture. It appears as if the OCC wanted to make a determination based upon the type and extent of the impermissible activities rather than making the determination in advance.97

---

96. OCC Interpretive Letter 677, *supra* note 90.
d. Divestitures

When a national bank acquires entities engaging in impermissible activities, the normal requirement is for the bank to cease engaging in that particular activity. In the context of acquiring a state chartered bank, for instance, the OCC routinely provides a two-year period in which to divest impermissible assets. In a recent approval, the OCC indicated that this two-year period would be applicable when a company in which a national bank invests commences engaging in impermissible activities.98

2. Federal Reserve Board

The Federal Reserve, of course, operates under a different statutory scheme, and thus its flexibility to address impermissible activities is different. Section 4(c)(8) of the Bank Holding Company Act99 provides, with certain exceptions, that a bank holding company may not hold or acquire more than 5% of the shares of any company not engaged in business so closely related to the business of banking or managing or controlling banks as to be a proper incident thereto. As the Federal Reserve has amplified the meaning of the statutory prohibition over the years, it has determined that data processing activities, at least insofar as the activities relate to economic, financial or banking data, are permissible activities for bank holding companies.

a. Data Processing Exemption Under Regulation Y

The Federal Reserve has long permitted bank holding companies to engage in data processing activities. In 1971, data processing was added to the list of activities deemed to be closely related to banking, and permitted the processing of banking, fi-

98. See id.
nancial or related economic data. The Board noted at the time that banks had historically performed certain types of billing and processing services for their customers, and concluded that such billing and data processing services were integrally related to the basic money transmission functions traditionally performed by banks.

In 1982, the Board expanded its data processing regulation to allow additional types of related activities. Bank holding companies were allowed to engage in processing all financial, banking or economic information, thus permitting the processing of all types of economic data without the requirement that the economic data be related to other banking or financial data. It was clear that the deletion of the term "related" was intended to be significant.

While the ability to engage in data processing activities provides critical authority to engage in a variety of technology activities, in practice the limitation that the activities be limited to banking, financial or economic data proved to be somewhat restrictive. Technology companies often do not fit into neat boxes, and companies processing permissible data often have components of their businesses that are outside the scope of the permissible limits of the prior regulation. When the Federal Reserve revised Regulation Y in 1997, it provided much needed relief by permitting a 30% "basket," pursuant to which processing activities could involve activities other than the banking, financial or economic data.

In a similar vein, the Federal Reserve had been restrictive with respect to sales of hardware as part of permissible data processing activities. In the past, the hardware either had to be special purpose hardware (e.g., hardware specifically designed for the transmission of the banking, financial or economic data) or the general purpose hardware had to be not more than 10% of

102. See Memorandum from Legal Division to the Board of Governors, August 12, 1982; Order, Citicorp (Citishare), 53 Fed. Res. Bull. 505 (1982).
the cost of a packaged offering. The revision lifted the 10% basket to 30%.104

b. Two-year divestitures

There is no statutory authority permitting a bank holding company to commence an impermissible activity and then divest the activity at some later date. There is authority in the act, under certain conditions, for a bank holding company to have a period of time to bring non-conforming activities into conformity. For example, when a company becomes a bank holding company, it has two years in which to divest or cease impermissible nonbanking activities.105 Similarly, banks that “inherit” impermissible assets as a results of debts previously contracted are allowed time to divest the assets.106

The Federal Reserve has been willing to allow bank holding companies an opportunity to divest shares of companies that they do not control if the companies commence impermissible activities.107 Under the circumstances, the Federal Reserve indicated a willingness to allow the bank up to two years to divest its ownership of shares were the entity to commence impermissible activities.

c. MECA and Paribas Orders

Two orders issued prior to the Regulation Y Revision in 1997 provide some indication that the Federal Reserve might be flexible under appropriate circumstances. On February 6, 1996, the Federal Reserve permitted The Royal Bank of Canada to acquire 20% of the voting stock of MECA Software, L.L.C. Royal Bank applied to join BankAmerica, NationsBank, Fleet, and First

104. See id. at § 225.28(b)(14)(i)(B).
106. See id. at § 1842(a) and 1843(c)(2).
Bank Systems as owners of MECA. Each of the other banks owned their respective shares of MECA through bank operating subsidiaries; Royal Bank, as a foreign bank, needed the Federal Reserve's approval under Regulation Y.

The MECA Managing Your Money software and related services easily fall within the parameters of Regulation Y. It is a computer program that allows customers to conduct basic banking functions and personal financial management using personal computers. The software, and related financial software, is marketed both to consumers and financial institutions, to allow the institutions to offer such services to their customers. From the Federal Reserve's point of view, there was no problem associated with the acquisition of at least that portion of MECA that was engaging in the financial software programs.

Importantly, MECA had also developed and marketed various non-financial software, including games, a computer security program, a medical reference library, and a program providing basic legal forms. These activities do not fall within the Regulation Y limitations. The Board, however, permitted MECA to keep, and indeed continue, these activities. MECA and the Bank indicated that the revenues from the impermissible activities were small, amounting to approximately 7% of 1994 revenues, that MECA had no intention of developing new non-financial software or to upgrade, enhance or promote its current non-financial programs, and that the non-financial portion of the company's business was expected to diminish over time. Based on the limited nature of the activity, the Board approved the acquisition and did not require the cessation or divestiture of the impermissible activities.

On February 26, the Board approved an application of Compagnie Financiere de Paribas to engage de novo in providing an integrated software program to operators of digital mobile telephone networks to perform billing and account-related services for customer accounts. The software calculates bills...

---

108. See FRB, Order Approving a Notice to Engage in Data Processing Activities (Feb. 6, 1996), available in 1996 WL 47572.
109. See FRB, Order Approving Notice to Provide Mobile Telephone Billing
based on data provided by the telephone operator, such as date, time, duration, and destination of the call, the customer's service contract, and individual account balances. The company also provides general accounting services, such as recording payments and balances, provides billing and settlement services, and generates various related reports to the operator.

Part of the services performed consist of customer identification and account information and the generation of certain reports used by the operator to detect fraud. While these functions would be performed only in connection with the data processing and billing services, they are not within the list of "banking, financial or economic" information described in Regulation Y. The Board, however, allowed the company to engage in these activities, describing them as a "relatively small part" of the operation of the company, "incidental" to the primary billing and account functions to be provided to the telephone operator.

Interestingly, and perhaps significantly, Paribas owns a majority of France Telecom, the French national telephone operating company, and owns 49.9% of Financiere Sema, a French investment company that in turn owns 41.6% of Sema Group plc, which developed the software. It was not stated whether Sema offered the product overseas. Sema proposed to establish the company as a wholly-owned U.S.-based subsidiary to sell the software described in the proposal.

These two orders were well beyond the regulatory framework in place at the time they were issued. Perhaps they were just precursors of the revision allowing the 30% basket for otherwise impermissible activities. They may indicate, however, a more pragmatic and practical outlook towards acquisitions of and investment in technology companies.110


110. See also Letter, Federal Reserve Bank of New York (Royal Bank of Canada/Integrion/CheckFree, 1999).
IV. JOINT VENTURES AND SIMILAR ARRANGEMENTS: EXPLOITING THE TECHNOLOGY PROWESS OF OTHERS

A. Operating Subsidiaries and Minority Investments – National Banks

1. Operating Subsidiaries

Both the Comptroller of the Currency and every state regulator will permit a bank to establish an operating subsidiary. An operating subsidiary is a subsidiary of the bank established to engage in activities which the bank itself could engage in directly. The decision to engage in bank-permissible activities through subsidiaries is viewed as a corporate and strategic decision. While banks do conduct a wide variety of fairly mundane activities through operating subsidiaries, they have become the vehicles for some of the most interesting developments in the expansion of products and services, particularly joint activities with non-bank entities.

Establishing an operating subsidiary generally requires the approval of the bank's chartering authority, either the OCC for national banks or the state for state banks. There is no separate approval required from the Federal Reserve or the FDIC for a state bank to establish an operating subsidiary. There are two important caveats to this latter statement, however. First, the Federal Reserve does take the position that without prior approval, a state bank subsidiary of a bank holding company may not acquire less than all of the shares of a subsidiary company engaged in activities permissible for the parent bank without prior approval under Section 4 of the Bank Holding Company Act.111

The OCC has recently revised its rules for establishing op-

erating subsidiaries in part 5 of its regulations. The regulation previously required that the parent bank own at least 80% of the voting stock of the subsidiary. That requirement has been reduced to 50%. The revision provides that certain types of activities may be conducted in subsidiaries without the need for any notice to the OCC. An after the fact notice is sufficient for well-capitalized, well-managed institutions. Other banks must generally go through a notice or approval process, and this process will be applied to all banks with respect to certain types of activities. The OCC may condition its approval of an operating subsidiary.\textsuperscript{112}

No notice or approval from the OCC is required for an operating subsidiary if the activities are limited to those previously approved for an operating subsidiary of the bank, those activities continue to be legally permissible, and the activities are conducted in accordance with any previously imposed conditions.

The OCC's regulations generally require that the operating subsidiary must limit its activities to those permissible for the bank, and will be subject to the same examination and supervision as the parent bank. The revised regulations hold out the possibility that an operating subsidiary might not need to limit its activities precisely to those permissible for the bank, and indicate that the subsidiary need not necessarily be supervised and examined as a bank. Various orders of the OCC indicate that compliance even with the 50% requirement is not mandatory, and that various ventures are permissible through operating subsidiaries which, while not impermissible for a bank to engage in, are in practical terms unlikely to be subject to bank-like supervision and regulation.

The OCC's regulations speak in terms of subsidiary corporations. The OCC has approved a bank's participation in an operating subsidiary structured as a limited liability company, and has allowed a bank to be a limited partner in a partnership. The OCC can not approve a bank becoming a general partner in a partnership, due to concerns relating to the unlimited liability of

\textsuperscript{112} See id. at § 5.34.
a partner, but it has allowed a bank to establish a corporate subsidiary to serve as the general partner of a partnership.

Depending upon the activity, the OCC may impose limitations on a bank's investment in an operating subsidiary. Such limitations are typically imposed when the bank is engaging in activities perceived to be risky or where there is substantial participation by non-affiliated entities. "Investment" includes both the direct equity investment in the operating subsidiary as well as any loans or extensions of credit to or for the benefit of the subsidiary. The common limitation is 5% of assets.

The OCC has indicated that it will consider on a case by case basis whether an operating subsidiary might engage in activities which, while closely related to banking, are not within the ambit of legal or permissible activities. The bank would have to establish a number of safeguards to insulate itself from any liability or exposure to the activities of the subsidiary, and the OCC would have to satisfy itself that there are no legal or policy reasons why the activity could not be conducted in the subsidiary. At this point, the only activity the OCC has approved under this authority is the underwriting and dealing in municipal revenue bonds, an activity closely related to traditional bank activities, but impermissible for national banks under provisions of the National Bank Act. The earliest approval was of a request by Zions Bank, OCC Conditional Approval 262 (December 11, 1997). There have been three subsequent approvals. There have been no technology or electronic commerce requests, although there is no reason why such a request could not be made or approved.

2. Minority Investments

Of much more interest, perhaps, and unquestionably the subject of more regulatory attention, is the issue of the minority investment. The minority investment allows the bank to participate in ventures with technology companies and others where the parties are each bringing substantial expertise and assets to the venture, but the bank will not be the controlling owner. Commencing in about 1995, the OCC adopted a series of straightforward rules for determining whether the investment would be permissible.

A national bank may engage in activities that are part of or incidental to the business of banking by means of an operating subsidiary.116 In a variety of circumstances the OCC has permitted national banks to own, either directly or indirectly through an operating subsidiary, a minority interest in an enterprise. The OCC has concluded that such minority investments are permitted in the event four criteria are satisfied. These standards are as follows:

a. The activities are limited to those that are part of, or incidental to, the business of banking.

The OCC's analysis of the business of banking has been broad and expansive. Many of the Interpretive Letters and Conditional Approvals referenced in Part II above were issued in the context of minority investments.

b. The investing bank must be able to prevent the enterprise from engaging in activities that are not part of or incidental to the business of banking, or must be able to withdraw their investment.

The bank is generally able to satisfy this requirement in one of several ways. Generally, the governing documents of the venture will limit the activities of the venture to activities that are bank permissible. As the venture lacks the power to engage in impermissible activities, the OCC is comforted. Alternatively, special voting rights may be given the bank investor to veto or block any attempt to engage in impermissible activities. Finally, the bank, if it is unable to prevent the venture from engaging in impermissible activities, must be able to exit the venture.

c. The liability of the bank must be limited, as a legal and accounting matter, and the bank must not have open-ended liability for the obligations of the enterprise

A primary concern of the OCC is that national banks should not be subjected to undue risk. Where the investing bank will not control the operations of the entity in which the bank holds an interest, it is important that a bank's investment not expose it to unlimited liability. It is relatively easy to satisfy this standard through the use of corporate entities or other forms of organization with limited shareholder liability. Perhaps the most common structure for many of the ventures is the Delaware limited liability company, providing statutory protection for shareholders as well as potential pass-through tax treatment.

In assessing a bank’s loss exposure as an accounting matter, the OCC has previously noted that the appropriate account-

117. See, e.g., OCC Conditional Approval Letter 317, Application of First Tennessee Bank, N.A., Memphis, Tennessee, to Participate in a Joint Venture Real Estate Tax Reporting and Management Services (July 17, 1999), available in 1999 WL 711407 (involving a request from First Tennessee Bank, N.A. to participate in a joint venture real estate tax reporting and management service, where partnership agreements limited the power of participants to engage in impermissible activities).

118. See, e.g., OCC Conditional Approval 289, supra note 81 (where the OCC indicated that the ability to divest the interests acquired within a two year period would satisfy this criteria. In this particular interest, the banks held only warrants in the target company, had no board representation, and no legal or contractual power to limit the activities of the target company).
ing treatment for a minority investment by a bank in a company is to report it as an unconsolidated subsidiary under the equity or cost method of accounting. Under the cost method, losses recognized by the investor will not exceed the amount of the investment (including extensions of credit or guarantees, if any) shown on the investor's books. Under the equity method, unless the bank has guaranteed any of the liabilities of the entity or has other financial obligations to the entity, losses are generally limited to the amount of the investment, including loans and other advances shown on the investor's books. The equity method of accounting is generally appropriate for investments of 20% or more of the equity of a company. Under either method, however, the losses of the venture do not pass to the books of the parent owners.

d. The investment must be convenient or useful to the bank in carrying out its business, and not a mere passive investment unrelated to that bank's banking business.

A national bank's investment in an enterprise or entity must also satisfy the requirement that the investment have a beneficial connection to the bank's business. That is, it must be convenient or useful to the bank's business and not merely a passive investment unrelated to the bank's banking business. 12 U.S.C. 24 (Seventh)\(^\text{119}\) gives national banks incidental powers that are "necessary" to carry on the business of banking. "Necessary" has been judicially construed to mean "convenient or useful."\(^\text{120}\) OCC precedents on non-controlling investments have indicated that the investment must be convenient or useful to the bank in conducting that bank's business. The investment must benefit or facilitate that business and cannot be a mere passive or speculative investment.

\(^{120}\) Arnold Tours v. Camp, 472 F.2d 427, 432 (1st Cir. 1972).
B. Minority Investments – Bank Holding Companies

1. The Less Than 5% Investment

As noted above, the Bank Holding Company Act precludes a bank holding company from owning or controlling voting shares of any company that is not a bank except under certain conditions. One of the more significant of those conditions is found in Section 4(c)(5) of the Bank Holding Company Act, 12 U.S.C. 1843(c)(5), which allows a bank holding company to hold "shares of any company which do not include more than 5 percentum of the outstanding voting shares of such company."

While there is a fair amount of regulatory gloss on this exception (e.g., it is generally intended to be a non-controlling, passive investment), it can provide an important avenue for a bank holding company to engage in venture capital investing or other forms of strategic investing in technology companies without having to (i) obtain prior approval or satisfy notice requirements, or (ii) be particularly concerned about whether the activities of the target are bank holding company permissible. As a result, bank holding companies are actively structuring investments involving combinations of debt, non-voting and voting equity and equity rights such as warrants and options, designed to allow them to participate strategically, technologically and financially in technology companies.

An important guidance is the Federal Reserve’s policy statement on non-voting equity investments. The policy statement details the types of structures that are consistent with the provisions of the Bank Holding Company Act, and those that are likely to cause problems under the Act. While the Federal Reserve issued the policy statement in the context of bank holding company investments in other banking organizations, the Federal Reserve applies the logic of the policy statement to investments in non-banking organizations.

122. See II F.R.R.S. 4-172.1 (March 1994).
Section 4(c)(8) of the Bank Holding Company Act allows investments in companies that the Board has determined to be so closely related to the business of banking or of managing or controlling banks as to be a proper incident thereto. As implemented by the Board’s Regulation Y, the Board has elucidated the list of activities that satisfy the statutory criteria.

Importantly, data processing is a permissible activity for bank holding companies. Regulation Y now provides as follows:

Data processing.

(i) Providing data processing and data transmission services, facilities (including data processing and data transmission hardware, software, documentation, or operating personnel), data bases, advice, and access to such services, facilities, or data bases by any technological means, if:

(A) The data to be processed or furnished are financial, banking, or economic; and

(B) The hardware provided in connection therewith is offered only in conjunction with software designed and marketed for the processing and transmission of financial, banking, or economic data, and where the general purpose hardware does not constitute more than 30 percent of the cost of any packaged offering.

(ii) A company conducting data processing and data transmission activities may conduct data processing and data transmission activities not de-
scribed in paragraph (b)(14)(i) of this section if the total annual revenue derived from those activities does not exceed 30 percent of the company's total annual revenues derived from data processing and data transmission activities.

Regulation Y now provides an expedited notice process permitting well-capitalized and well-managed banks to commence on a de novo basis or acquire companies engaged in data processing activities. The notice requirement consists of submitting basic financial and managerial data regarding the activity and the investment. Companies that are not eligible for the expedited notice process can still go through an application and approval process.

C. Outsourcing

It would be unusual for a bank to perform all of its technology functions internally. Most banks will go through an extensive evaluation process to measure in-house capabilities, in-house costs and the corresponding capacities of non-bank providers. Each of the regulatory authorities recognizes the business necessity of outsourcing, and thus is generally supportive of the concept. On the other hand, each also recognizes that the bank maintains the underlying obligations to its customers, and the overall responsibility for compliance with laws, rules and regulations. Accordingly, outsourcing arrangements should be subject to intense scrutiny by the institution, as they will be subject to intense scrutiny by the regulators.

1. The FFIEC Information Systems Handbook

The FFIEC has provided an extensive handbook125

---

for banks as they address possible outsourcing arrangements. The handbook describes some of the primary considerations in outsourcing arrangements and the essential contractual elements to be contained in any agreement. Of particular importance, according to the FFIEC, are the following:

- An accurate description of the services to be performed, with appropriate service level agreements and including a precise allocation of responsibilities. Among other things, the agreement should address the frequency of processing and the types and frequency of reports. Timing and delivery requirements are also critical.

- Costs, including development, conversion, processing, upgrades and enhancements and special items. The mechanism for increases or modifications should be addressed. The arrangement should also address the penalties for inadequate or non-performance.

- On-line communications availability, transmission line security and alternate data entry methods.

- Audit rights and responsibilities.

- Backup data retention, record protection and disaster recovery responsibilities and requirements.

- Liability for loss or damage to information or equipment, and related insurance protection.

- Confidential treatment of data and compliance with privacy and confidentiality policies.
- Rights upon termination to data, equipment and related items, including appropriate transition arrangements and assistance and related costs.

- Termination or cancellation rights and associated fees and penalties.

- Processing priorities.

- Notification of system changes, upgrades or any potential interruptions in service.

- Periodic reporting of financial condition of the servicer. Obviously, the importance of this provision escalates with (i) the size of the servicer and (ii) the overall importance of the services provided to the institution.

- Training responsibilities.

- Impact of insolvency or receivership of either party.

- Contract and penalty provisions.

- Ability to assign duties and responsibilities.

- Sensitivity to essential services.

- Prohibition of gifts, premiums or bonuses that might run afoul of anti-bribery proscriptions.
2. The Bank Service Corporation Act

The Bank Service Corporation Act,\(^{126}\) allows the bank regulatory agencies examination authority over entities providing banking services to banks under contractual arrangements. 12 U.S.C. 1867(c) provides:

> [W]henever a bank that is regularly examined by an appropriate Federal banking agency, or any subsidiary or affiliate of such a bank that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services authorized under this chapter, whether on or off its premises

> (1) such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the bank itself on its own premises, and

> (2) the bank shall notify such agency of the existence of the service relationship within thirty days after the making of such service contract or the performance of the service, whichever occurs first.

The existence of the regulatory authority may come as a surprise to certain vendors. It is extremely important that they be aware of the regulatory jurisdiction. The contract should require the vendor to submit to such jurisdiction and examination, provide all necessary information and generally cooperate with respect to the regulatory obligations.

---

3. FDIC Authority over Disadvantageous Contracts

When FIRREA\textsuperscript{127} was enacted in 1989, Congress added a provision to the FDIC's powers prohibiting a depository institution from entering into a contract with any person to provide goods, products or services to or for the benefit of such depository institution if the performance of such contract would adversely affect the safety or soundness of the institution.\textsuperscript{128} The provision was prompted by a series of data processing contracts the FDIC "inherited" when an institution failed which were extremely disadvantageous to the institution, and thus to the FDIC.

In that light, the FFIEC Handbook mentions a series of provisions that should be avoided in outsourcing contracts. These directly relate to inducements that may have a short-term positive effect on a bank's capital position, but have long-term detrimental effects. For example, the FFIEC warns against offers to purchase certain assets (e.g., computer equipment or foreclosed real estate) at book value, offers to purchase capital stock, offers to make an up-front cash payment, or offers to allow deferral of conversion costs or fees. In general, the FFIEC advises that the service provider will usually recoup the costs of these inducements through a premium charge for the underlying data processing services, which adversely affects the financial condition of the bank.

V. Privacy

Privacy of customer information has taken on an important role in banking today as customers have grown increasingly sensitive to the treatment of their personal information. This concern becomes even more significant given the increasing use of the Internet by banks to deliver their services to the public. Consumers' fears concerning their personal information could


\textsuperscript{128} 12 U.S.C. § 1831g (1994).
quickly turn to distrust of Internet banking. Therefore, effective privacy practices are a key to the future success of Internet banking.

Bank privacy statements and policies vary greatly. Banks have taken varied approaches to the issue of transferring or selling customer information to third parties for the purposes of facilitating the marketing of products and services to the customer base.\textsuperscript{129}

A. \textit{Fair Credit Reporting Act}

The \textit{Fair Credit Reporting Act}\textsuperscript{130} is discussed above,\textsuperscript{131} and imposes strict requirements on entities that collect, transmit and use information on consumers for the purpose of making (or allowing others to make) credit and certain other decisions. The definitional sections in the Act are of extreme importance, as they define consumer report, consumer reporting agency, and the various other entities that can be brought within the scope of the act by virtue of their collection, transmission or use of consumer information.

The \textit{Fair Credit Reporting Act} allows banks to gather and use their own experiential information in making credit decisions, and allows them to share certain of that information with credit reporting agencies. It also allows banks to use information from credit reporting agencies in making credit and certain other decisions, but imposes certain obligations on banks when they deny credit or access to other services or opportunities on the basis of information contained in the credit report. A bank can become a credit reporting agency and thus become subject to the requirements associated with maintaining accurate information.

\begin{footnotesize}
\begin{enumerate}[\textsuperscript{129}.
\item Some examples include:  
\item[129.] <http://www.firstunion.com/help/legal/privacy.html>  
\item[129.] <http://wellsfargo.com/privacy/>  
\item[129.] <http://www.bankofamerica.com/privacy/>  
\item[129.] <http://www.firstib.com/about/privstate.html>.  
\item[130.] 12 U.S.C. \S 1681 (1994)  
\item[131.] See supra part I.C.3.e.
\end{enumerate}
\end{footnotesize}
and allowing consumers to correct erroneous information.

Recently the OCC has expressed some concern about banks withholding information from credit reporting agencies. While there is no statutory obligation for banks to share the information they may have obtained based upon direct transactions with the customer, the OCC has indicated that as accurate credit information is of benefit to the overall credit industry, it would look unfavorably upon a lender that refused to share basic information with the credit reporting agencies.

The FCRA obligations must be considered by banks when developing privacy statements for their customers. Banks will clearly want to reserve the right to share permissible experiential information with the credit reporting agencies, even though they might be willing to commit to their customers not to share information with third party marketers.

B. OCC Advisory Letter 99-6, Guidance to National Banks on Web Site Privacy Statements.

In Advisory Letter 99-6, issued May 4, 1999, the OCC provides national banks and examining personnel with examples of effective practices for informing consumers who access bank web sites about bank privacy policies relating to confidential customer information. These practices fall into three basic categories: clear disclosure about the handling of customer information, consistent internal polices concerning private customer information, and mechanisms to enhance compliance with bank privacy policies.

Effective disclosure consists of two elements, disclosing the proper information and choosing an effective mechanism to make the disclosure. With respect to the first element, many banks choose to post privacy notices on their web sites that acknowledge their clients' privacy expectations and indicate how those expectations will be met. Additionally, banks may inform

---

their customers of the limitations placed on bank employees regarding the use of customer information. They may also choose to describe the circumstances in which customer information will be given to third parties. Some banks even allow customers themselves to restrict the use of their personal information.

With regard to the mechanism used to disclose the bank’s privacy policies, some banks simply post their policies directly on their web sites. Other institutions choose to use a “hypertext” link that allows the customer to view their banks policies if they so choose. Finally, some banks place links to their privacy policies in the footer of each of their web site pages.

In addition to disclosing their privacy policies to consumers, banks also need internal guidelines for implementing those policies. Effective internal guidelines tend to have several common elements. For instance, they generally involve senior management. This is because senior management is uniquely capable of providing a broad perspective on the issues, allocating the necessary resources, and creating the necessary culture to ensure that privacy matters are given due care across the organization. Another common trait of effective internal policies is that they are often developed in interdisciplinary groups to guarantee that the policies are suitable to the entire organization.

Well-intentioned internal policies are, however, of little importance if there is not a system in place to ensure policy compliance. With this in mind, banks have taken action to encourage compliance by their own personnel as well as unaffiliated third parties. Banks have worked to inform their personnel of their privacy policies through employee handbooks, training programs, codes of ethics, and Intranet postings among other things. Banks have also begun using internal audits to evaluate policy compliance. Finally, banks have started punishing violations of their confidentiality policies as they would any other breach of policy. With respect to third-parties such as data processing agents, banks have simply begun requiring the execution of confidentiality agreements.
C. **FDIC FIL 86-98, Online Privacy of Consumer Information.**

Financial institutions have been compiling consumer data for many years. Recent surveys have revealed, however, that bank customers are growing increasingly concerned with the collection, use and dissemination of such information, particularly over the Internet. FIL 86-98\(^\text{133}\), like OCC Advisory Letter 99-6, addresses these concerns. The overarching issue in both publications is the growing role of the Internet in banking and the potential harm caused to the reputations of banks if customer information is not adequately protected.

FIL 86-98 articulates several fundamental elements of a successful privacy policy. Foremost on this list is the need for banks to provide their customers notice of the banks' information collection practices. This notice should include the identity of the party collecting the consumer data, how the information will be collected, why the information is being collected, how the information will be used, and how the consumer may limit disclosure of the information. According to the FDIC, this notice should be conspicuously placed on the financial institution's web site, should be clearly stated and easily understood by consumers.

FIL 86-98 emphasizes that privacy issues are a self-regulatory matter for the financial services industry to handle on its own. In this self-regulatory context, privacy polices and information protections can only be effective if accompanied by personnel training and adequate internal controls. Internal controls should effectively check compliance with the institution's privacy polices and information practices. Even beyond their own personnel, banks are now also responsible for ensuring that third parties such as parties to outsourcing agreements avoid making improper disclosures of personal consumer information.
