United States General Accounting Office

GAO

Report to the Chairman,
Committee on Banking and Financial
Services, House of Representatives

July 1999

ELECTRONIC BANKING

Enhancing Federal Oversight of Internet Banking Activities

GAO/GGD-99-91

GAO

United States
General Accounting Office
Washington, D.C. 20548

General Government Division

B-280366

July 6, 1999

The Honorable James A. Leach
Chairman, Committee on Banking and Financial Services
House of Representatives

Dear Mr. Chairman:

As you requested, this report discusses federal oversight of depository institutions' Internet banking activities. Internet banking involves individuals' use of personal computers connected to their depository institutions over the Internet to transfer funds between accounts, make payments, or obtain information, such as account balances. The recent rapid growth of Internet banking services has led to congressional concern about the safety and security of such banking activities and the preparedness of banking regulators to help ensure safe and sound Internet banking operations. The objectives of this report are to (1) describe the risks posed by Internet banking and the extent of any industrywide Internet banking-related problems, (2) assess the methods used by regulators to track depository institutions' plans to provide Internet banking services, (3) determine how regulators examined Internet banking activities, and (4) determine the extent to which regulators examined firms providing Internet banking support services to depository institutions.

Results In Brief

Internet banking heightens various types of traditional banking risks of concern to regulators, including strategic, compliance, security, reputation, and transactional risks.[1] As provided in regulatory guidance to banks, savings and loan associations (thrifts), and credit unions, these risks should be managed through implementation of risk management systems that emphasize, among other things, active board and senior management oversight, effective internal controls, and comprehensive and ongoing internal audit programs. Examinations of Internet banking that we reviewed found that some depository institutions were not taking all the necessary precautions to mitigate Internet banking risks. While deficiencies were found, none of these examinations reported any financial losses or security breaches. However, during the time of our review, too few examinations had been completed to identify the extent of any industrywide Internet banking-related problems.

[1] For a definition of these risks see pages 8 and 9.

In general, the regulators said that few examinations had been completed because Internet banking is a relatively new activity and implementation of examination programs has required examiner training and testing of new examination procedures. In addition, they said that the number of examiners with expertise in information systems was limited and that some examiners who might otherwise have been deployed by some regulators to monitor Internet banking in the past 2 years were diverted by higher-priority efforts to address the Year 2000 computer problem.[2] While the regulators have shared information on issues of common concern to them in the past, they have not routinely shared information on identified Internet banking risks and examination results. As more examinations are completed, sharing of information among the regulators could help them better understand the extent of the risks posed by Internet banking, develop risk characteristics allowing them to target institutions requiring further attention, and help them allocate limited resources among competing priorities.

Regulators use a variety of methods to identify depository institutions that are already offering Internet banking services; however, only two regulators had systematically obtained centralized information on depository institutions' plans to provide such services and had a database of this information at the time of our review. The Office of Thrift Supervision (OTS), which regulates thrifts, recently established a requirement that depository institutions (1) notify it in advance of plans to establish a transactional Web site and (2) report their Web site address in quarterly Thrift Financial Report filings. Such information is maintained in a centralized electronic database. In addition, the Federal Deposit Insurance Corporation (FDIC) developed a centralized database that contains, among other things, information on a depository institution's plans to provide Internet banking services. Information in this centralized database is collected as part of the examination process. When FDIC examiners encounter an institution that is not currently conducting Internet banking activities, they are still required to gather minimal information about whether the institution plans to establish Internet banking. These or other methods could be used by other regulators to inform them about Internet banking plans and activities and better enable them to provide specific risk management guidance to individual

[2] The Year 2000 computer problem exists because the data that computers store and process often use only the last two digits to designate the year. On January 1, 2000, such systems may mistake data referring to 2000 as meaning 1900, possibly leading to numerous errors and disruptions in processing of financial data.

depository institutions when needed. The information could also be used to help ensure regulatory awareness of the growth of Internet banking, plan the scope and timing of future examinations, and determine the need for additional examiners with information technology expertise.

During our review, most regulators were developing, testing, or implementing new on-line banking examination procedures, which included procedures for examinations of Internet banking, and most had conducted at least some examinations of depository institutions' Internet banking operations. Because Internet banking is a relatively new and evolving banking activity, FDIC and OTS expect their examiners to thoroughly examine an institution's Internet banking activities during their first examination after those activities are implemented. While the Federal Reserve System (FRS) and the Office of the Comptroller of the Currency (OCC) also consider Internet banking to be an evolving activity, they do not require that an institution's new Internet banking activity be thoroughly examined. The National Credit Union Administration (NCUA), which reported a significant diversion of resources due to work related to the Year 2000 computer problem, was the only regulator that had not developed requirements and procedures for Internet banking examinations. Because NCUA lacked an effective Internet banking examination program, it could not provide assurances that credit unions with Internet banking were appropriately managing risks that could affect their safety and soundness.

Many depository institutions contract with third-party firms for Internet banking support services they choose not to provide themselves. Each regulator has the authority to examine depository institutions' banking services provided by a third party and to avoid duplication of effort, regulators often cooperate in examining third-party firms. Joint examination of firms providing Internet banking services could better enable regulators to share technical resources and fill expertise gaps in this emerging activity. In late 1998, the five regulators, working under Federal Financial Institutions Examination Council (FFIEC) auspices, cooperatively initiated a joint study of Internet banking services provided by third-party firms. The study is to provide the regulators with a greater understanding of the services and security features provided to depository institutions by third-party firms.

While each regulator has the authority to examine third-party firms providing services to depository institutions, NCUA's authority to examine such firms is temporary. Its authority, which was granted so that NCUA could conduct examinations related to the Year 2000 computer problem,

expires on December 31, 2001. The expiration of this authority would limit NCUA's future ability to effectively oversee third-party firms that provide Internet banking services to credit unions.

We are making recommendations to federal banking regulators and raising a matter for congressional consideration to address these issues.

Background

Internet banking is one form of on-line banking; PC direct dial banking is another. Before Internet banking, customers using direct-dial PC banking needed to use specialized computer software provided and supported by their depository institution. More recently, these direct-dial connections are being replaced by Internet connections over which customers can use their computers and browser software to connect to their depository institution's Web site.

In general, regulators distinguish three types of Internet banking Web sites:

- Purely informational sites, which have information about the depository institution and its products and services but no interactive capability;
- Information-exchange sites, which provide information and allow customers to send information to the depository institution or make inquiries about their accounts; and
- Fully transactional sites, which offer the previously described capabilities as well as some additional services, such as real-time account queries, transfers of funds among accounts, bill payments, or other banking services.

Internet banking services are offered by a rapidly growing number of depository institutions. According to recent data, at least 3,610 federally insured depository institutions—about 17 percent of all U.S. banks, savings associations, and credit unions—offered some form of Internet banking service as of February 1999.[3] About 20 percent of these depository institutions offered fully transactional Web sites.[4] Information available from the banking regulators and industry studies suggest that Internet banking is accelerating. According to FDIC and NCUA statistics, in the 11

[3] In February 1999, approximately 2,500 banks and thrifts—about 23 percent of all banks and thrifts—had Web sites, according to FDIC. As of June 30, 1998, 1,110 credit unions had Web sites, according to NCUA.

[4] According to FDIC, 436 banks and thrifts offered fully transactional Web sites as of February 4, 1999. According to NCUA, 256 credit unions offered such sites as of June 30, 1998.

months ending February 1999, the number of banks, thrifts, and credit unions with transactional sites almost tripled. According to projections reported by the Department of Commerce, the number of customers who went on-line to perform banking transactions increased by 22 percent, from 4.6 million to 5.6 million, in the 6 months ending April 1998.[5]

Five federal regulators—FDIC, FRS, NCUA, OCC, and OTS—supervise and examine all federally insured depository institutions. FDIC, a government corporation, is the primary federal regulator of state-chartered banks that are not members of FRS. FRS, another independent body, shares responsibility with state banking regulators for supervising and examining state-chartered banks that are members of FRS. In addition, FRS supervises bank holding companies and their nonbank subsidiaries. Banks under FRS' supervision are supervised by 12 regional Reserve Banks that conduct examinations under delegated authority from the Board of Governors in Washington. NCUA is an independent body responsible for examining and supervising federally insured credit unions and works with state regulators to monitor the safety and soundness of state-chartered credit unions. OCC, an agency, that is a bureau of the Department of the Treasury, supervises all national banks. OTS, which is also a bureau of the Department of the Treasury, serves as the primary regulator for thrifts and thrift holding companies. The regulators oversee a mix of large, medium, and small depository institutions, as shown in table 1.

Table 1: The Number and Asset Size of Depository Institutions Overseen by Banking Regulators, as of June 30, 1998

Dollars in billions

		Large institutions[a]		Small and medium institutions[b]	
Regulator	Total institutions supervised	Number	Assets	Number	Assets
FDIC	5,449	5	$87	5,444	$822
FRS	989	19	1,013	970	282
OCC	2,546	40	2,160	2,506	819
OTS	1,181	16	374	1,165	412
NCUA	11,130	1	10	11,129	375
Total	**21,295**	**81**	**$3,644**	**21,214**	**$2,710**

[a]$10 billion or more in assets.

[b]Less than $10 billion in assets.

Source: GAO analysis of FDIC and NCUA data.

Banking regulators also work together through FFIEC, an interagency forum Congress created in 1979 to promote consistency in the examination

[5] The Emerging Digital Economy (U.S. Department of Commerce, April 1998).

and supervision of depository institutions.[6] In 1996, FFIEC updated its "Information Systems Handbook," which provides regulators with general guidance on information systems and technology examinations.

To help ensure the safety and soundness of federally insured banks, thrifts, and credit unions, banking regulators conduct various types of monitoring activities. They include the following:

- Off-site monitoring, which generally consists of reviews and analyses of depository institution-submitted data, including call reports, and discussions with bank management,[7] is carried out to monitor compliance with requirements or enforcement actions; formulate supervisory strategies, especially plans for on-site examinations; and identify trends, areas of concern, and accounting questions.

- On-site safety-and-soundness examinations are conducted to assess the safety and soundness of a depository institution's practices and operations. Specific objectives of these on-site examinations that are common to all the banking regulators include (1) determining the institution's condition and the risks associated with its current and planned activities; (2) evaluating the institution's overall integrity and the effectiveness of its risk management by testing the institution's practices; and (3) determining the institution's compliance with laws, regulations, and rulings.

- Information systems examinations are conducted to identify and correct information and technology-related risk exposures of significance that threaten the depository institution. These examinations focus on various components of an institution's information system, such as the capabilities of its information technology management; the adequacy of its systems development and programming; and the quality, reliability, availability, and integrity of its information technology operations.

[6] FFIEC is composed of the Comptroller of the Currency, one FRS Governor, the OTS Director, the FDIC Chairman, and the Chairman of the NCUA Board.

[7] Call reports for banks are also called the Consolidated Reports of Condition and Income. The reports for bank holding companies are called the Consolidated Financial Statements for Bank Holding Companies. Similar quarterly reports on thrifts and thrift holding companies are submitted to OTS. The reports are prepared by institution management and submitted to the primary regulator on a quarterly basis. The reports include a balance sheet, income statement, and various supporting detailed analyses of balances and related activities. The reports for credit unions are called Financial and Statistical Reports.

- Finally, special technical examinations of banking services by third parties are conducted to ensure that banking operations performed by third-party firms are consistent with the safety and soundness of the depository institutions using the services. These examinations, which often include a review of the management systems, operations, and financial condition of the service providers, can provide regulators with greater assurances of the reliability of services than can be obtained during normal safety and soundness examinations of a depository institution.

The banking regulators also conduct reviews of on-line banking systems for compliance with consumer protection laws and regulations. These include examinations of an institution's obligation to provide required notices and disclosures on Internet banking products and services.

Scope and Methodology

To address our four objectives, we interviewed officials and reviewed available documents from the five banking regulators. This included obtaining information on Internet banking risks and each regulator's strategy for overseeing Internet banking activities, the methods used to identify depository institutions that offer Internet banking, the existence of safety and soundness and information systems examination procedures for reviewing Internet banking, and the extent of examinations of third-party firms. We did not independently verify the accuracy of data that banking regulators provided. We also interviewed representatives from selected depository institutions and third-party firms to obtain their views on the scope and frequency of examinations by bank regulators and their assessment of risks posed by Internet banking systems. In addition, we developed a data collection instrument to document our review of 81 safety and soundness and information systems examinations that included on-line banking and we also used a structured questionnaire to interview 43 selected examiners who had conducted these on-line banking examinations. (See app. I for a more detailed description of our scope and methodology.)

We did our work from April 1998 to May 1999 in Washington, D.C.; Los Angeles, CA; San Francisco, CA; Atlanta, GA; Kansas City, KS; and New York, NY, in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the five banking regulators and FFIEC, and these comments are discussed near the end of this letter and are reprinted in appendixes III through VIII.

Regulators Agree Internet Banking Presents Risks and Oversight Challenges, While Extent of Any Industrywide Problems Is Unknown

Internet banking services heighten various types of risks that are of concern to banking regulators, and the regulators have advised institutions to mitigate these risks through the implementation of risk management systems that emphasize, among other things, (1) active board of directors' oversight, (2) effective internal controls, and (3) comprehensive internal audits. Too few examinations that included a review of Internet banking had been conducted at the time of our review for the extent of Internet banking-related problems industrywide to have been identified. However, our review of 81 such examinations revealed that some depository institutions had not always adhered to risk mitigation guidance provided by the regulators. Few examinations had been conducted because, according to the regulators, Internet banking was a relatively new activity, and examination procedures were still being developed. Other reasons reported by regulators were that the number of examiners with expertise in information systems was limited and that some examiners who might otherwise have examined on-line banking during our study period were diverted by higher priority efforts to address the Year 2000 computer problem. As more examinations are completed, sharing of information among the regulators could help them better understand the extent of risks posed by Internet banking, develop risk characteristics allowing them to target institutions requiring further attention, and help make decisions on how best to allocate information technology expertise among competing priorities.

Internet Banking Risks

Internet banking heightens various types of traditional banking risks that are of concern to banking regulators. These risks, which are discussed in regulatory guidance provided to depository institutions, include the following:

- Security risk is the risk of potential unauthorized access to a depository institution's networks, systems, and databases that could compromise internal systems and customer data and result in financial losses. The use of an electronic channel, such as the Internet, to deliver products and services introduces unique risks for a depository institution due to the speed at which systems operate and the broad access in terms of geography, users, applications, databases, and peripheral systems.

- Transactional risk is the risk of financial losses arising from problems with service or product delivery. Transactional risk often results from deficiencies in computer system design, implementation, or ongoing maintenance.

- Strategic risk is the risk to earnings or capital arising from adverse business decisions or adverse implementation of those decisions. Depository institutions face strategic risk whenever they introduce a new product or service, such as Internet banking.

- Reputation risk is the risk of significant negative public opinion that results in a critical loss of funding or customers. This risk can also expose the depository institution to costly litigation. Failure of Internet banking products to perform as promised, such as a communication failure that prevents customers from accessing their accounts, could expose a depository institution to reputation risk.

- Lastly, compliance risk is the risk arising from violations of, or nonconformance with, laws, rules, regulations, required practices, or ethical standards. This risk may arise if a depository institution fails to comply with regulatory guidance or an enforcement action.

Regulators Have Provided Guidance on Risk Mitigation

Banking regulators have provided depository institutions with advisory guidance on how to mitigate risks posed by Internet banking, including risks related to services provided by third-party firms. In their guidance, regulators describe how depository institutions in general should plan for, manage, and monitor risks associated with the use of technology. Most regulators provided such guidance in advisory letters to all covered depository institutions. FRS provided its guidance in a "sound practices paper" released at a FRS information security conference in September 1997. The guidance was not tailored to fit individual institutions. (See app. II for descriptions of guidance provided by each regulator.) As discussed in these advisory guidance, risk management systems include the following critical components.

- Active board and senior management oversight: Boards of directors have ultimate responsibility for on-line banking systems, including Internet banking systems, offered by their depository institutions. The guidance points out that the Internet facilitates broad access to confidential or proprietary information, and deficiencies in planning and deployment can significantly increase the risk posed to a depository institution and decrease its ability to respond satisfactorily to problems that arise. For this reason, directors, senior managers, and line officers are to be fully informed of the significant investments, opportunities, and risks involved in deploying such technology. Boards of directors should approve the overall business and technology strategies, and senior management should ensure that adequate risk management systems are in place.

- Effective internal controls: Internal controls are the means by which the board of directors, management, and other personnel obtain reasonable assurance that an institution's assets are safeguarded and that its systems and operations are reliable and efficient. Regulators' guidance describes a variety of internal controls to help mitigate risks involving such areas as systems security, management of third-party firms, and various operating policies and procedures that should be considered to keep pace with new technological developments.

- Adequate internal audits: Regulators' guidance points out that an objective review of on-line banking should identify and quantify risk, and detect possible weaknesses in a depository institution's risk management system as it pertains to on-line banking. When coupled with a strong risk management program, a comprehensive, ongoing audit program allows the institution to protect its interests as well as those of its customers and other participants.

Too Few Examinations Had Been Conducted to Identify the Extent of Any Industrywide Internet Banking-Related Problems

While examiners found that some depository institutions were not taking all of the prescribed precautions to mitigate risks, too few examinations with documented on-line banking assessments were available at the time of our review to identify the extent of any industrywide Internet banking-related problems. According to the regulators, few examinations had been conducted because Internet banking is a relatively new activity and regulators have had to develop and implement new policies and procedures and related training programs to assess this activity. In addition, regulatory examinations required to address the higher priority Year 2000 computer problem were contemporaneous with our review, and some regulators reported that limited information systems resources prevented them from conducting both Year 2000 and on-line banking examinations.

Between March 1998 and August 1998, we asked each regulator to provide us with information on safety and soundness and information systems examinations in which (1) examiners applied their agency's on-line banking examination procedures written for both direct-dial and Internet banking systems or (2) where the examination's scope included on-line banking. It was difficult for most regulators to provide such information because, with the exception of FDIC, information was not maintained centrally to identify examinations that included on-line banking assessments. We reviewed 81 examinations that regulators were able to provide. The 81 examinations included 58 small-, 18 medium-, and 5 large-

sized depository institutions.[8] The Internet banking activities examined by the regulators included informational sites, information-exchange sites, and transactional sites.

In the examinations we reviewed, examiners noted that the on-line banking risk mitigation systems had various types of weaknesses. None of the examined depository institutions, including those whose risk management systems evidenced weaknesses, were reported to have experienced financial losses or security breaches due to Internet banking activities. However, in the 81 depository institutions examinations we reviewed, regulators found that 36 (44 percent) had not completely implemented the on-line banking risk mitigation steps outlined by the regulator. As summarized in table 2, in 20 of the 81 examinations (25 percent), strategic planning deficiencies were discovered. For example, the regulators found that some institutions had not prepared strategic plans or had not obtained board of directors' approval before initiating on-line banking. In 26 of the examinations (32 percent), the regulators found that the institution did not have policies and procedures in place to guide its on-line banking operations. In 29 of the examinations (36 percent), the regulators found that the institution lacked adequate audit coverage of its on-line operations. Fifteen examinations (18 percent) disclosed that the institution had not taken steps to evaluate its third-party firm or lacked a written contract with the firm. Examiners whom we interviewed expressed concerns about deficiencies similar to those revealed in the examinations we reviewed. For example, examiners were concerned that some smaller institutions were implementing Internet banking systems before they had established operating policies and procedures and that bank management had to be reminded that operating policies and procedures were not optional.

[8] The examinations we reviewed included 62 that were conducted by FDIC, 6 by FRS, 8 by OCC, and 5 by OTS. FDIC also provided some examinations that were conducted between June 1997 and February 1998.

Table 2: On-line Banking-Related Weaknesses in Risk Mitigation Systems, as Reported in 81 Examinations Completed From June 1997 to August 1998

	Size of banks and thrifts offering on-line banking services with reported weaknesses							
	Small[a]		Medium[a]		Large[a]		Total	
Type of weakness	Number	Percent[b]	Number	Percent[b]	Number	Percent[b]	Number	Percent[b]
Deficiencies in strategic planning	18	31	2	11	0	0	**20**	**25**
No policies and procedures to address security concerns and standard operating practices	21	36	4	22	1	20	**26**	**32**
Insufficient audit coverage of on-line banking activities	25	43	4	22	0	0	**29**	**36**
Management had not properly initiated or documented agreements with third-party firms	12	21	2	11	1	20	**15**	**18**

Note: The number of weaknesses reported exceeds the number of institutions examined (81) because some depository institutions were reported to have more than one type of weakness.

[a]Small depository institutions are defined as institutions with less than $1 billion in assets. Medium-sized institutions have $1 billion to $10 billion in assets, and large institutions have more than $10 billion in assets.

[b]Percent of institutions examined in the size group with identified weaknesses.

Source: GAO analysis of FDIC, FRS, OCC, and OTS data.

Because the examinations we reviewed did not represent a statistically valid sample, we are unable to project the number of weaknesses beyond the institutions reviewed. However, the extent of problems identified at smaller institutions is consistent with views expressed by some banking industry officials that smaller institutions have the potential to encounter Internet banking-related problems. These officials generally believed that smaller institutions may have insufficient in-house expertise to operate an Internet banking system or lack the ability to adequately evaluate the Internet banking services offered by third-party firms to ensure that such systems operate as intended. In particular, NCUA officials observed that smaller institutions might move too quickly into Internet banking because of the relatively low costs of providing such services through third-party firms and the desire to remain competitive.

Regulators Face Human Capital Challenges Because of Internet Banking Growth

Banking regulators have told us that depository institutions' increasing use of information technology—such as that employed in Internet banking—and the growth forecast for Internet banking, present them with human capital management challenges. The adequacy of regulatory efforts to ensure safe and sound operations of complex transactional Internet

banking systems will depend increasingly upon the availability of examiners with appropriate expertise or training in information technology management. During our review, banking regulators expressed concern about their ability to address technological changes in the banking industry with their existing resources.

Awareness of Internet Banking Plans Could Help Regulators Provide Timely Guidance and Manage Existing Resources

Information about depository institutions' plans to provide Internet banking services could help ensure that regulators are aware of growth and technological trends in Internet banking. This information could be instrumental in enabling regulators to provide individual depository institutions with more timely and specific risk-management guidance and advice before such institutions enter into contracts with third-party firms or independently develop their own Internet banking services. Awareness of an institution's Internet banking plans could also provide regulators with useful information to plan the scope and timing of future examinations as well as to identify the need for examiners with the appropriate information technology expertise. OTS recently established a requirement that it receive advance notice of an institution's plans to establish a transactional Web site. OTS and FDIC were the only regulators that captured Internet banking information gathered during examinations, including information about institutions' plans to offer Internet banking, in a centralized database that could be used in planning examinations and monitoring Internet banking activities. Other methods used by regulators to identify depository institutions that are already offering Internet banking do not allow the regulators the opportunity to evaluate the effectiveness of an institution's Internet risk mitigation plans or to provide institutions with more timely and specific risk management guidance and advice prior to implementation.

OTS Requires Advance Notification of Institutions' Plans to Offer Internet Banking

OTS regulations, effective January 1999, require thrifts to provide a written notice to OTS before establishing a transactional Web site. The regulations state that the notice must describe the transactional Web site; indicate the date the site will become operational; and list a contact familiar with the deployment, operation, and security of the site.[9] According to OTS officials, the one-time notification requirement will enable the agency to better monitor technological innovations and thus assess emerging security and compliance risks. OTS officials said they believed that this monitoring would also enable the agency to more proactively provide guidance to thrifts as they plan for or begin to conduct Internet operations.

[9] 12 C.F.R. 555.310(a).

At the time of our review, OTS was beginning to develop procedures for providing such guidance. If, after receiving the notice OTS informs the thrift of any concerns, the thrift must follow any procedures that OTS imposes. If the thrift does not receive any comments from OTS, it is free to go on-line 30 days from the filing date of its notice with OTS.

Before adoption of the final proposal, OTS recognized that this notice requirement would impose some burden on thrifts. However, it determined that the one-time expenditure by a thrift of an estimated 2 hours to report its plans represented a minimal burden. Before January 1999, the effective date of the reporting requirement, OTS officials told us that OTS identified thrifts' Internet banking activities primarily during examinations, although some of its regional offices used other means to identify Web sites. For example, the western region periodically had surveyed thrifts, and the Atlanta region used the Internet to identify thrifts' Web sites.

In August 1998, OTS asked for public comment on its advance notice proposal. The agency received nine comments in response—six from thrifts, two from trade associations, and one from a public interest organization. Seven commenters supported the proposal's overall flexible regulatory approach. Two commenters argued for even greater flexibility and opposed the proposed notification requirement. Four commenters also argued that the notice requirement would place thrifts at a competitive disadvantage, because other banking regulators did not impose a similar requirement. OTS' response was that it did not anticipate that the notification requirement would place thrifts at a significant competitive disadvantage because, once a thrift has addressed any follow-up questions from OTS' regional office or the 30-day period has expired, the thrift would be free to operate the transactional Web site.

Finally, one commenter questioned whether requiring regulatory notice 30 days prior to installing a transactional site would mitigate the risks mentioned by OTS. The commenter noted that developing a system requires substantial advance planning, possibly across multiple departments, and perhaps a contract with an outside third-party firm. Thus, at the time of notice, according to the commenter, the work essentially would be completed, and the financial costs of development already would have been absorbed by the institution. The commenter pointed out that, for this reason, an advance notice after the financial risk had been assumed would not substantially protect the institution. OTS' response was that it encourages thrifts concerned with such expenditures of resources to consult their regional office in the early stages of development, even before filing a notice.

FDIC and OTS Maintain Centralized Databases on Internet Banking Information

Currently FDIC and OTS are the only regulators that maintain a centralized database on Internet banking information gathered during banking examinations. In regards to FDIC, if an examiner identifies an institution that plans to offer Internet banking, this information is to be entered into the centralized system along with other on-line banking data collected. In addition to data on institutions offering or planning to offer Internet banking, this database includes information on third-party firms supplying Internet banking services. According to FDIC officials, information captured in the centralized system facilitates the creation of uniform records of all examined institutions with on-line banking and avoids capturing redundant information across FDIC's eight regions. They said that the system also provides an improved means across separate regional systems for headquarters' staff and examiners to understand how electronic banking is changing and to more effectively plan the scope, timing, and staffing of future examinations. As of April 1, 1999, the FDIC centralized system included information from 391 on-line banking examinations.[10]

OTS began collecting information centrally in November 1998. OTS officials told us that their centralized database includes on-line banking information from all examined thrifts. In addition, the database includes the Web site address of over 400 thrifts that reported this information on their quarterly filings as well as information gathered as part of OTS' advanced notification requirement.

Other Monitoring Methods to Identify Depository Institutions Offering Internet Banking

Regulators use a variety of other methods to identify depository institutions that are already offering Internet banking services. All of the regulators said that they gathered information on institutions' Internet banking services during pre-examination planning activities. The regulators also said that they periodically searched the Internet for Internet banking Web sites. In March 1998, NCUA began requiring credit unions to report their electronic mail addresses and the type of Web site offered on their periodic financial and statistical reports. In addition, at the close of our review, FRS said it was beginning to centrally collect examination and survey information on the types of Internet banking services being offered by its regulated entities (e.g., account balance inquiries, bill payment, and loan application) as well as the names of third-party firms and software vendors. OCC plans to centrally collect similar information on institutions that are already providing Internet banking services. However, such "after-the-fact" methods do not give the regulators the opportunity to provide individual institutions with more timely and

[10] This figure includes examinations of transactional sites, both direct-dial and Internet.

specific risk mitigation guidance and advice before they go on-line, and these methods do not give regulators the opportunity to evaluate an institution's risk mitigation plans before an institution's Internet banking services are operational.

Most Regulators Were Developing or Implementing Examination Procedures

With the exception of NCUA, the regulators were developing, testing, or implementing on-line banking examination procedures, which included those for examinations of Internet banking. NCUA said that it had not established procedures for Internet banking examinations or conducted Internet banking examinations because of the need to conduct Year 2000 reviews. In addition, we found that regulators' examination programs used differing methods in conducting and staffing Internet banking examinations. For example, because Internet banking is a new and evolving activity, FDIC and OTS required their examiners to thoroughly examine an institution's Internet banking activities during the first examination after those activities were implemented, while FRS and OCC did not. We also found variations in the level of expertise and training required of examiners who reviewed Internet banking systems. The regulators have shared information on issues of common concern to them in the past but have not routinely shared information on Internet banking risks and examination results. As each regulator gains experience in applying their examination methods and procedures, it would be useful for the regulators to share their expertise to help determine which methods and procedures are the most efficient and effective.

Examination Procedures Were in Differing Stages of Development

Each of the regulators had implemented similar examination policies that reflected the regulators' overall risk-based approach to supervision. These policies required examiners to determine how various existing or emerging issues facing an institution or the banking industry affected the nature and extent of risks at particular institutions. Based on a risk evaluation, examiners are expected to develop supervisory plans and actions that would direct their resources to the issues presenting the greatest risks, especially those risks that present material, actual, or potential risks to the banking system.

While the banking regulators' examination policies were established, their procedures for examining on-line banking activities were in differing stages of development. Generally, FDIC, FRS, OCC, and OTS had already implemented or were testing examination procedures for conducting on-line banking examinations. FDIC and OTS had both issued final examination procedures and were using the procedures to conduct examinations that included Internet banking activities. FDIC was the first to implement an on-line banking examination program in 1997 and had

identified more examinations for our review than any other banking regulator. In commenting on a draft of this report, FDIC said that it had also developed three technical work programs that it is field-testing and has shared with the other regulators. In addition, FDIC said that it had increased the number of information systems examiners. OTS was the next regulator to issue final examination procedures. FRS and OCC were still developing their on-line banking examination programs and were field testing their examination procedures at the close of our review.[11]

NCUA Had Not Developed or Implemented an Internet Banking Examination Program

At the time of our review, NCUA had not established procedures for Internet banking examinations or conducted such examinations. The primary reasons for this, according to NCUA officials, were that the agency did not have the necessary expertise to develop Internet banking procedures and that its examination resources were dedicated to examinations geared to averting the Year 2000 computer problems.

According to NCUA, as work related to the Year 2000 computer problem diminishes, the agency is beginning to focus attention on Internet banking activities. NCUA first began to consider the need for Internet banking examinations in 1997, when it informally distributed a white paper on "cyber credit union services." This paper was distributed to NCUA examiners who had attended a specific training course and was also provided to each regional director, who had the option of making the paper more widely available to regional staff.

NCUA officials told us the agency now expects to develop new Internet examination procedures that will be closely aligned to FFIEC's guidance on supervisory oversight of information systems, but no time frames have been established for developing or implementing these procedures. In 1998, NCUA filled three new information systems officer positions. While these individuals have been primarily devoted to the Year 2000 project, agency officials told us that these individuals will begin to develop Internet banking examination procedures and train agency examiners.

Regulators' Approaches to Examining an Institution's On-line Banking Activity Varied

While FDIC, FRS, OCC, and OTS on-line banking examination policies were similar, their approaches to examining an institution's on-line banking activity varied. For example, because Internet banking is a new banking activity that can potentially introduce new risks to an institution, FDIC and OTS expect their examiners to thoroughly examine an institution's Internet banking activities during the first examination after

[11] While still developing their program, FRS officials told us that the agency had begun to use the FDIC developed computerized examination procedures and standard forms.

those activities are implemented. In contrast, FRS and OCC do not require that an institution's new Internet banking activity be thoroughly examined. Instead, these regulators permit safety and soundness or information systems examiners to exercise discretion in determining the relative risk and the need for and scope of their examinations of new banking activities, including the establishment of Internet banking services. In this regard, examiners may decide not to devote further resources to examining Internet banking if they determine after an initial assessment that Internet banking is a small segment of an institution's overall business, posing little risk to the safety and soundness of the institution.

We also found differences in the type of examiners used to perform on-line banking examinations. Two regulators, FDIC and FRS, designed their examination procedures to mainly assess the safety and soundness aspects of Internet banking, such as the appropriateness of an institution's strategic planning, internal controls, and operating policies and procedures. These regulators said that, due to the orientation of the examination procedures, safety and soundness examiners generally conducted examinations that included a review of Internet banking. If, in the judgment of the safety and soundness examiner, a more sophisticated assessment of an institution's Internet banking activities were needed, more technically proficient information system specialists were to be called in to perform a separate assessment. In contrast, OCC said that information system specialists conducted most of its Internet banking examinations, utilizing procedures that included more technical aspects of an institution's Internet banking activities, such as policies addressing passwords, firewalls, encryption, and physical security. OCC requires that most Internet banking examinations be conducted by information system specialists because it believes that the technology-related aspects of Internet banking require examiners with expertise in information systems. OTS also requires the use of information systems examiners for examinations of complex or large institutions. Small or less complex institutions are to be examined by safety and soundness examiners.

Regulators also differed in the degree to which their examiners were trained in on-line banking systems. FDIC, FRS, and OTS initiated training programs for their safety and soundness examiners on electronic-banking issues. Topics in the training programs included electronic banking trends and developments, risks and vulnerabilities, and regulatory concerns. At the close of our review, FDIC said that it had trained nearly all of its safety and soundness examiners, and OTS said that it expected to complete their training for safety and soundness examiners by the end of 1999. FRS officials also said that they expected to complete an initial training

program for safety and soundness examiners by the end of 1999. These officials added that additional training would likely be required as Internet banking activities evolve and a greater understanding of the risks is developed. FDIC also had developed a training program that provided more in-depth information systems training to a group of information systems examiners and certain safety and soundness examiners. After the training, these examiners were expected to provide services that ranged from providing verbal consultation to other safety and soundness examiners who were conducting an examination of an institution's Internet banking activities, to independently performing information system reviews of complex on-line banking systems. OCC planned no on-line banking training of its safety and soundness examiners because on-line banking examinations were performed by information system specialists. Rather than establishing an in-house training program for these specialists, OCC said that it relied solely on external training opportunities, such as seminars and conferences hosted by FFIEC and the Bank Administration Institute.

The differing methods and approaches utilized by the regulators were too new for their overall effectiveness to be evaluated. Over time, sharing of information among the regulators on the success of these varying methods and approaches could help them assess the strengths and weaknesses of their individual programs.

Joint Regulatory Examinations of Third-Party Firms Could Enhance Internet Banking Oversight

Joint regulatory examinations of the operations of third-party firms providing depository institutions' Internet banking support services might increase the economy and efficiency of federal oversight of Internet banking activities. This would be particularly true if regulators could share technical expertise in developing and conducting examinations. In late 1998, the five regulators initiated a joint research project to study Internet banking support services provided by third-party firms. However, the extent to which this interagency group will be able to commit the necessary resources to this effort is unclear. Also, NCUA's authority to conduct examinations of third-party firms is set to expire on December 31, 2001, and the lack of such authority in the future could limit the effectiveness of the oversight provided to firms providing services to credit unions. According to NCUA, third-party firms providing credit union services are not likely to be included in any joint regulatory examinations because these firms typically only provide services to credit unions, and other regulators thus have little incentive to select these firms for a joint review.

Regulators Studying Third-Party Firm Support Services

Joint interagency examinations of traditional third-party data-processing firms, such as check-processing centers, have tended to focus on large multiregional data-processing providers serving banks and thrifts and supervised by more than one supervisory agency.[12] Regulators determined that it was more effective and efficient to conduct one interagency information systems examination instead of several separate examinations by each regulator. The regulators said that these examinations, for the most part, are conducted by examiners with expertise in information systems. In conducting these examinations, examiners and specialists from the participating regulators are to examine the policies, procedures, and practices of the third-party firm and make suggestions to the firm for improvements, if necessary. According to one regulator, two of these examinations have also included a partial review of two firms' Internet banking operations.

In late 1998, the banking regulatory agencies that comprise FFIEC initiated a special research project to study third-party firms that provide Internet banking software or services to banks and thrifts. The objectives of the project are to develop an understanding of the products and services offered by such third-party firms, identify risks and supervisory issues, and develop recommendations regarding supervisory oversight. The regulators said that the outputs from the project have not been determined but that they could include background materials to aid bank examiners, internal policy papers, supervisory guidance for institutions, or recommendations for development of examination programs or procedures. They added that the scope of the project and timetable for its completion are contingent upon available resources, which have been significantly curtailed due to the agencies' Year 2000 supervision program. As of March 1999, agency staff were gathering information on third-party firms that provided Internet banking services and preparing invitations to selected firms to discuss their services. At this initial stage of the project, regulators said they were not examining the firms but instead obtaining background information.

[12]Regulators also have conducted similar interagency examinations of third-party firms on a regional basis.

Credit Union Third-Party Firms Might Not Be Subjects of Joint Examinations

While NCUA has recently begun to participate in the joint agency study of third-party firms, it had not participated in any joint reviews of third-party Internet banking firms or independently conducted any reviews of third-party firms serving credit unions. About 13 firms provide the bulk of these services to credit unions. One of these firms provides services to about 51 percent of the credit unions offering Internet banking.[13] NCUA officials cited the lack of technical expertise as a key reason for their inactivity. Further, NCUA officials said that, on the basis of discussions at a January 1999 FFIEC planning meeting, it appeared unlikely that other regulators would participate with NCUA in joint reviews of third-party firms servicing credit unions. The NCUA officials explained that regulators typically provide staff and resources to a particular joint review when there is a regulatory overlap involving firms that provided services to both banks and thrifts. In the case of third-party firms servicing credit unions, other types of depository institutions have received few if any services from these firms.

Regulators' Authority to Examine Third-Party Firms Providing Banking Services

Since 1962, FDIC, FRS, and OCC have had the authority through the Bank Service Company Act[14] to examine the performance of certain services provided by third-party firms that affect the safety and soundness of bank operations. In deliberations prior to enacting the Bank Service Company Act, Congress made it clear that banks could not avoid examinations of banking functions by outsourcing the functions to third-party firms. The legislative history shows that Congress intended that banking regulators be able to examine all bank records and that they must be able to exercise proper supervision over all banking activities, whether performed by bank employees on the bank's premises or by anyone else on or off their premises. Regulators generally believe that this authority is important because it allows them to take a broader approach to examining the services of banks or thrifts and their providers. These examinations are not intended to replace a depository institution's oversight and monitoring of its third-party firms, which remains the responsibility of the depository institution. Instead of examining particular services that a third-party firm provides to a single bank or thrift, regulators can assess the entire broad range of services a third-party firm provides to the banking industry. In addition to being a more direct approach, most regulators believe such examinations also may be more efficient and effective. Over time, the

[13] In February 1999, this firm announced marketing agreements with traditional processing firms to offer Internet banking. These processing firms provide core services to about 1,500 depository institutions.

[14] The Bank Service Company Act, 12 U.S.C. 1861-1867.

authority to examine third-party firms has become even more important, as depository institutions have contracted out an increasing proportion of their operations. FRS officials noted, however, that such examinations (1) extend bank supervision outside the banking industry, (2) may unnecessarily consume scarce government resources unless effectively risk focused, and (3) may create a moral hazard by undermining the incentive for banks and thrifts to manage their service provider relationships effectively.

In March 1998, NCUA and OTS were given authority to examine certain third-party firms through the Examination Parity and Year 2000 Readiness for Financial Institutions Act (the Parity Act).[15] Specifically, the Parity Act gave NCUA and OTS independent authority to examine services provided by service providers to credit unions and thrifts by amending the Federal Credit Union Act and the Homeowners' Loan Act, respectively.[16] The acts primarily focus on ongoing computer services and turnkey operations in which transactions are transmitted at the end of the day to a central location. Specifically, NCUA and OTS are authorized to examine data processing, information system management, and the maintenance of computer systems that are used to track everything from day-to-day deposit and loan activity to portfolio management at a depository institution.

Expiration of NCUA's Authority to Examine Third-Party Firms Could Limit NCUA's Ability to Effectively Oversee Internet Banking

While NCUA and OTS have the same authority under the Parity Act, the act specifically sunsets NCUA's authority on December 31, 2001. According to NCUA officials, and a review of the legislative history surrounding this action, NCUA' s authority was sunset because the Parity Act focused primarily on Year 2000 computer problems that for the most part were expected to be resolved by the Year 2000. In addition, at the time the Parity Act legislation was being considered, one credit union trade association strenuously objected to strengthening NCUA's examination authority. As a result a compromise was reached that NCUA's authority would be sunsetted. Unless Congress amends the sunset provision, NCUA will not have the third-party oversight authority already provided to all other banking regulators. This is of particular concern because NCUA officials said that most credit unions offering Internet banking services lack in-house expertise and rely in part or totally on third-party firms to provide such services. In its comments on a draft of this report, NCUA officials

[15] The Parity Act, P.L. 105-162, 112 Stat. 32 (1998).

[16] The Federal Credit Union Act, (12 U.S.C. 1781 et seq.); Homeowners' Loan Act (12 U.S.C. 1464(d)).

stated that the agency plans to request Congress to amend the Parity Act to provide permanent supervisory authority over service providers.

Conclusions

Internet banking is a relatively new and rapidly growing activity that presents various types of risks that are of concern to banking regulators. At the time of our review, too few examinations of Internet banking had been conducted to identify the extent of potential Internet banking-related problems industrywide. Nonetheless, the examinations we reviewed revealed that some depository institutions had not taken all the necessary precautions to mitigate on-line banking risks. As banking regulators conduct more Internet banking examinations, they could usefully pool and share their findings to establish the extent of such problems industrywide. Sharing information on such findings could provide regulators with information to better understand the risks posed by Internet banking, allow regulators to better monitor industry trends, make more informed decisions on the scope and timing of examinations, and allocate limited resources among competing priorities.

At a time when Internet banking appears to be accelerating rapidly, banking regulators either have or plan to utilize a variety of means to identify depository institutions that are already offering Internet banking services. However, OTS and FDIC were the only regulators with procedures to gather centralized information on depository institutions' plans to offer Internet banking. OTS required that it receive advance notification of a depository institution's intentions, and FDIC required its examiners to collect information on an institution's Internet banking plans for inclusion in a centralized database. Such early identification procedures could enable regulators to provide more timely and specific risk management guidance and advice to depository institutions, and the procedures could also provide the regulators useful information to assess the scope and timing of future examinations and determine the need for examiners with information technology expertise. Given concerns that some institutions, particularly smaller ones, might move too quickly into Internet banking because of a desire to remain competitive, regulatory procedures that provide advance notification could be an effective means for regulators to proactively oversee this new and evolving banking activity.

With the exception of NCUA, the banking regulators were developing, testing, or implementing new on-line banking examination procedures and had conducted at least some examinations of institutions' Internet banking services. However, regulators' examination programs used differing methods in conducting and staffing Internet banking examinations. In

addition, differences exist in the degree to which examiners received training on how to examine such activities. As each regulator gains experience in the application of its examination procedures, it could be useful for the regulators to share their findings and approaches to help determine which methods yield the most effective and efficient results. In addition, NCUA, which has reported resource constraints due to the Year 2000 computer problem, has an obligation to help ensure the safety and soundness of credit unions' Internet banking operations and needs a reasonable strategy to do so once work on the Year 2000 computer problem diminishes.

The banking regulators' joint study of third-party firms providing Internet banking service is a good first step toward providing efficient and effective oversight, because it has the potential to lead to single coordinated examinations. However, it is too early to tell whether the study will result in a proposal to jointly examine third-party firms.

Also, NCUA's authority to examine firms providing Internet banking services expires on December 31, 2001. If this authority is not extended, NCUA will not have the third-party oversight authority provided to other federal banking regulators. Given the expected growth of Internet banking and its attended risks, the lack of such authority in the future could limit NCUA's effectiveness in ensuring the safety and soundness of the credit unions' Internet banking activities.

Matter for Congressional Consideration

Congress may wish to consider whether NCUA's current authority to examine the performance of services provided to credit unions by third-party firms is needed to ensure the safety and soundness of credit unions and, thus, should be extended beyond December 31, 2001.

Recommendations

To help regulators better understand the extent of risks posed by Internet banking and to more effectively evaluate examination methods and procedures, we recommend that, as more experience is gained in conducting examinations of Internet banking services, the heads of the banking regulatory agencies share information on the problems depository institutions have had in operating Internet banking activities as well as which Internet banking examinations methods and procedures they find to be most efficient and effective.

We also recommend that the Comptroller of the Currency and the Chairmen of the Board of Governors of the Federal Reserve System and the National Credit Union Administration establish procedures to obtain centralized information on institutions' plans to offer Internet banking.

They should use this information to (1) enhance monitoring of technological trends and innovations and thus their ability to assess emerging security and compliance issues; (2) provide more timely and specific risk management guidance to individual depository institutions, as necessary; and (3) augment the information used to plan the scope and timing of future examinations as well as to plan for the availability of examiners with appropriate information systems expertise.

To help ensure that reviews of the adequacy of Internet banking services provided by third-party firms are conducted in a cost-efficient manner, we recommend that, on the basis of the results of its research project, the Chairman of FFIEC through the FFIEC Task Force on Supervision develop plans and a timetable for the regulators' oversight of third-party firms.

To help ensure the safety and soundness of Internet banking at credit unions, we recommend that, as work related to the Year 2000 computer problem diminishes, the Chairman of NCUA expeditiously develop Internet banking examination procedures and begin to examine Internet banking-related activities offered by credit unions.

Agency Comments and Our Evaluation

FDIC, FRS, NCUA, OCC, OTS, and FFIEC provided written comments on a draft of this report, and their comments are reprinted in appendixes III through VIII. We also received written or oral technical comments and suggestions from these agencies that we have incorporated where appropriate.

In general, the five regulators and FFIEC concurred with the majority of the report's findings, conclusions, and recommendations. Three specific comments are discussed more fully below, and other more technical comments are discussed in the appendixes.

In response to our recommendation that it gather more timely information on institutions' plans to implement Internet banking, FRS commented that it has enhanced its monitoring and information gathering efforts through routine supervisory contacts, on-site examinations, and informal surveys. The agency also said that it was developing more powerful automation tools to aid more generally in examination planning, review, and reporting. However, FRS did not believe it had seen sufficient evidence on the need for a formal advance notification procedure or preimplementation regulatory reviews for Internet banking, which it said our report appeared to favor. We did not intend to prescribe the specific method(s) for gathering information on depository institutions' plans to offer Internet banking and have made some changes to clarify this point in our report.

The report describes two different methods employed by FDIC and OTS that provide them with useful information on depository institutions' plans to offer Internet banking. We continue to believe that implementation of one of these methods or an alternative method for obtaining centralized information on depository institutions' plans is necessary for regulators to (1) enhance monitoring of Internet banking technological trends and innovations and thus their ability to assess emerging security and compliance issues; (2) provide timely and specific risk management guidance to individual depository institutions, as necessary; and (3) augment the information used to plan the scope and timing of future examinations as well as to plan for the availability of examiners with appropriate information systems expertise.

FDIC and OTS also disagreed with an inference in the report that smaller institutions were more likely to encounter Internet banking-related problems. FDIC commented that it had observed numerous examples of small banks successfully employing sophisticated technology and believed that it is up to bank management, regardless of the size of the bank, to properly manage any new technology. OTS similarly commented that it did not believe that it is inherently more difficult for smaller banks to properly manage on-line and Internet banking activities and believed that such technology should not be exclusively the province of large institutions. We did not intend to broadly characterize small banks as being technologically deficient and agree that a bank's success in managing new technology depends on the strength of its management. Our review of 81 examinations of on-line banking assessments showed that examiners found that some small- and medium-sized depository institutions were not taking all of the prescribed precautions to mitigate Internet banking risks. However, the report specifically notes that too few examinations had been conducted to identify the extent of any industrywide Internet banking-related problems.

Finally, FRS concurred with the need for the regulators to develop supervisory plans with respect to outsourcing of Internet banking operations by depository institutions. However, it commented that it was not clear whether we were recommending a change in the current policies and practices regarding interagency examinations of service providers or some other form of regulatory oversight. Further, FRS stated that the report provided no evidence of problems at Internet vendor firms that would indicate the need to expand the regulators' responsibility to oversee directly all providers of Internet banking products and services, and it suggested that the report emphasize that banks, and not bank supervisors, bear the responsibility for monitoring and overseeing their service providers.

We are encouraged by the banking regulatory agencies' efforts to conduct a joint research project designed to develop a greater understanding of the oversight issues associated with assessments of Internet banking products and services offered to banks and thrifts by third-party firms. We believe that joint regulatory examinations of the operations of third-party firms providing depository institutions' Internet banking support services could increase the economy and efficiency of federal oversight of Internet banking activities. In this regard, our recommendation is intended to ensure that an interagency strategy, instead of individual agency strategies, is developed to examine those third-party firms. We also agree with FRS that banks, and not banking supervisors, are responsible for overseeing their service providers and have added language to the report to emphasize the responsibilities of the depository institutions. However, that does not negate the need for bank regulatory agencies to exercise proper supervision over Internet banking activities, whether performed by bank employees on the bank's premises or by a third-party firm off the bank's premises.

As arranged with your office, unless you announce the contents of this report earlier, we plan no further distribution until 30 days after the date of this letter. At that time, we will provide copies of this report to Representative John J. LaFalce, Ranking Minority Member of the House Committee on Banking and Financial Services; the Honorable John D. Hawke, Jr., Comptroller of the Currency; the Honorable Alan Greenspan, Chairman, Board of Governors of the Federal Reserve System; the Honorable Donna A. Tanoue, Chairman, Federal Deposit Insurance Corporation; the Honorable Norman E. D'Amours, Chairman, National Credit Union Administration; the Honorable Ellen S. Seidman, Director, Office of Thrift Supervision; the Honorable Laurence H. Meyer, Chairman, Federal Financial Institutions Examination Council; and other interested parties. We will also make copies available to others on request.

This report was prepared under the direction of Richard J. Hillman, Associate Director, Financial Institutions and Markets Issues, who may be reached on (202)-512-8678 if you or your office has any questions. Key contributors to this assignment are listed in appendix IX.

Sincerely yours,

Nancy R. Kingsbury
Acting Assistant Comptroller General

Contents

Tables

Abbreviations

FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FRS	Federal Reserve System
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
OTS	Office of Thrift Supervision

Objectives, Scope, and Methodology

Our objectives were to (1) describe risks posed by Internet banking and any identified industrywide Internet banking-related problems, (2) assess the methods used by regulators to track depository institutions' plans to provide Internet banking services, (3) determine how regulators examined Internet banking activities, and (4) determine the extent to which regulators examined firms providing Internet banking support services to depository institutions.

To identify the risks posed by Internet banking, we interviewed officials from the Federal Deposit Insurance Corporation (FDIC), Federal Reserve System (FRS), Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), and National Credit Union Administration (NCUA). We also obtained and reviewed agency documents, including advisory guidance provided to the industry and examiners on risks posed by Internet banking. We also interviewed 8 representatives from selected small-, medium-, and large-sized depository institutions and 11 representatives from related third-party firms to obtain their views on the scope and frequency of examinations and their assessment of risks posed by Internet banking. We selected these depository institutions based on their size and also on the probability that they would offer Internet banking. We identified the third-party firms from the examinations of Internet banking that we reviewed.

To determine the methods regulators used to identify depository institutions' plans to offer Internet banking services and to track growth and technological trends in Internet banking, we reviewed the five agencies' off-site monitoring procedures and interviewed their officials about the requirements each places on the institutions to provide Internet banking information. We also discussed with FDIC officials both their database on banks and thrifts with transactional Web sites and their Electronic Banking Data Entry System. In addition, we reviewed OTS' recently established requirement on advance notice of a thrift's plans to implement a transactional Web site.

To understand the regulators' safety and soundness and information systems on-line banking examination programs, which included Internet banking, we reviewed the on-line banking examination policies and procedures from each agency. In addition, we contacted the banking regulators to obtain their safety and soundness and information systems examination reports and workpapers pertaining to on-line banking. Since not all regulators track examinations of on-line banking operations, we could not ascertain how many on-line banking examinations had been conducted. FDIC was the only regulator that was able to tell us the number

of on-line banking examinations it completed during the period of our review. FRS did not maintain centrally on-line banking examinations conducted by the various Federal Reserve districts at the time of our review. As such, FRS officials directed us to the Reserve Banks, which maintain examination workpapers and are responsible for scheduling and conducting examinations. We discussed with the San Francisco District Bank staff their on-line banking procedures and related examiner training and obtained copies of examination work papers. We then contacted the New York District Bank, which was field testing the on-line banking procedures. To review additional examinations, we contacted the Atlanta and Kansas City District Banks.

OCC was not able to provide the number of on-line banking examinations conducted by its district offices. To obtain this information, we obtained OCC's listing of national banks with electronic activities and compared the names of the banks on this listing to a list of information system examinations conducted by OCC examiners during our review period. For those banks that appeared on both lists, we then requested a Profile Extract Report for each bank to determine the scope of examination activities. This method resulted in our identifying eight examinations with a scope that included Internet banking. Initially, OTS was also not able to tell us with certainty the number of on-line banking safety and soundness and information systems examinations conducted by its regional offices. To obtain this information, OTS contacted each office for the information because each office maintains its own information and determines its own examination schedule.

We were able to identify 81 on-line banking safety and soundness and information systems examinations conducted during the period June 1997 to August 1998. These examinations consisted of 62 FDIC examinations, 6 FRS examinations, 8 OCC examinations, and 5 OTS examinations. We reviewed available on-line banking examinations using a data collection instrument that allowed us to collect information on the extent and scope of Internet banking examinations and any exceptions noted in the workpapers. We then compiled this information in a database, determined the nature of the exceptions, and grouped them by type. Because the examination sample size was small, it was not possible to determine the adequacy of examination procedures, nor could we make any statistical generalizations regarding the safety and security of on-line banking operations.

To determine the extent to which regulators examined third-party firms that provided Internet banking services to depository institutions, we

interviewed regulatory officials and examiners involved with the examinations we reviewed, as well as 11 selected third-party firms. In particular, we gathered information on the authority regulators have to examine these third-party firms and the nature and extent of joint interagency examinations of traditional third-party data processing firms. With the assistance of our Office of the General Counsel, we researched the Bank Service Company Act and the Examination Parity and Year 2000 Readiness for Financial Institutions Act to determine the regulators' authority to examine and regulate third-party firms that provide Internet banking services.

Our early work on this assignment focused on PC banking, which included both direct-dial computer banking systems and Internet computer banking systems. As our work progressed, it became evident that institutions were moving from proprietary direct-dial to Internet banking and that many institutions initiating on-line banking were offering access via the Internet.

We did our work from April 1998 to May 1999 in Washington, D.C.; San Francisco, CA; Los Angeles, CA; Atlanta, GA; Kansas City, KS; and New York, NY, in accordance with generally accepted government auditing standards.

Banking Regulators Guidance on On-line Banking

Banking regulators have issued guidance to depository institutions on on-line banking. The guidance advises depository institutions that, before implementing on-line banking, including Internet banking, management should exercise due diligence and develop comprehensive plans to identify, assess, and mitigate potential risks and establish prudent controls. Most regulators have also issued policies and procedures to examiners. Table II.1 lists the guidance and policies and procedures published by the regulators.

Table II.1: Regulatory Guidance on On-line Banking

Regulator	Date	Guidance	Policies and procedures
FDIC	February 1997	N/A	Electronic Banking Safety and Soundness Examination Procedures
	December 1997	Security Risks Associated with the Internet	N/A
	August 1998	Electronic Commerce and Consumer Policy	N/A
FFIEC	December 1997	Guidance for Financial Institutions on Reporting Computer-Related Crimes	N/A
	July 1998	Guidance on Electronic Financial Services and Consumer Compliance	N/A
FRS	September 1997	Sound Practices Guidance for Information Security for Networks	N/A
	March 1998	N/A	Draft examination module on Retail Banking Via Personal Computers
	April 1998	Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations	N/A
NCUA	April 1997	Interagency Statement on Retail On-line PC Banking	N/A
OCC	February 1998	Technology Risk Management	N/A
	August 1998	Technology Risk Management: PC Banking	N/A
	August 1998	N/A	Draft General PC Procedures
	March 1999	Infrastructure Threats From Cyber-Terrorists	N/A

Regulator	Date	Guidance	Policies and procedures
OTS	June 1997	Statement on Retail On-line Personal Computer Banking	N/A
	October 1997	N/A	Updated bulletin on information technology examination guidelines that include the evaluation and control of risks associated with the Internet
	August 1998	N/A	Notice of modified proposed rulemaking regarding electronic banking operations
	January 1999	Regulation Requiring A Thrift's Written Notice Before Establishing A Transactional Web Site	N/A

Note: N/A equals not applicable.

Source: GAO analysis of information provided by FDIC, FRS, NCUA, OCC, and OTS.

Comments From the Federal Deposit Insurance Corporation

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

FDIC
Federal Deposit Insurance Corporation
Washington, D.C. 20429 Office of Internal Control Management

June 1, 1999

Mr. Richard J. Hillman
Associate Director
Financial Institutions and
Market Issues
U.S. General Accounting Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Hillman:

Enclosed is the FDIC Division of Supervision's response to the United States General Accounting Office draft report to Congress entitled, "ELECTRONIC BANKING: Enhancing Federal Oversight of Internet Banking Activities." We appreciate the opportunity to respond to the draft report. If you have any additional questions, please feel free to contact Cynthia Bonnette on (202) 898-6583, or Elroy Holden on (202) 736-3036.

Sincerely,

Robert M. Cittadino
Acting Director

Enclosure

cc: Dennis F. Geer
James D. Collins
Fred Selby
James A. Sexton
Simona L. Frank

FDIC
Federal Deposit Insurance Corporation
550 17th Street, NW, Washington, DC 20429
Division of Supervision

SUBJECT: GAO Draft Report - ELECTRONIC BANKING: Enhancing Federal Oversight of Internet Banking

Overview

This memorandum summarizes the Division of Supervision's official response to the GAO draft report entitled, "ELECTRONIC BANKING: Enhancing Federal Oversight of Internet Banking." As a leader among the regulatory agencies in developing and implementing examination procedures and guidance addressing electronic banking activities, we recognize the important supervisory implications of emerging technology in the financial services industry.

In general, we concur with the majority of the findings and observations outlined in the GAO's report. However, there are a few items that we feel are worthy of comment and we would also like to identify a few technical issues that may warrant minor modifications. With respect to the GAO's recommendations for future action, there is only one item that directly impacts the FDIC. This recommendation notes that it would be beneficial for the Federal banking agencies to share information on the problems depository institutions may experience in the area of Internet banking. We agree with this recommendation and will take steps to work with our counterparts in the other agencies to improve communication of our experience with examination methods and procedures. The remainder of this memorandum offers more specific comments on the report and is organized into three sections: FDIC's response to the GAO's recommendations, comments on substantive report issues, and comments of a technical nature.

Comments on the GAO's Recommendations for Federal Bank Regulators

The GAO makes several recommendations for Federal bank regulators; however, only one of these directly impacts the FDIC. This recommendation involves improved sharing of information and experience related to Internet banking activities among the agencies. We agree with this recommendation; however, we would like to note that the FDIC has already shared a great deal of information and examination resources with its regulatory counterparts. Specifically, we shared our draft technical workprograms covering the Unix Operating System, NT Operating System, and Firewalls with the other FFIEC agencies shortly after their development in 1998. We have also readily made available our information on transactional Internet banks. FDIC is frequently consulted by the other agencies for information on the number of banks with transactional web sites and we are pleased to offer this resource to others. The FDIC commits to working with the other Federal banking agencies to develop methods for sharing examination experience and other information related to Internet banking, as recommended by the GAO.

Comments on Substantive Report Items

At the outset of the GAO's review of online banking activities, the scope was defined as "PC banking" which includes direct dial-up computer banking systems and Internet computer

See comment 1.

banking systems. During all interviews and communications with the GAO, FDIC representatives responded to questions with the understanding that both forms of PC banking were being evaluated. However, the final report appears to concentrate solely on Internet banking. We recommend that a more detailed explanation of the scope's evolution be provided in the background section of the report.

Now on p. 12.

See Comments p. 26.

On page 18 of the report, the statement is made that certain regulators expressed the view that, "smaller institutions are more likely to encounter Internet banking related problems." The FDIC disagrees with the broad characterization of small banks as technologically deficient. In the FDIC's experience, we have observed numerous examples of small banks that have successfully employed sophisticated technology. We believe the ability to properly manage technology and maintain appropriate internal and external resources reflects on the quality of bank management. This can be effectively accomplished in banks of all sizes.

Now on p. 12.

See comment 2.

On page 18 of the report, a comment is made about human resource challenges facing the bank regulatory agencies with respect to Internet banking supervision. We would like to note that several recent initiatives have been undertaken by the FDIC to address this issue. Specifically, during late 1998 and early 1999 we have posted and filled several additional information systems examiner positions. We have also expanded the number of examiners in our Electronic Banking Subject Matter Expert Program by approximately 100% resulting in a cadre of over 200 specialists.

Now on p. 16.

On page 24 of the report, observations are made about several agencies that are in the process of developing and testing electronic banking examination procedures. We would like to note that while the FDIC's electronic banking safety and soundness examination procedures have been in place since early 1997, we continue to improve and enhance the program. Furthermore, the FDIC has developed three draft technical workprograms that address the Unix Operating System, the NT Operating System, and Firewalls. We have shared these draft workprograms with the other FFIEC agencies and are actively field testing them. We have also developed, tested, finalized and shared examination procedures addressing telephone banking systems.

Now on p. 18.

On page 28 of the report, it is noted that the banking agencies have issued or are developing procedures to address safety and soundness issues related to Internet banking. FDIC would again like to note that we have initially developed and are actively testing draft workprograms that address technical issues and concerns.

Now on p. 22.

See comment 3.

On page 35 of the report, a statement is attributed to "one regulator" that examinations of third party service providers may be unnecessary and may create "moral hazard." The FDIC would like to note that we do not agree with that statement. We would also like to suggest that, unless the statement can be directly attributed to a specific regulator (as their official position), it should be removed from the report.

The following are GAO's comments on the Federal Deposit Insurance Corporation's letter dated June 1, 1999.

GAO Comments

1. FDIC said that it understood the scope of our review to include both PC direct-dial and Internet banking. It suggested that the evolution of the report's scope be explained in more detail in the background section. We further discuss in appendix I why this report focused on Internet banking instead of reporting on PC banking which also includes direct dial-up computer banking systems.

2. FDIC stated that it has taken several additional steps to address the challenges facing Internet banking supervision, including developing new procedures, increasing the number of information systems examiners, and expanding agency training. A reference to these efforts, which occurred after the completion of our fieldwork, has been added to this report.

3. FDIC requested that the report attribute to the specific regulator the statement that examinations of third-party service providers may be unnecessary and may create "moral hazard." FDIC said that it did not agree with the statement because it raised questions about the need for examinations of third-party providers. While we believe that regulatory oversight of banking activities outsourced to third-party firms is essential, we also believe the referred-to statement reflects a useful observation—that depository institutions still have the basic responsibility to oversee their third-party firms. In the report, we have attributed the statement to FRS officials.

Comments From the Board of Governors of the Federal Reserve System

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

ALAN GREENSPAN
CHAIRMAN

June 11, 1999

Mr. Thomas M. McCool
Director
Financial Institutions and Market Issues
United States General Accounting Office
Washington, DC 20548

Dear Mr. McCool:

We appreciate the opportunity to comment on the General Accounting Office's draft report Electronic Banking: Enhanced Federal Oversight of Internet Banking Activities. The draft report provides a useful overview and comparison of the efforts underway in this area among the Federal Reserve and the other federal banking supervisory agencies as of the time of the GAO's review last year.

As the report notes, the Federal Reserve relies on a risk-focused approach to examinations, whereby our limited supervisory resources are focused on areas that pose the greatest risk to banking organizations that we supervise. To date, the growth of Internet banking has been fairly gradual, and we have not seen significant risks emerge. As Internet services become a more widespread and significant part of banking operations, however, we expect to devote more supervisory resources to examining these activities.

While we generally agree with the conclusions of the report, we offer the following comments on the GAO's recommendations that relate to the Federal Reserve:

First, we agree with the recommendation that the banking agencies should share their experience and expertise in developing effective approaches to the supervision of Internet banking activities. The member agencies of the Federal Financial Institutions Examination Council (FFIEC) have traditionally developed coordinated examination procedures and guidance in the information technology area. We expect that these efforts will continue with respect to emerging issues such as

See comment 1.

Internet banking, particularly when more examination experience has been gained and when resources currently dedicated to other priorities, such as Year 2000 reviews, become available.

Second, the draft report recommends that the banking agencies should obtain timely information on institutions' plans to implement Internet banking activities in order to monitor trends, determine the need for supervisory guidance, and plan the scope of future examinations. Over the last year, as Internet banking has become more widespread among the institutions we supervise, the Federal Reserve has enhanced its monitoring and information gathering regarding Internet banking through routine supervisory contacts, on-site examinations, and informal surveys. We are also developing more powerful automation tools to aid more generally in examination planning, review, and reporting.

See Comments pp. 25-26.

We have not seen the need for a formal advance notification procedure for Internet banking or other new technologies that banks may be considering for delivering banking services to their customers, a procedure that the GAO's report appears to favor. Such a procedure could impede banks' business decisions and create unnecessary regulatory burden. If the GAO views advance notification and pre-implementation regulatory review as critical supervisory tools for Internet banking, the GAO may wish to provide additional evidence in the report to support the need for significantly greater regulatory attention to this area relative to other banking activities.

See Comments pp. 26-27.

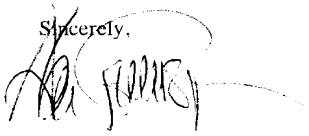
Third, the draft report recommends that the FFIEC develop plans and a timetable for regulatory oversight of third-party Internet banking vendors--on the basis of the results of an interagency research project. We would concur with the need for the banking supervisory agencies to develop supervisory plans with respect to outsourcing of Internet banking operations by banking organizations. However, it is not clear whether the GAO is recommending a change in the current policies and practices with respect to the scheduling and coordination of interagency examinations of service providers, or proposing some other form of regulatory oversight.[1] Although the GAO's report is useful in highlighting potential concerns with smaller banking organizations, it does not provide any evidence of problems at Internet vendor firms that would indicate the need to expand the banking agencies' responsibility to oversee

[1] See Federal Financial Institutions Examination Council, SP-1 "Interagency EDP Examination, Scheduling and Distribution Policy," as revised September 1991.

directly all providers of Internet banking products and services. The GAO's report should emphasize the fact that banks, not bank supervisors, bear the primary responsibility for monitoring and overseeing their service providers, as they do with bank customers and counterparties.

Thank you for the opportunity to review and comment on the draft report.

Sincerely,



The following are GAO's comments on the Board of Governors of the Federal Reserve System's letter dated June 11, 1999.

GAO Comments

1. FRS agreed with our recommendation on sharing of experience and expertise and added that FFIEC member agencies have traditionally developed coordinated procedures and guidance in the information technology area. While our recommendation did not specifically address the mechanism to be used to share experience and expertise, we agree with FRS' suggestion that having FFIEC member agencies develop coordinated examination procedures and guidance would be one way to do this. Such interagency coordination could not only develop a more effective and efficient oversight program but also provide common guidance to the industry.

Comments From the National Credit Union Administration

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

National Credit Union Administration

June 3, 1999

Mr. Richard J. Hillman
Associate Director, Financial Institutions
and Market Issues
United States General Accounting Office
Washington, DC 20548

Dear Mr. Hillman:

This is in reply to your letter, dated May 12, 1999, and accompanying report entitled, ELECTRONIC BANKING: Enhanced Federal Oversight of Internet Banking. I believe that the report effectively describes the risks imposed by Internet Financial Services. I offer the following general comments, which were not evident in the draft audit report:

See comment 1.

1. In 1997, NCUA provided on-line financing training to 45 percent of our examiner staff. Furthermore, we have more training classes planned for the remainder of 1999 to provide a total of 74 percent of examiner staff with on-line financial services training;

See comment 2.

2. We have developed a draft Electronic Financial Services Questionnaire, which was shared with Regional Offices and senior examiners. This questionnaire will form the cornerstone of our Internet Financial Services program to be implemented next year;

3. NCUA staff have been discussing the agency's Sunset provision contained in the Examination Parity and Year 2000 Readiness for Financial Institutions Act, and plan to request Congress amend the provision to provide permanent supervisory authority over service providers; and,

See comment 3.

4. In 1998, NCUA created and filled three Information Systems Officer positions. While these individuals have been primarily devoted to our Year 2000 project, Internet Financial Services has been designated as a high priority for them. They have attended, and will continue to attend electronic financial services training and interagency functions, and will provide such training to NCUA staff.

I also offer the following comments regarding specific sections of the audit report:

Now on p. 3, 2nd paragraph.

⇒ Page 5, 1st Paragraph - While NCUA has not formalized examination procedures specifically tailored to Internet Financial Services, our examiners inquire about new services or products planned by each credit union during routine safety and soundness examinations. If an Internet Financial Services program has been initiated or is planned, our examiners,

See comment 4.

1775 Duke Street - Alexandria, VA 22314-3428 - 703-518-6300

review the officials' process to ensure proper controls are in place or are planned. I recommend the report be amended to reflect this.

Now on p. 5, 2nd paragraph.

See comment 5.

⇒ Page 8, 1st Paragraph - NCUA works closely with State Supervisory Authorities, who are responsible for supervising state-chartered credit unions. As such, I suggest the wording used to describe NCUA as a regulator be amended to reflect this. Wording similar to that used to describe the FRS is appropriate for NCUA. Our agency's description should be re-worded as follows, "NCUA is an independent body responsible for insuring, examining, and supervising federal credit unions, and insuring state-chartered credit unions - working closely with state regulators to monitor the safety and soundness of institutions."

Now on p. 9, 4th paragraph.

See comment 6.

⇒ Page 14, 1st Paragraph - The draft report mentions, "..guidance was not tailored to an individual institution." This comment seems to imply the steps initiated to date by regulators, such as issuing white paper guidance or questionnaires on Internet Financial Services, is missing the mark. Initially, such a macro approach is necessary to provide basic guidance to over 11,000 federally insured credit unions. Once Internet Financial Service issues are uncovered during routine safety and soundness examinations, or special Internet Financial Services examinations, corrective guidance measures can be individually tailored to credit unions.

In closing, NCUA agrees the popularity of Internet Financial Services has increased dramatically, and with this comes a need to ensure credit union management provides adequate oversight of its Internet Financial Services program, and establish proper internal controls and audit procedures to minimize potential risk exposure. Additionally, NCUA will also address, through training, education, and exam procedures, issues pertaining to security and privacy. As NCUA is able to shift resources from our Year 2000 project, we intend to devote attention to Internet Financial Services.

I appreciate the opportunity to comment on the report. Should you have any questions, please feel free to contact me.

Sincerely,

Norman E. D'Amours
Chairman, National Credit Union Administration

EI\MJB:mjb

The following are GAO's comments on NCUA's letter dated June 3, 1999.

GAO Comments

1. NCUA commented that the draft of this report did not recognize the agency's on-line banking training in 1997 and 1999. The draft report did mention NCUA's 1997 training. We have added language to this report to recognize NCUA's planned training in 1999.

2. NCUA commented that the draft of this report did not recognize its development of a draft Electronic Financial Services Questionnaire. We did not specifically mention the questionnaire because it was included in the white paper on "cyber credit union services" that was mentioned in the draft report.

3. NCUA commented that the draft of this report did not recognize its creation of three information systems officer positions. We have added a discussion of these positions to this report.

4. While stating that the agency did not have formalized examination procedures specifically tailored to Internet banking, NCUA commented that the report should recognize that examiners did review Internet banking processes when they became aware of a credit union's Internet banking program. In the report we state that each of the regulators had policies requiring examiners to determine how various existing or emerging issues facing an institution or the banking industry affected the nature and extent of risks at particular institutions. Since NCUA lacked Internet examination policies and procedures and its examiners lacked training in Internet risks and mitigation controls, we do not believe that NCUA's approach adequately addresses the Internet banking risks facing credit unions.

5. NCUA commented that the draft of this report should be expanded to recognize its work with state regulators. We have made this change.

6. NCUA commented that the report seems to imply that guidance initiated to date by regulators is missing the mark. We did not intend to imply this. To the contrary, as NCUA said, regulatory guidance to the entire industry on risks posed by Internet banking is a necessary first step. However, as noted in a later section of the report, we encourage regulators to take the next step, which is to work with individual institutions that examiners find are not sufficiently prepared to mitigate risks posed by Internet banking.

Comments From the Comptroller of the Currency

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

Comptroller of the Currency
Administrator of National Banks

Washington, DC 20219

June 3, 1999

Mr. Richard J. Hillman
Associate Director, Financial Institutions and Markets Issues
General Government Division
United States General Accounting Office
Washington, DC 20548

Dear Mr. Hillman:

We have reviewed your draft audit report titled Electronic Banking: Enhancing Federal Oversight of Internet Banking Activities. The report was prepared in response to congressional concern about the safety and security of banking activities on the Internet, and the preparedness of banking regulators to help ensure safe and sound Internet banking operations. The report outlines the following conclusions:

- Regulators agree Internet banking presents risks and oversight challenges, however too few examinations have been completed to identify the extent of any industry wide Internet banking-related problems.
- As more examinations are completed, sharing information among the regulators could help them to better understand the extent of the risks posed by Internet banking and help them to allocate resources among competing priorities.
- Awareness of bank plans to offer Internet banking could help regulators provide timely risk management guidance and manage existing agency resources.

We agree that it would be beneficial to share any problem and best practice information obtained through the examination process with the other banking regulators. Currently, the FFIEC's Information Systems (IS) Subcommittee is gathering information on Internet banking service providers. The objective of this project is to produce an analysis of risks and make recommendations for supervisory oversight. The results of the analysis will be shared by the banking regulators and may result in joint regulatory examinations. Since the IS subcommittee provides a good forum for gathering and sharing information among the banking regulators, we will also pursue the possibilities of using this group as a focal point for sharing other Internet banking information among the regulators.

See Comment 1.

With regard to collecting aggregate information for banks planning to offer Internet banking, the OCC will investigate the following four options:

- Draft a regulation requiring banks offering transactional Internet banking activities to give notification to the OCC,
- Develop a bank survey that would be updated periodically,
- Develop a central database of information collected through the examination process, and
- Research industry reports on the current scope of Internet banking and future plans for these services.

Although we do not collect in a centralized database information for banks planning to offer Internet banking, or require prior notification, we do discuss plans for Internet banking with the banks we regulate. For every national bank, OCC examiners conduct a quarterly review. One of the objectives of the review is to determine whether significant changes in the bank's risk profile are evident. Per the OCC's examination handbook, examiners are to discuss with bank management:

- Significant changes in bank products or services, and
- Changes in technology, including operational systems, or plans for new products that involve new technology.

Thus, through the quarterly reviews, our examiners receive advance notice of plans by national banks to offer Internet services. We consider this information, as well as many other issues, when analyzing a bank's risk profile each quarter. Supervisory strategies and resource allocations are determined from the results of these analyses.

We take the challenges electronic banking poses to banks and their supervisors seriously. The OCC has:

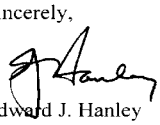
- Issued technology risk management and PC Banking guidance (OCC 98-3, OCC 98-38) to bankers and examiners,
- Provided training on electronic commerce and related technology to examiners in all of our districts,
- Drafted PC Banking examination procedures which will be issued before year end 1999, and
- Agreed to revise the Report of Condition as of June 30, 1999 to require banks to identify their URL designations,
- Been a leader in information sharing efforts with other Basle Committee supervisors.

We will continue to monitor electronic banking activities in our banks and to allocate the necessary resources available to ensure these activities are conducted in a safe and sound manner.

2

Thank you for the opportunity to review and comment on the draft report. We provided clarifying comments and editorial suggestions to your evaluators informally.

Sincerely,



Edward J. Hanley
Senior Deputy Comptroller for Administration
and Chief Financial Officer

3

The following are GAO's comments on the Office of the Comptroller of the Currency's letter dated June 3, 1999.

GAO Comments

1. While stating that the agency did not collect information centrally for banks planning to offer Internet banking or require advance notification, OCC commented that it does conduct a quarterly review of a bank's risk profile, which would include significant changes in bank products or services. According to OCC's guidance to examiners, examiners are to assess the overall condition and risk profile of the bank, but they need not answer or complete optional steps. Assessing changes in technology, such as Internet banking, is an optional step in the guidance. OCC's efforts to use other methods to collect information on a bank's Internet banking plans will enhance information gathered during its quarterly reviews and achieve the intent of our recommendation.

Comments From the Office of Thrift Supervision

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

Office of Thrift Supervision
Department of the Treasury
1700 G Street, N.W., Washington, DC 20552 • (202) 906-6590

Ellen Seidman
Director

June 3, 1999

Mr. Richard J. Hillman
Associate Director, Financial Institutions and Market Issues
Unites States General Accounting Office
Washington, D.C. 20548

Dear Mr. Hillman:

Thank you for the opportunity to review and comment on the GAO's draft report entitled, *Electronic Banking: Enhancing Federal Oversight of Internet Banking*. We appreciate the conscientious efforts of your team and Mr. Wong's management of the review.

We support the recommendations in the draft report. We will also cooperatively implement those recommendations, with the other agencies represented on the Federal Financial Institutions Examination Council (FFIEC), that pertain to the Office of Thrift Supervision's work in the Internet banking area. In fact, we are already working through the FFIEC to develop our examination approach for third party Internet service providers and to share information from our examinations of the Internet banking activities of thrift institutions.

Enclosed are staff comments on specific portions of the draft report that we discussed with Mr. Wong and understand that appropriate changes will be made to address these comments. Questions can be directed to Jennifer Dickerson at 202-906-5631, or Paul Reymann at 202-906-5645.

Sincerely,

Ellen Seidman

Enclosure

cc: Kane Wong, Assistant Director
General Accounting Office

Now on pp. 2 and 15.

See comment 1.

Now on pp. 6 and 7.

See comment 2.

Now on pp. 11 and 12.

See Comments p. 26.

Now on pp. 15 and 16.

See comment 3.

Office of Thrift Supervision
Staff Comments on Draft GAO Report
ELECTRONIC BANKING: Enhancing Federal Oversight of Internet Banking

1. Pages 4 and 22 refer to the efforts of the OTS and the FDIC to collect information on depository institutions' plans to provide Internet banking services. In addition to our transactional web site notice requirement, we require all thrifts to report their web site address in quarterly Thrift Financial Report filings. This information is essential to our off-site monitoring efforts. Since the time that the GAO began its review, we have also taken steps to enhance our national databases to collect more information on the electronic activities of thrifts, their subordinate organizations (e.g., subsidiaries and service corporations), affiliates, service providers, and software vendors. We believe these efforts should be mentioned in your report.

2. Pages 9 and 10 discuss various types of regulatory monitoring activities. The second bullet in this subsection should also mention that on-site compliance examinations are conducted to determine that institutions are following the requirements of the consumer protection laws and regulations, particularly as they apply to on-line and Internet banking products and services.

3. Pages 16, 17 and 18 discuss the results of the GAO's review of 81 examination reports that addressed on-line banking activities. Based on Table 2, it appears that there was one or possibly two of the total of five "large" institutions in the limited sample with "weaknesses" in this area. Given the limited sample of large institution examination reports available for this review, the table, accompanying narrative, and the results of interviews with "banking officials" suggest that it is inherently more difficult for "small" and "medium" sized institutions to properly manage on-line and Internet banking activities. We do not believe that is necessarily true; nor do we believe that on-line and Internet banking is, or should be, the province of large institutions. By working with third party service providers, monitoring those service providers (who, in addition to the institutions themselves are also examined by the agencies), and instituting internal risk mitigation strategies, we believe that smaller institutions can increase their competitive edge and better serve their communities through application of on-line and Internet banking. This same approach makes sense for large institutions, as well. Further, we do not know that examination results for large institutions would be remarkably different in the aggregate from those of smaller institutions, especially when one considers the relatively early developmental stage of on-line and Internet banking.

4. Pages 23 and 24 characterize the variety of methods used by the agencies to identify and monitor Internet banking activities as "after-the-fact." Although we agree that some of the methods cited can be characterized as "after-the-fact," we believe that we are taking a proactive approach as evidenced by our thrift notice requirement for transactional web sites and our requirement for each thrift to report its web site address in its quarterly Thrift Financial Report.

Page 1 of 2

Now on p. 18.

See comment 4.

Office of Thrift Supervision
Staff Comments on Draft GAO Report
ELECTRONIC BANKING: Enhancing Federal Oversight of Internet Banking

5. Page 28 suggests that OTS only examines Internet banking activities through our safety and soundness examination program. In fact, Internet banking activities are examined by Information Technology (IT) examiners in accordance with the interagency FFIEC Information Systems Examination Guidelines. Further, our compliance examiners also review Internet banking activities for adherence to consumer protection laws and regulations.

The following are GAO's comments on OTS' letter dated June 3, 1999.

GAO Comments

1. OTS commented that the draft of this report did not include information on its Web site reporting requirement and the agency's national database. We added language to this report discussing both points.

2. OTS commented that the draft of this report did not discuss compliance examinations that are conducted to assess an institution's compliance with consumer protection laws and regulations. We have added to this report a discussion of compliance examinations.

3. OTS referred to a section of the report that discusses after-the-fact methods used by other regulators to obtain information that OTS gathers through its advance notice requirement. OTS commented that it was proactively supervising thrifts as evidenced by its thrift notice requirement. We agree and believe that the report clearly reflects that.

4. OTS commented that the draft of this report suggested that the agency only examined Internet banking activities through its safety and soundness examination program. We added language to this report discussing compliance examinations. We also have added language to clarify that we are referring to safety and soundness and information systems examinations.

Comments From the Federal Financial Institutions Examination Council

Federal Financial Institutions Examination Council

2000 K Street, NW, Suite 310. Washington, DC 20006. (202) 872-7500. FAX (202) 872-7501

June 4, 1999

Mr. Thomas M. McCool
Director
Financial Institutions and Market Issues
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. McCool:

On behalf of the Federal Financial Institutions Examination Council (FFIEC), I appreciate the opportunity to comment on the General Accounting Office's draft report Electronic Banking: Enhanced Federal Oversight of Internet Banking Activities. The FFIEC member agencies have also been asked to submit comments on the draft report; these comments will be transmitted separately by the respective agencies.

The GAO's draft report includes one recommendation that pertains to the FFIEC:

> To help ensure the adequacy of Internet banking services provided by third-party firms in a cost-efficient manner, we recommend that, on the basis of the results of its research project, the Chairman of the FFIEC develop plans and a timetable for the regulators' oversight of third-party firms.

The FFIEC concurs with the need to ensure effective oversight of third-party vendors that provide Internet banking services and to complete the interagency research project cited in the report. This project is expected to produce an analysis of risks to supervised financial institutions from the use of third-party vendors of Internet banking services and to make recommendations regarding supervisory oversight for interagency consideration by the FFIEC's Task Force on Supervision. However, the nature of these recommendations will not be known until later this year, when the study group conducting the project is expected to complete its review. Thus, it would be premature to comment on the FFIEC's specific plans in this area.

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision

Mr. Thomas M. McCool
June 4, 1999
Page 2

Thank you for the opportunity to review and comment on the draft report.

Sincerely,

Laurence H. Meyer

Laurence H. Meyer
Chairman, Federal Financial Institutions Examination Council

cc: FFIEC Members
Richard Hillman, GAO

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision

GAO Contacts and Staff Acknowledgments

GAO Contacts

Richard J. Hillman, (202) 512-8678
Kane Wong, (415) 904-2123

Acknowledgments

In addition to those named above, Abiud Amaro, Bruce Engle, Robert Pollard, Nolani Traylor, and Karen Tremba made key contributions to this report.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Order by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touch-tone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested

(233562)