

GAO

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

---

January 1998

# ELECTRONIC BANKING

## Experiences Reported by Banks in Implementing On-line Banking



---

---

**General Government Division**

B-275222

January 15, 1998

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

Dear Mr. Chairman:

Information technology has increased the ability of bank customers to review their account balances, pay bills, or transfer funds between accounts while at home or work. This growing accessibility of on-line banking services through computers with direct dial-up or Internet connections, however, has led to heightened concerns about the vulnerability of bank and electronic payment systems. Accordingly, you requested that we examine the extent of on-line banking, federal regulatory efforts pertaining to on-line banking, and any problems posed by on-line banking for the security of Fedwire.<sup>1</sup>

As agreed with your office, we are studying these issues under separate reviews. This report summarizes the results of the first of these reviews, which addressed our objectives of identifying (1) the number of banks and thrifts (referred to as banks in this report) that reported they offer or plan to offer on-line banking and the types of services they reported<sup>2</sup> and (2) experiences reported by banks in implementing their on-line banking systems as well as efforts to mitigate associated risks. Our subsequent review will examine federal regulatory efforts pertaining to on-line banking and the security of Fedwire.

To gather this information, we surveyed 349 banks from May 1997 to June 1997, which included 219 banks that available information suggested were offering on-line banking services and 130 banks selected at random from the remaining banks in the United States. (See app. I for our telephone survey instrument.) We used this information to project to the total population of U.S. banks in two instances: (1) the number of banks offering and planning to offer on-line banking and (2) the number of banks offering specific types of on-line banking services.

---

<sup>1</sup>Fedwire is one of the nation's primary electronic funds transfer systems. Its network is used by participating banks to transfer the payments banks make to each other and their customers within the United States.

<sup>2</sup>For this study, a bank was considered to offer on-line banking if its customers, either retail or corporate, had access to bank services through computers equipped with dial-up or Internet access. Banks were not considered to offer on-line banking if they established Web pages on the World Wide Web solely to provide information on bank services and products.

---

In conducting our survey, we found that 185 of the banks were providing on-line banking services. We also found that many of the banks providing on-line banking were affiliated and that a single official was able to provide on-line banking information on more than one bank in our survey. Hence, 93 bank officials provided certain information on 185 banks offering on-line banking. Information provided on the 185 banks allowed us to determine (1) the channels used to deliver on-line banking services, (2) the reasons for implementing on-line banking, (3) whether on-line banking met or exceeded expectations, and (4) the electronic links that banks had with other payment systems. Certain information obtained from these 93 officials was limited to the banks that they directly represented. Specifically, we collected information for 93 banks on (1) problems experienced, (2) risk identification, and (3) risk mitigation efforts.

We also interviewed information security experts and federal agency and banking regulatory officials to identify potential risks and problems associated with on-line banking as well as basic security features that could help prevent such problems. In addition, we reviewed relevant technical literature and documents pertaining to these issues. We did not attempt to determine the effectiveness of security measures adopted by banks to prevent on-line banking-related problems, nor did we verify the information they provided. (See app. II for our detailed objectives, scope, and methodology.)

Our review was conducted between October 1996 and October 1997 in accordance with generally accepted government auditing standards. We provided a draft of this report to the Federal Reserve System (FRS), Office of Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and the Department of Justice for comment. The four regulatory agencies' written comments are discussed at the end of this letter and are reprinted in appendixes III through VI. The Department of Justice's Federal Bureau of Investigation (FBI) provided technical comments, which we incorporated, where appropriate.

---

## Results in Brief

As of June 1997, we projected that an estimated 7 percent of U.S. banks ( $\pm 3$  percent sampling error<sup>3</sup>) offered on-line banking services, which most typically allow customers to access account information and transfer funds between their accounts. On the basis of plans reported to us by

---

<sup>3</sup>All of the projected estimates made in this report have sampling errors which are calculated at the 95 percent confidence level.

---

surveyed banks, we projected rapid growth in on-line banking over the next year and a half as the number of U.S. banks implementing on-line systems is expected to increase about fivefold nationwide. Bank officials identified three primary reasons for their banks' offering on-line banking: keeping existing customers, remaining competitive, and attracting new customers. Officials of 170 of the 185 surveyed banks (92 percent) currently offering on-line services said their on-line banking systems had met or exceeded their expectations.

Although an estimated 47 percent of U.S. banks ( $\pm$  15 percent) reported that they expect to offer on-line banking services by the end of 1998, introduction of this technology brings with it some attendant risks. Responses from 93 of the banks we surveyed indicated that some had not performed risk assessments, which can serve as a tool to protect the integrity, confidentiality, and availability of their on-line operations. Although 65 of the banks (70 percent) responded that their banks had assessed the potential risk exposure of their systems, 12 banks (13 percent) reported that they had not assessed these types of security risks, and another 16 banks (17 percent) said they did not know if they had assessed such risks. Risk assessments are an important step in protecting an on-line system so that appropriate controls can be implemented to mitigate risks.

Although many of the 93 banks that responded to this question reported they had implemented controls to prevent unauthorized access to their on-line systems, 9 banks (10 percent) said they lacked firewalls for restricting access between computer networks. Ten banks (11 percent) reported that they did not have such basic security features as detection software for computer viruses and worms. Many of the 93 banks that responded indicated they had experienced lapses in service (38 percent), security problems (30 percent), or system operation difficulties (36 percent). With the projected rapid growth in on-line banking, it is important that banks take those steps necessary to ensure they protect their on-line banking operations.

---

## Background

Banks have provided electronic banking services to customers for a number of years using such familiar access devices as telephones and automated teller machines. Corporate customers also have had access to on-line banking features by dialing into a bank's system using proprietary software. More recently, retail customers have been able to access their bank accounts from computers in their homes or workplaces by

---

connecting to on-line banking systems. Such systems offer services that enable individuals or businesses to verify their account balances, apply for loans, authorize bill payments, or transfer funds between their accounts and from other banks. Some on-line banking systems also let customers reorder checks, review their account histories, stop check payments, or facilitate wire transfers.

Customers with computer modems can access their banks' on-line banking computer systems in one of several ways. Some of them can use banking software installed on their personal computers, local area networks, or mainframe computers to connect to the banks' on-line banking systems. Other customers may be able to access their banks' on-line banking systems by dialing into an Internet service provider and accessing the banks' World Wide Web<sup>4</sup> sites. Banks may operate their on-line banking systems in-house or contract out the operation of these systems to third-party vendors.

After connecting to an on-line banking system, a customer generally enters a personal identification number and a password. Typically, customers must go through this step to identify themselves every time they sign on to the on-line banking system. According to bank officials, once customers have confirmed that they are legitimate account holders, they can proceed to use their computers to initiate the desired transactions, and the on-line banking system processes and routes the transaction data as needed to carry it out.

---

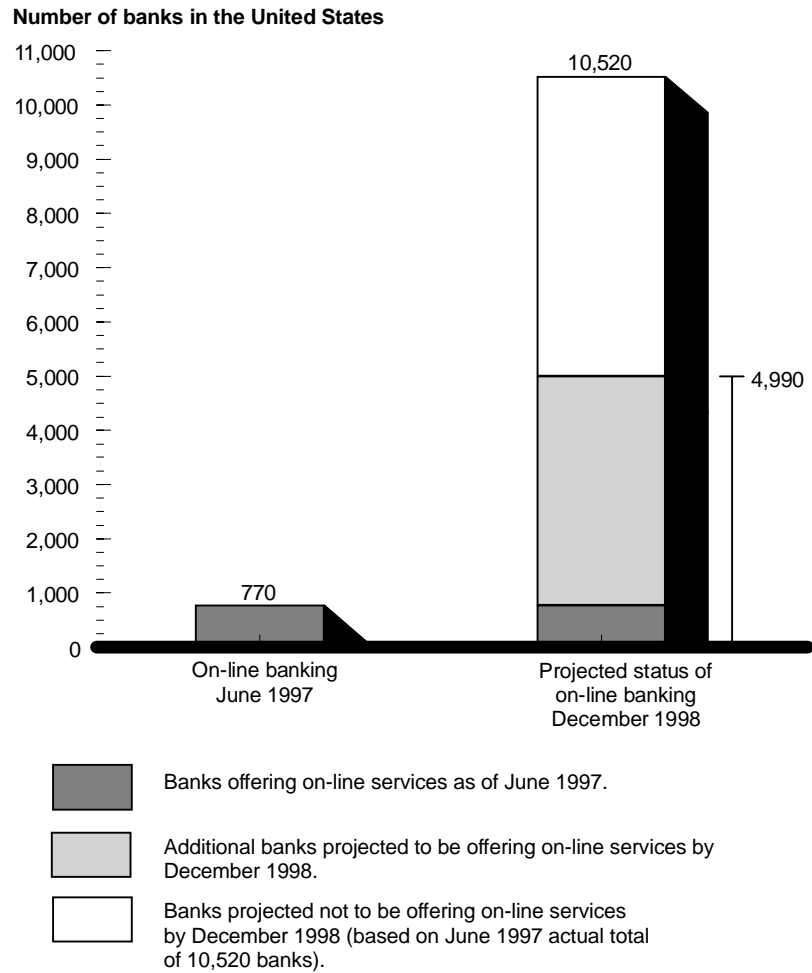
## Number of Banks Implementing On-Line Banking Systems Growing Rapidly

Our survey results indicated that the number of banks implementing on-line banking systems is planned to grow about fivefold by December 1998. We estimate that about 770 banks, or 7 percent ( $\pm 3$  percent) of the approximately 10,520 banks active in the United States at the time of our survey, had implemented on-line banking as of June 1997. According to the responses to our survey results, an estimated 4,990 banks, or about 47 percent ( $\pm 15$  percent) of the banks in the United States, plan to offer some type of on-line banking service to their customers by the end of 1998. This estimate of 4,990 banks includes the 770 banks offering on-line services in June 1997 as well as 4,220 banks projected to begin offering such services by December 1998 (see fig. 1).

---

<sup>4</sup>The World Wide Web is a portion of the Internet through which information is exchanged via text, graphics, audio, and video that can be accessed with the use of a browser or search engine software.

**Figure 1: Projected Rapid Growth of On-Line Banking Between June 1997 and December 1998**



Note 1: The above numbers do not include banks establishing Web pages on the World Wide Web solely to provide information on bank services and products, rather than to allow customers to access banking services.

Note 2: The sampling error for the estimate of banks currently offering on-line banking is 3 percent. Sampling errors for the other two estimates (4,220 and 4,990) are both ± 15 percent.

Source: GAO analysis of survey results.

Although U.S. banks offer a wide range of services on-line, reviews of account information and funds transfers between a customer's accounts

were the most common services reported to be available to bank customers at the time we conducted our survey in June 1997. Our analysis indicated that over 99 percent ( $\pm 1$  percent) of the estimated 770 banks offering on-line banking allowed their customers to check their balances, and the same percentage allowed customers to transfer funds between their own accounts. In comparison, 54 percent ( $\pm 24$  percent) of these banks reported allowing their customers to transfer funds to other banks (see table 1).

**Table 1: Projected On-Line Banking Services Offered by Banks as of June 1997**

Services	Weighted estimate of banks saying "yes"	
	Percent	Number
Review account balance	99%	768
Transfer funds between customer's accounts	99	762
Bill payment	37	281
Transfer funds to other banks	54	413
Accept loan applications	14	106
Other <sup>a</sup>	64	496

Note 1: Based on GAO's estimate that 770 banks offered on-line banking as of June 1997.

Note 2: Sampling errors by offered services are: review account balance (<1 percent), transfer funds between customer's accounts (<1 percent), bill payment ( $\pm 19$  percent), funds transfers to other banks ( $\pm 24$  percent), accept loan applications ( $\pm 7$  percent), and other ( $\pm 22$  percent).

<sup>a</sup>Other on-line services included check reordering and stop check payment orders.

Source: GAO analysis of survey results.

As part of our survey, we asked officials from all 185 banks we surveyed that reported offering on-line banking for more detailed information on the channels they used to deliver on-line services. Their survey responses indicated that most banks used software that enables customers to directly connect to the banks' own on-line systems or a vendor's system. Of the 185 banks, 116 (63 percent) reported using software that provides for a direct connection to a vendor's system, and 79 (43 percent) reported using software that allowed customers to directly connect to their banks' on-line computer systems. More than half of the banks reported they offered on-line banking by allowing customers to connect with their on-line systems through the Internet (see table 2).



**Table 2: Surveyed Banks Reporting Use of Various Delivery Channels for Their On-Line Banking Operations**

<b>Delivery channel</b>	<b>Percent</b>	<b>Number</b>
Direct connection	91%	168
Personal computer banking software allowing for direct dial-in to on-line banking system operated by third-party vendor	63	116
Personal computer banking software allowing for direct dial-in to bank's on-line banking system	43	79
Internet	54	100
Internet Web site maintained by bank, third-party vendor, or affiliated bank	49	91
Internet service provider (e.g., Prodigy, America OnLine)	31	57

Note 1: Banks may use more than one delivery channel in offering on-line services.

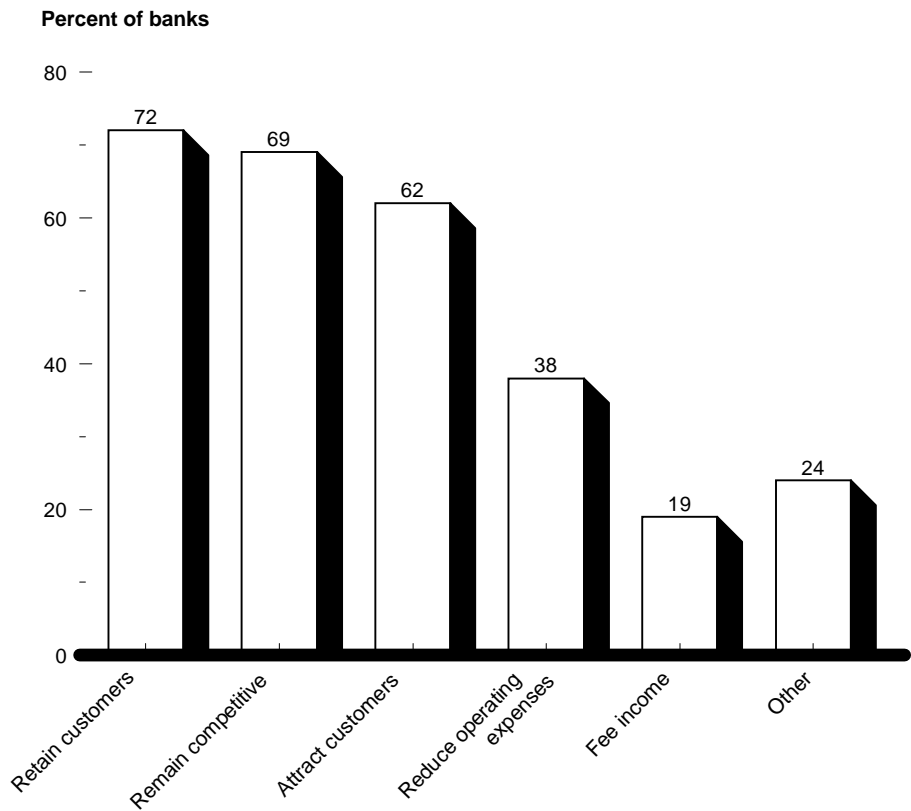
Note 2: Based on information for 185 banks.

Source: GAO analysis of survey results.

We also asked officials who represented the 185 banks that reported offering on-line banking for their reasons for implementing their on-line banking systems. Key reasons bank officials cited for their banks' decisions to offer on-line banking involved the intention to remain competitive with other banks, retain customers, attract new customers, reduce operating expenses, or generate fee income.

Although 133 banks (72 percent) indicated they implemented on-line banking to retain customers, two other motivating factors—remaining competitive and attracting new customers—were cited almost as often. Other motivating factors, such as keeping up with banking technologies and the desire to offer customers alternative delivery channels, were cited by some banks (see fig. 2). Banks planning to offer on-line banking responded similarly to questions about motivating factors. Among the 36 banks planning to implement on-line banking by December 1998, the desires to remain competitive and to retain their customers were the most frequently cited motivating factors.

**Figure 2: Reasons Cited by Surveyed Banks for Implementing On-Line Banking**



**Reasons for implementing on-line banking**

Note: Based on information for 185 banks.

Source: GAO analysis of survey results.

Survey responses for 185 banks indicated that their on-line banking systems generally met or exceeded their expectations (see table 3). Half of the banks reported that their expectations were met, and another 77 banks (42 percent) said that their expectations were exceeded. Bank officials commonly reported that customer usage of on-line banking systems met or surpassed initial targets. One bank official told us that about 400 new employees were hired to meet the customer demand for on-line banking.

In a few instances, banks' experiences fell short of expectations. In one case, a bank official told us that customer use was much lower than expected. The official said that the rural location of the bank may have been a contributing factor.

**Table 3: Extent to Which Surveyed Banks That Reported On-Line Banking Said Their Expectations Were Met**

<b>Expectations</b>	<b>Percent</b>	<b>Number</b>
Exceeded	42%	77
Met	50	93
Fell short	3	6
Too early to tell	4	7
Don't know	1	2

Note: Based on information for 185 banks.

Source: GAO analysis of survey results.

### **Some Banks That Reported Offering On-Line Banking Said They Did Not Conduct Risk Assessments**

On-line banking presents a wide range of potential risks, according to information security experts and banking regulators. On-line banking can expose bank and customer information and transactions to risks from electronic interception, data corruption, or fraud because of the widespread access characterizing these systems. An important step in ensuring the integrity of an on-line system is ascertaining the vulnerabilities and threats potentially affecting individual on-line systems and establishing compensating internal controls to mitigate risks. Accordingly, information security experts and federal banking regulators suggest that banks analyze risks associated with their on-line banking systems and evaluate whether their security policies protect the integrity, confidentiality, and availability of their on-line operations and are capable of limiting or mitigating identified risks.<sup>5</sup>

Information security experts and federal regulators stated that although risk assessments specific to on-line banking are not a federal banking requirement, such assessments are a useful tool for identifying, measuring, monitoring, and managing potential risks. Assessments can help banks evaluate the seriousness of such potential problems as viruses, unauthorized access into banking systems, and lost transactions.

<sup>5</sup>The Federal Reserve System and the Office of Thrift Supervision have indicated that they expect financial institutions that provide services over the Internet to analyze risks related to the security of customer information and other data and to use the results of their risk analyses to make appropriate modifications to their on-line systems and implement necessary controls and monitoring tools to mitigate risks.

---

Our survey results indicated that 54 of the 93 banks (58 percent) that reported having on-line systems had conducted formal risk assessments of their on-line banking systems. However, 12 banks (13 percent) said they had not performed such assessments. Another 16 banks (17 percent) did not know if they had performed risk assessments of their on-line banking systems. The remaining 11 banks (12 percent) reported holding limited or informal discussions about potential risks of on-line banking. Two bank officials we interviewed explained that their banks did not perform a risk assessment because the latest industry information their banks had obtained on the security of on-line banking systems suggested that such systems were secure.

To help prevent unauthorized access to on-line banking systems, information security experts and regulatory officials emphasize the importance of banks' implementing mitigating controls, such as restrictions on access, secure firewalls that restrict access between computer networks, intrusion detection software, and tests of on-line banking system vulnerability. The risk mitigation process can be used to not only identify controls necessary to protect an on-line system, but also to weigh the cost of implementing controls against their benefits. The Federal Reserve Bank of New York notes that the level of protection of an Internet site should be commensurate with the degree of risk associated with the level of services offered and the value of assets at risk. For example, the cost of implementing strong authentication controls, through techniques such as digital signatures, would tend to be more appropriate for a bank that offers extensive on-line banking services, such as bill payment and funds transfers to other banks, than for a bank that limits its on-line banking services to the review of account balances.

---

## **Some Banks Reported Problems With Their On-Line Banking Systems**

For the 93 banks that they directly represented, we asked bank officials for information on the types of problems they had experienced with their systems, whether other banking systems were connected to their systems, and the types of controls they had in place to mitigate risks. Many of the 93 reported that they had experienced service availability lapses (38 percent), security problems (30 percent), or operational problems (36 percent) with their systems (see table 4). We could not assess the significance or underlying causes of these apparent problems because we did not examine individual banks' systems and processes. Moreover, we did not determine the appropriateness of a bank's mitigating features, which could vary depending on the complexity of the on-line banking system as well as the types of services offered.

**Table 4: Extent to Which Banks Reported Various On-Line Banking Problems**

<b>Problems</b>	<b>Percent</b>	<b>Number</b>
<b>Service availability difficulties</b>	<b>38%</b>	<b>35</b>
Denial/disruption of system	35	33
Difficulties in tracking on-line banking transactions as transmission volume increases	4	4
<b>Security difficulties</b>	<b>30</b>	<b>28</b>
Unauthorized access attempts <sup>a</sup>	19	18
Transactions lost during transmission	15	14
Proving valid customers are using on-line banking system	4	4
Employee sabotage of on-line banking system <sup>b</sup>	1	1
Theft of PINs or passwords	1	1
Viruses and worms <sup>c</sup>	1	1
<b>Operational difficulties</b>	<b>36</b>	<b>33</b>
Upgrade or replacement of software	22	20
Staffing & training	29	27
<b>Other difficulties<sup>d</sup></b>	<b>22</b>	<b>20</b>

Note 1: The list of problems is not comprehensive, and some reported problems could be classified under more than one category.

Note 2: Based on information from 93 banks.

<sup>a</sup>Only 1 of the 93 banks reported an instance of successful unauthorized entry into its on-line banking system.

<sup>b</sup>According to the National Institute of Standards and Technology, examples of computer-related employee sabotage include theft of customer data, destruction of hardware, incorrect data entry, and deletion or alteration of data.

<sup>c</sup>A virus is a computer program that replicates itself by attaching copies of itself to existing computer programs. The new copy of the virus is executed when a user loads a program or opens an electronic mail message attachment. A worm, which does not require a host program, is a self-replicating computer program that commonly uses network systems to propagate to other host systems.

<sup>d</sup>Other problems reported by bank officials include software or hardware not working as designed and customers attempting to fraudulently transfer funds between their accounts.

Source: GAO analysis of survey results.

## Service Availability Problems

One category of on-line banking problems reported by banks involved lapses in the availability of services. Thirty-three of the 93 banks (35 percent) reported that their on-line banking systems had experienced service availability problems involving the denial or disruption of service (see table 4). Such problems frequently can be caused by a breakdown in

---

the hardware or software supporting the system, which in turn may be the result of a design defect, insufficient system capacity, or a mechanical breakdown. Almost half of the 33 banks that reported experiencing denial or disruption of service indicated that some type of damage resulted, such as loss of customer confidence or customers closing their accounts.

Banks should be able to prevent or at least partly mitigate service availability problems by monitoring vendor systems and by adopting emergency or contingency plans, which are designed to allow banks to continue their on-line banking operations after a system failure. Forty-one of the 58 surveyed banks (71 percent) that relied on vendors to operate their on-line systems said that they monitored vendor systems as a mitigation measure. Two of the 58 banks (3 percent) said that they request certifications or guarantees from vendors that proper controls are in place to mitigate potential risks. A few other banks that reported they did not monitor their vendors' systems said that they relied on the vendors to ensure that emergency or contingency plans were in place to guard against, among other things, lapses in the availability of services. Seventy-nine of the 93 banks (85 percent) we surveyed said they had emergency or contingency plans in place (see table 5).

**Table 5: Percent of 93 Banks That Reported Having Implemented Various Features Designed to Mitigate Problems**

<b>Problem</b>	<b>Mitigating feature in place</b>	<b>Yes</b>	<b>No</b>	<b>Don't know</b>	<b>Not applicable</b>
Unauthorized access attempts	Access restricted after at least 3 failed entry attempts	89%	7%	4%	
	Firewalls in place <sup>a</sup>	79	10	12	
	Intrusion detection software	45	23	32	
	Penetration testing	51	27	23	
Staffing and training	On-line banking guidelines established	88	9	3	
	On-line banking training provided	96	1	3	
Denial/disruption of service	Emergency or contingency plans <sup>b</sup>	85	11	4	
	Bank oversight of vendor <sup>c</sup>	44	10	9	38%
Employee sabotage	Separation of system control duties	86	5	8	1
Viruses and worms	Detection software	70	11	18	1
Transactions lost during transmission	Audit logs and/or reports generated	90	4	5	
Difficulty in tracking on-line banking transactions as volumes increase	Audit logs routinely reviewed	85	5	0	10
Outdated software	Software update control program	66	15	7	13
Theft of PINs or passwords	Codes or encryption used	83	9	9	
Proving authorized customers are using on-line banking systems	Digital signature <sup>d</sup>	8	81	12	

Note 1: Based on information from 93 banks.

Note 2: Row percentages do not always sum to 100 due to rounding.

Note 3: This table contains examples of features that banks can use to mitigate potential problems and is not meant to be an all-inclusive list.

<sup>a</sup>Fifty-five of the 73 survey banks (75 percent) that had firewalls reported that their firewalls distinguished among customers, vendors, and/or internal systems.

<sup>b</sup>Emergency or contingency plans can be used to respond to natural disasters, acts of terrorism, sabotage, or power disruptions of an electronic banking system.

<sup>c</sup>The percentages for this mitigation feature were calculated on the basis of the responses of the 58 surveyed banks that provided their on-line banking services through third-party vendors.

<sup>d</sup>Digital signatures are generally recognized as being a more secure and sophisticated authentication method than personal identification numbers and passwords.

Source: GAO analysis of survey results.

---

## Security Problems

Of the 28 surveyed banks that reported experiencing security problems, almost two-thirds involved attempts at unauthorized access (see table 4). Experts described a number of methods that can be used to try to gain unauthorized entry for illicit purposes. For instance, personal computer banking software may be taken apart to find its vulnerabilities or may be used to access the bank system to decipher the bank's payment protocol. Another method involves the use of devices to capture bank information as it travels across telecommunication lines.

Two of the 18 banks that reported there had been attempts at unauthorized access could not tell us how many attempts had been made on their systems, because they did not have systems in place for monitoring such attempts. However, 1 bank reported that up to 50 attempts at unauthorized access had been made on its system. One bank we surveyed reported a successful unauthorized access into its internal systems.

The number of successful unauthorized access attempts involving the banking industry has been difficult to determine. According to the FBI, cross-industry sector surveys indicate that the number of computer intrusions and the amount of financial losses resulting from those intrusions are rapidly increasing. Although segments of the financial services industry are included in many of these studies, none focus solely on financial institutions or the banking industry. Nonetheless, a FBI official told us that he knew of many alleged attempts at unauthorized entry into on-line banking systems. However, the FBI has not been able to substantiate through the banking industry or other intelligence sources whether successful unauthorized entries are actually occurring either. He attributed the difficulty his agency and others have had confirming whether unauthorized entries are occurring to various factors, including banks' reluctance to disclose unauthorized entry incidents, the inability of banks to detect or recognize such incidents, and the lack of a separate category for banks to report successful or attempted unauthorized entries on the forms required to be filed on known or suspected violations of federal criminal law. To improve the reporting of computer-related crimes, the FBI, working with the federal banking agencies and other federal law enforcement agencies, recently issued guidance providing further definitions and specific examples for financial institutions to assist them in reporting unauthorized computer entries.

Eighty-three of the banks (89 percent) we contacted reported that they restricted access after three unsuccessful entry attempts into their



---

systems (see table 5). Although 73 of the 93 banks (79 percent) indicated that either their systems or the vendors' systems had firewalls in place, 12 of the 73 (16 percent) reported that their firewalls did not distinguish among customers, vendors, and/or internal systems.

Fewer of the banks reported that they had conducted vulnerability tests or had installed intrusion detection software. Twenty-five of the 93 banks (27 percent) reported that tests were not performed to see whether their on-line systems were subject to penetration. Fewer than half said that intrusion detection software was in place.

Problems involving transactions that were lost by the bank or by the vendor operating the bank's on-line banking system reportedly occurred less frequently than unauthorized access attempts. Fourteen of the 93 banks (15 percent) indicated that on-line banking transactions have been lost (see table 4). Officials reported a variety of reasons for these losses, such as customers not knowing how to use their on-line banking software and system failures. One bank official told us that lost transactions had led to a financial loss, and two others reported reduced customer confidence in the banks' on-line systems as a consequence.

To help prevent losses of on-line banking transactions, Federal Deposit Insurance Corporation guidelines and security experts recommend that audit logs and reports be generated and subsequently routinely reviewed. Monitoring these reports can provide bank officials with an indication of problems requiring their attention, according to security experts. As shown in table 5, 79 of the 93 banks (85 percent) reported that audit reports were both generated and routinely monitored.

Some federal agencies and information security experts have pointed out that unauthorized entries into a bank's on-line banking system can also entail risks for other financial institutions with which the bank has electronic links. They point out that an individual gaining access into one bank's system could potentially also gain access to other systems for illicit purposes if the bank's on-line banking system is electronically linked to other financial institutions and computer systems. Recently issued guidance by the Federal Reserve Bank of New York<sup>6</sup> warns that the Internet potentially exposes a bank's on-line system, and in turn its internal computer network, to worldwide attack and compromise.

---

<sup>6</sup>Sound Practices Guidance on Information Security, Federal Reserve Bank of New York, September 1997.

Many of the 185 banks in our survey with on-line systems reported having electronic links with various other computer systems (see table 6). Most said their on-line systems were linked to a vendor’s system or to the banks’ business partners. To a lesser extent, they reported their on-line systems were electronically linked to the Fedwire or other computer systems. At one bank we contacted, an individual was able to break into the bank’s on-line system and use its electronic connection to transfer funds fraudulently to other financial institutions.

**Table 6: Surveyed On-Line Banks Reporting Electronic Links Between Their On-Line Banking System and Other Computer Systems<sup>a</sup>**

<b>Links to other computer systems</b>	<b>Percent</b>	<b>Number</b>
Fedwire <sup>b</sup>	15%	28
Clearing House Interbank Payment System (CHIPS) <sup>c</sup>	16	29
Society for Worldwide Interbank Financial Telecommunications (S.W.I.F.T.) <sup>d</sup>	17	31
Vendor systems <sup>e</sup>	65	120
Other financial institutions	17	31
Bank’s business partners	32	59

Note: Based on information for 185 banks.

<sup>a</sup>For more information about computer systems mentioned in this table, see *Payments, Clearance, and Settlement: A Guide to the Systems, Risks, and Issues* (GAO/GGD-97-73, June 20, 1997).

<sup>b</sup>Fedwire serves approximately 9,500 depository institutions.

<sup>c</sup>CHIPS is the main U.S. wire transfer system for processing international U.S. dollar transfers. CHIPS is operated by the New York Clearing House Association and serves 95 foreign and domestic banks representing 28 countries.

<sup>d</sup>S.W.I.F.T. is an international financial payment cooperative organization that operates a network that facilitates the exchange of payment and other financial messages between financial institutions throughout the world.

<sup>e</sup>Vendor systems are on-line banking systems operated by a third party under contract to a bank.

Source: GAO analysis of survey results.

## Operational Problems

The third category of problems reported by the 93 banks involved operational problems, most of which involved staffing or training problems or difficulties in upgrading or replacing outdated software. Twenty-seven of the 93 banks (29 percent) reported that they had experienced staffing and training problems (see table 4). Some banks reported that their employees lacked the computer-related technical backgrounds needed to handle on-line banking problems. One bank official said that the volume of customer inquiries far exceeded the ability

---

of his bank's current staff to handle them promptly. Another bank said that staffing and training problems led to a loss of customer confidence.

To reduce difficulties stemming from inadequate or limited staffing or training, information security experts and federal regulators have suggested that banks should equip their staffs to respond to problems affecting on-line systems by establishing guidelines or providing associated training. Nearly all of the 93 banks reported providing training to staff (see table 5). One bank that attributed its staffing problems to the newness of its on-line banking system believed that such problems would decrease over time.

Twenty of the 93 banks (22 percent) reported operational difficulties relating to the need to upgrade and replace outdated software (see table 4). One bank explained that it must at least partly rely on its customers to buy banking software upgrades on their own. According to information security experts, problems stemming from a failure to upgrade and replace software can pose a risk to banks. For instance, as software becomes dated, it becomes easier for someone to exploit the vulnerabilities of software programs.

Information security experts stated that software update control programs can identify which customers have not updated their software and automatically upgrade the access software installed on a customer's personal computer. Sixty-one of the 93 banks (66 percent) reported that they had installed some type of a software update control program (see table 5). A few banks told us that they had not yet implemented this type of measure because of the newness of their banks' systems.

---

## Conclusions

Our analysis indicated that the number of banks implementing on-line banking systems is planned to increase about fivefold by December 1998. Although responses of most of the banks we contacted indicated that their on-line banking systems had met or exceeded their expectations, the introduction of on-line banking technology exposes banks and their customers to risks from electronic interception, data corruption, and fraud. Accordingly, information security experts and federal banking regulators suggest that banks assess risks associated with their on-line banking systems and take measures to protect against them. Although many of the banks we surveyed had conducted such assessments, others had not and, thus, lacked assurance that they were taking appropriate mitigating measures to protect their on-line banking systems. Moreover,

---

over two-thirds of the banks reported some combination of service availability, security, or operational problems with their on-line banking systems. Although difficulties such as these can be expected with the introduction of new banking technology, our work suggests that banks will face considerable challenges implementing and maintaining secure and dependable banking services as on-line banking in the United States continues to grow.

---

## Agency Comments and Our Evaluation

The Federal Reserve System, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and Office of Thrift Supervision provided written comments on a draft of this report, and their comments and our additional responses are reprinted in appendixes III through VI. In addition, these four agencies and the FBI provided technical comments, which we have incorporated where appropriate.

The four regulatory agencies generally found that the report provided useful information and insights on the challenges faced by banks and thrifts when implementing and maintaining on-line banking services. FRS and OCC expressed concerns about the presentation of certain data in the report. Specifically, FRS believed it would be useful to differentiate between problems caused by hardware, software, or operational failures and those caused by attacks on systems and felt that presentation problems prohibited it from being able to interpret the data sufficiently to determine the underlying causes of the issues identified in the report. OCC was concerned that the report did not sufficiently distinguish between significant and relatively minor problems. We amended the report to reflect the actual percentage of problems experienced for each category discussed, rather than aggregating the problems into a single category. However, the purpose of our survey was to obtain information on the problems experienced by banks and thrifts that offered on-line banking, and the scope of this work did not include an assessment of the significance or underlying causes of the problems each institution experienced. Moreover, information security experts we spoke with emphasized that each of the problems identified was considered to be a serious issue warranting attention.

OTS and FDIC stated that our projection that 47 percent of all U.S. banks will be offering on-line banking by the end of 1998 appeared high. This projection is based on the responses of randomly selected banks that we surveyed and represents what they reported to us about their future plans. Due to the size and characteristics of our sample, our projection of the

---

percentage of banks offering on-line banking by the end of 1998 is subject to a sampling error of  $\pm 15$  percent, resulting in a confidence interval which ranges between 32 percent and 62 percent. We incorporated additional material in appendix II to provide greater detail on our sampling and projection methodology. In addition, we now show the sampling error for each projection presented in the report.

---

As agreed 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 send copies of the report to the Ranking Minority Member of your Committee, the Chairmen and Ranking Minority Members of other interested congressional committees, and individual Members. Copies will also be made available to others on request.

This report was prepared under the direction of Kane Wong, Assistant Director, Financial Institutions and Markets Issues. Other major contributors are listed in appendix VII. Please contact either Mr. Wong on (415) 904-2000 or me on (202) 512-8678 if you have any questions about this report.

Sincerely yours,



Thomas J. McCool  
Director, Financial Institutions  
and Markets Issues

---

# Contents

Letter	1
Appendix I Telephone Survey Instrument	22
Appendix II Objectives, Scope, and Methodology	35
Appendix III Comments From the Federal Reserve System	39
Appendix IV Comments From the Comptroller of the Currency	42
Appendix V Comments From the Federal Deposit Insurance Corporation	44
Appendix VI Comments From the Office of Thrift Supervision	50

---

**Appendix VII** 53  
**Major Contributors to**  
**This Report**

---

**Tables**

Table 1: Projected On-line Banking Services Offered by Banks as of June 1997	6
Table 2: Surveyed Banks Reporting Use of Various Delivery Channels for Their On-line Banking Operations	7
Table 3: Extent to Which Surveyed Banks That Reported On-line Banking Said Their Expectations Were Met	9
Table 4: Extent to Which Banks Reported Various On-line Banking Problems	11
Table 5: Percent of 93 Banks That Reported Having Implemented Various Features Designed to Mitigate Problems	13
Table 6: Surveyed On-line Banks Reporting Electronic Links Between Their On-line Banking System and Other Computer Systems	16
Table II.1: Disposition of Bank and Thrift Survey Sample	35

---

**Figures**

Figure 1: Projected Rapid Growth of On-line Banking Between June 1997 and December 1998	5
Figure 2: Reasons Cited by Surveyed Banks for Implementing On-line Banking	8

---

**Abbreviations**

CHIPS	Clearing House Interbank Payment System
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FRS	Federal Reserve System
OCC	Office of the Comptroller of the Currency
OTS	Office of Thrift Supervision
S.W.I.F.T.	Society for Worldwide Interbank Financial Telecommunications

# Telephone Survey Instrument

## TELEPHONE SURVEY INSTRUMENT

1. Which of the following best describes this financial institution?
  1.  independent financial institution or single-bank holding company
  2.  an individual member of a multibank holding company or other family of banks
  3.  a bank holding company or other parent institution answering for one or more individual banks (3a. How many are you answering for? \_\_\_\_\_)
  4.  other
  
2. How many accounts does your financial institution (or all of the institutions you are answering for) maintain: (Obtain best estimate)
  1.  for retail/personal accounts?
  2.  for corporate/business accounts?
  
3. Does your financial institution presently offer or plan to offer any on-line banking services to any of its retail/personal account customers or to any of its corporate/business account holders within the next 18 months? (On-line banking is defined for this survey as banking services performed by your customers, such as account balance review, bill payment, funds transfers, or accepting loan applications via the Internet or by PC banking software.

(Check all that apply)

  1.  Yes, presently offers to retail/personal account holders only  
(GO TO QUESTION 4)
  2.  Yes, presently offers to corporate/business account holders only  
(GO TO QUESTION 9)
  3.  Yes, presently offers to both personal account and corporate/business account holders  
(GO TO QUESTION 4)
  4.  Yes, plans to offer to retail/personal account holders only within 18 months  
(GO TO QUESTION 20)
  5.  Yes, plans to offer to corporate/business account holders only within 18 months  
( GO TO QUESTION 21)
  6.  Yes, plans to offer both to retail/personal account and corporate/business account holders  
(GO TO QUESTION 20)
  7.  No  
(GO TO QUESTION 24)



**Appendix I  
Telephone Survey Instrument**

**QUESTIONS FOR FINANCIAL INSTITUTIONS THAT PRESENTLY OFFER ON-LINE BANKING**

4. Does your financial institution offer any of the following on-line banking services to any of your retail/personal account holders?

*DK= don't know*

*1      2      3  
YES   NO   DK*

***ON-LINE BANKING SERVICE***

	<i>1</i>	<i>2</i>	<i>3</i>
	<i>YES</i>	<i>NO</i>	<i>DK</i>
1. Review account balance information?			
2. Authorize or perform bill payment?			
3. Accept loan applications?			
4. Authorize or perform funds transfers between customer's accounts?			
5. Authorize or perform Interbank funds transfers?			
6. Other? please specify _____			

5. How does your financial institution currently offer on-line banking services to its personal/retail account holders?

*(Please circle)*

*1      2      3*

- |   |            |           |           |
|---|------------|-----------|-----------|
| 1. Internet web sites maintained by your financial institution, third-party vendor, or member bank?                     | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 2. Internet service providers, (e.g., America On-Line, Prodigy, Compuserve)?  | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 3. PC banking software that allows for direct dial from customer's computer to financial institution's internal server? | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 4. PC banking software that allows for direct dial from customer's computer to system maintained by third-party vendor? | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 5. Other? (please describe _____)   | <i>Yes</i> | <i>No</i> | <i>DK</i> |

6. What year did your financial institution establish its on-line banking program for any of your retail/personal account holders?

1. [ ] specify year
2. [ ] don't know

**Appendix I  
Telephone Survey Instrument**

7. About how many retail/personal accounts are currently registered to use your institution's on-line banking services? (Obtain best estimate)

- 1.  Number of personal/retail accounts
- 2.  Data not maintained
- 3.  Don't know

(ASK QUESTION 8 IF QUESTION 1, ANSWER 2 OR 3, WAS SELECTED: OTHERWISE SKIP TO QUESTION 9)

8. How many member banks/financial institutions of the holding company also offer on-line banking to its retail/personal account holders?

- 1.  number of member banks/financial institutions that offer on-line banking services
- 2.  don't know

Now, I would like to ask you questions concerning on-line banking for corporate/business accounts.

9. Does your financial institution offer any of the following on-line banking services to corporate/business account holders?

*DK= don't know*

*1      2      3*

*YES    NO    DK*

**ON-LINE BANKING SERVICE**

	<i>1</i>	<i>2</i>	<i>3</i>
	<i>YES</i>	<i>NO</i>	<i>DK</i>
1. Review account balance information?			
2. Authorize or perform bill payment?			
3. Accept loan applications?			
4. Authorize or perform funds transfers between customer's accounts?			
5. Authorize or perform interbank funds transfers?			
6. Other? (please specify _____)			

**Appendix I**  
**Telephone Survey Instrument**

10. How does your financial institution currently offer on-line banking services to its corporate/business account holders?

*(Please circle)*

- |   | <i>1</i>   | <i>2</i>  | <i>3</i>  |
|---|------------|-----------|-----------|
| 1. Internet web sites maintained by your financial institution, third-party vendor, or member bank?                     | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 2. Internet service providers, (e.g., America On-Line, Prodigy, Compuserve)?  | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 3. PC banking software that allows for direct dial from customer's computer to financial institution's internal server? | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 4. PC banking software that allows for direct dial from customer's computer to system maintained by third-party vendor? | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 5. Other? (please describe _____)   | <i>Yes</i> | <i>No</i> | <i>DK</i> |

11. What year did your financial institution establish its on-line banking program for corporate/business account holders?

1. [ ] specify year
2. [ ] don't know

12. About how many businesses/corporations are currently registered to use your institution's on-line banking services? (best estimate)

1. Number of businesses/corporations \_\_\_\_\_
2. [ ] data not maintained
3. [ ] don't know

(ASK QUESTION 13 IF QUESTION 1, ANSWER 2 OR 3, WAS SELECTED:  
OTHERWISE SKIP TO QUESTION 14)

13. How many member banks/financial institutions of the holding company also offer on-line banking to their corporate/business account holders?

1. [ ] number of member banks/financial institutions that offer on-line banking services
2. [ ] don't know

**Appendix I**  
**Telephone Survey Instrument**

Now, I would like to ask you questions dealing with why the financial institution decided to offer on-line banking and any potential risk(s) related to on-line banking.

14. What factors led your financial institution to offer on-line banking services?  
(For both retail/personal and corporate/business accounts)

*(please circle after  
response is given)*

	<i>1</i>	<i>2</i>	<i>3</i>
1. To attract new customers?	<i>Yes</i>	<i>No</i>	<i>DK</i>
2. To keep customers?	<i>Yes</i>	<i>No</i>	<i>DK</i>
3. To reduce operating expenses?	<i>Yes</i>	<i>No</i>	<i>DK</i>
4. To remain competitive with other financial institutions?	<i>Yes</i>	<i>No</i>	<i>DK</i>
5. Fee income?	<i>Yes</i>	<i>No</i>	<i>DK</i>
6. Other? (specify: _____)	<i>Yes</i>	<i>No</i>	<i>DK</i>

15. Did you conduct a formal risk assessment of on-line banking prior to its actual implementation?

1.  yes (GO TO 15a)
2.  no (please explain why not, then go to 16)
3.  don't know

**Appendix I**  
**Telephone Survey Instrument**

15a. Did the risk assessment cover the following issues?

*5b. If yes, was it  
 identified as a  
 significant risk?*

*Yes    No    DK*  
*1      2      3*  
*(circle)*

	<i>Yes</i> <i>1</i>	<i>No</i> <i>2</i>	<i>DK</i> <i>3</i>	
1. Upgrade and/or replacement of PC banking software?				<i>1. Yes 2. No 3. DK</i>
2. Staffing & training of on-line banking dept?				<i>1. Yes 2. No 3. DK</i>
3. As transaction volume increases, difficulty in tracing & monitoring transactions?				<i>1. Yes 2. No 3. DK</i>
4. Lack of proof or authentication of customer performing banking services on-line?				<i>1. Yes 2. No 3. DK</i>
5. Denial or disruption of on-line banking service?				<i>1. Yes 2. No 3. DK</i>
6. Insider threat?				<i>1. Yes 2. No 3. DK</i>
7. Unauthorized access into internal systems?				<i>1. Yes 2. No 3. DK</i>
8. Uncoded passwords and PINs?				<i>1. Yes 2. No 3. DK</i>
9. Loss of transactions during transmission?				<i>1. Yes 2. No 3. DK</i>
10. Viruses or worms?				<i>1. Yes 2. No 3. DK</i>
11. Uncertain legal or regulatory environment? (local, national, international)				<i>1. Yes 2. No 3. DK</i>
12. Systemic risk--financial institution's participation in a payment system can have a significant financial impact on all participants?				<i>1. Yes 2. No 3. DK</i>

**Appendix I  
Telephone Survey Instrument**

16. Do any of your on-line banking systems, operated by your institution (or a vendor), have any of the following security features? (**CHECK ONE**)

<i>Security feature</i>	<i>1 YES</i>	<i>2 NO</i>	<i>3 DK</i>
<b>(ASK IF ON-LINE BANKING IS DIRECT-DIAL BASED)</b>			
1. Is a system in place for ensuring that users receive updated software safely and/or securely? (software update control)			
2. a. On-line banking guidelines (such as access levels, reporting, and/or record retention) established?	a.	a.	a.
b. Are they regularly monitored?	b.	b.	b.
3. Separation of system control duties?			
4. Have employees received proper training?			
5. a. Audit logs and/or reports generated?	a.	a.	a.
b. Are they routinely reviewed?	b.	b.	b.
6. a. Digital signatures?	a.	a.	a.
b. Does it ensure the integrity of the data transmitted?	b.	b.	b.
7. Session encryption that codes the links between the customer's PC and internal servers?			
8. a. Emergency or contingency plans in place for responding to natural disasters, terrorism, employee mistakes, or unexplained disruption of your electronic banking programs?	a.	a.	a.
b. Have employees received proper training in implementing these plans?	b.	b.	b.
9. Access restricted after unsuccessful entry attempts? (user cannot log on to on-line system if 3 or more repeated attempts were made with an incorrect PIN or password)			
10. a. Firewalls in place?	a.	a.	a.
b. Does it distinguish between customers and/or vendors and/or internal systems?	b.	b.	b.
11. Intrusion detection software that provides for exception reporting?			
12. Coded or encrypted personal passwords and/or PINS?			
13. Antivirus and/or worm protection programs in place?			
14. Has the financial institution performed penetration testing?			
15. <b>(ASK IF ON-LINE BANKING IS OUTSOURCED TO THIRD PARTY)</b> Does the financial institution routinely monitor whether vendors are mitigating potential risks?			

**Appendix I  
Telephone Survey Instrument**

17. Has your financial institution experienced any of the following problems?

*a. If yes, how many times? go to b.*      *b. What damage resulted?*

**1      2      3**  
**Yes No DK**

**Enter Code**

	<b>1</b>	<b>2</b>	<b>3</b>		
	<b>Yes</b>	<b>No</b>	<b>DK</b>		<b>Enter Code</b>
1. Upgrading and/or replacing PC banking software?				NA	
2. Staffing & training of on-line banking dept.?				NA	
3. As transaction volume increases, difficulty in tracing & monitoring transactions?					
4. Lack of proof or authentication of customer performing banking services on-line?					
5. Denial or disruption of on-line banking service?					
6. Employee sabotage?					
7. Unauthorized access into internal systems?					
8. Theft of passwords and PINs?					
9. Transactions lost during transmission?					
10. Viruses or worms?					
11. Theft of web sites?					
12. Alteration of data on web informational page?					
13. What other problems has your financial institution experienced?					

Note: For 17b, what damage resulted? Please enter the code for the following potential responses.

- Code 1. financial loss ( )
- 1a. How much money was lost? (record answer in thousands)
  2. loss of customer confidence
  3. loss of customer accounts
  4. denial of service
  5. technical support inadequate
  6. none
  7. other (specify \_\_\_\_\_)

**Appendix I**  
**Telephone Survey Instrument**

17c. Has your financial institution experienced any ATTEMPTS of unauthorized access into your on-line banking system?

1.  yes ( About how many times?\_\_\_\_\_)
2.  no
3.  don't know

18. Are any of your on-line banking services electronically linked to the following systems?

*(please circle)*

- |                                  | <i>1</i>   | <i>2</i>  | <i>3</i>  |
|----------------------------------|------------|-----------|-----------|
| 1. Fedwire/Fedline?              | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 2. CHIPS?                        | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 3. SWIFT?                        | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 4. Vendor systems?               | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 5. Other financial institutions? | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 6. Business partners?            | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 7. Other? _____                  | <i>Yes</i> | <i>No</i> | <i>DK</i> |

19. Overall, have the benefits of on-line banking met, exceeded, or fallen short of expectations?

1.  met expectations
2.  exceeded expectations
3.  fallen short of expectation
4.  too early to tell
5.  don't know

19a. Describe how expectations were met, exceeded, or have fallen short?



**Appendix I  
Telephone Survey Instrument**

**FINANCIAL INSTITUTIONS THAT PLAN TO OFFER ON-LINE BANKING**

20. Does your financial institution plan to offer any of the following on-line banking services to retail/personal account holders?

<b>ON-LINE BANKING</b>	<b>1</b>	<b>2</b>	<b>3</b>
	<b>YES</b>	<b>NO</b>	<b>DK</b>
1. Review account balance information?			
2. Authorize or perform bill payment?			
3. Accept loan applications?			
4. Authorize or perform funds transfers between a customer's accounts?			
5. Authorize or perform Interbank funds transfers?			
6. Other? (please specify _____)			

21. Does your financial institution plan to offer any of the following on-line banking services to corporate/business account holders?

<b>ON-LINE BANKING SERVICE</b>	<b>1</b>	<b>2</b>	<b>3</b>
	<b>YES</b>	<b>NO</b>	<b>DK</b>
1. Review account balance information?			
2. Authorize or perform bill payment?			
3. Accept loan applications?			
4. Authorize or perform funds transfers between a customer's accounts?			
5. Authorize or perform interbank funds transfers?			
6. Other? (please specify _____)			

**Appendix I  
Telephone Survey Instrument**

22. What factors have led your financial institution to plan to offer on-line banking services? (For both retail/personal and corporate/business accounts)

**(please circle after response is given)**

- |   | <b>1</b>   | <b>2</b>  | <b>3</b>  |
|---|------------|-----------|-----------|
| 1. To attract new customers?                                | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 2. To keep customers?                                       | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 3. To reduce operating expenses?                            | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 4. To remain competitive with other financial institutions? | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 5. Fee income?  | <i>Yes</i> | <i>No</i> | <i>DK</i> |
| 6. Other? (specify: _____)                                  | <i>Yes</i> | <i>No</i> | <i>DK</i> |

23. Did or will you conduct a formal risk assessment of on-line banking prior to actual implementation?

1.  yes, a risk assessment has been conducted (GO TO 23a)
2.  yes, a risk assessment is planned to be conducted (END OF INTERVIEW)
3.  no (please explain why not\_\_\_\_\_) END OF INTERVIEW
4.  don't know (END OF INTERVIEW)

**Appendix I  
Telephone Survey Instrument**

23a. Did the risk assessment cover the following issues?

*Yes No DK 23b. If yes, was it identified  
1 2 3 as significant risk? (circle)*

1. Upgrade and/or replacement of PC banking software?				1. Yes 2. No 3. DK
2. Staffing & training of on-line banking dept?				1. Yes 2. No 3. DK
3. As transaction volume increases, difficulty in tracing & monitoring transactions?				1. Yes 2. No 3. DK
4. Lack of proof or authentication of customer performing banking services on-line?				1. Yes 2. No 3. DK
5. Denial or disruption of on-line banking service?				1. Yes 2. No 3. DK
6. Insider threat?				1. Yes 2. No 3. DK
7. Unauthorized access into internal systems?				1. Yes 2. No 3. DK
8. Uncoded passwords and PINs?				1. Yes 2. No 3. DK
9. Transactions lost during transmission?				1. Yes 2. No 3. DK
10. Viruses or worms?				1. Yes 2. No 3. DK
11. Uncertain legal or regulatory environment? (local, national, int'l)				1. Yes 2. No 3. DK
12. Systemic risk--financial institution's participation in a payment system can have a significant financial impact on all participants?				1. Yes 2. No 3. DK

**Appendix I**  
**Telephone Survey Instrument**

FOR FINANCIAL INSTITUTIONS THAT DO NOT OFFER OR DO NOT PLAN TO OFFER  
ON-LINE BANKING SERVICES

24. Can you describe the factors that led your financial institution to decide against offering on-line banking services? (Check all that apply after the response is given)
1.  security fears
  2.  high maintenance costs
  3.  costly start-up costs
  4.  customers not interested
  5.  not in corporate plan
  6.  don't know enough about on-line banking
  7.  other(specify:\_\_\_\_\_)
25. Does your financial institution currently have a World Wide Web site that offers information on mortgage rate quotes, credit card applications, or other informational services? (excludes banking functions that can be performed on-line)
1.  yes (CONTINUE)
  2.  no (SKIP TO END)
26. How was your home page built?
1.  third-party vendor
  2.  off-the-shelf Web page maker program
  3.  in-house system security personnel
  4.  other(specify:\_\_\_\_\_)
27. Is the home page:
1.  on a stand-alone PC
  2.  linked to the financial institution's computer system/network
  3.  don't know
28. Has more than one firewall been constructed behind the home page?
1.  yes
  2.  no
  3.  don't know
29. Has your home page ever been altered, compromised, or stolen?
1.  yes, a. how many times?\_\_\_\_\_
  2.  no
  3.  don't know

# Objectives, Scope, and Methodology

Our objectives for this assignment were to determine (1) the number of banks and thrifts (referred to as banks in this report) that reported they offer, or plan to offer, on-line banking and the types of services they reported; and (2) the experiences reported by banks in implementing their on-line banking systems as well as their efforts to mitigate associated risks. We focused our work on those U.S. banks and thrifts that accepted retail deposits or provided retail services.

To accomplish our objectives, we conducted a telephone survey between May 1997 to mid-June 1997 of 349 banks, which included 219 banks that available information suggested were offering on-line banking services<sup>7</sup> and 130 randomly selected banks that were representative of the remaining banks and thrifts in the United States. The random sample of 130, stratified across 7 size categories, was drawn from a population of 11,288 banks and thrifts that remained in a database of the September 1996 Federal Financial Institutions Examination Council's Call Reports and the Office of Thrift Supervision's Thrift Financial Reports after the banks and thrifts previously identified as on-line banking providers were removed, as shown in table I.1. Although neither GAO nor the agencies that produced the source data have fully assessed the reliability of this database, Call Report data are widely used by researchers in academia, government, and private industry.

**Table II.1: Disposition of Bank and Thrift Survey Sample**

Sample source	Original population	Sample	Sample disposition			Response rate <sup>b</sup>
			Ineligible <sup>a</sup>	Refusals/no response	Usable response	
Previously known on-line banking offerors	219	219	42	16	161	91%
Stratified random sample of remaining banks and thrifts	11,288	130	12	2	116	98%
<b>Totals</b>	<b>11,507</b>	<b>349</b>	<b>54</b>	<b>18</b>	<b>277</b>	<b>94%</b>

<sup>a</sup>No longer in business, acquired or merged with another institution, or duplicate listings.

<sup>b</sup>Response rate was calculated as the number of banks and thrifts completing usable questionnaires divided by the number of eligible banks and thrifts in the sample (original sample minus ineligible).

Source: GAO survey.

<sup>7</sup>We consulted an Internet-based directory of North American banks that offered on-line banking, maintained by the Online Resources & Communications Corporation. We did not validate the coverage or content of the directory.

We contacted officials representing the 349 institutions in our sample by telephone to determine whether the institution was currently an active bank eligible for our survey and found that 295 banks were eligible. For those eligible banks, we asked the bank to identify the most appropriate respondent, and we then mailed that person a letter requesting his or her participation in our telephone survey. We also faxed the telephone questionnaire to 10 banks that could not respond to our questionnaire by telephone and asked them to return the questionnaire by fax. When we completed our fieldwork in mid-June 1997, 277 of the 295 eligible banks (94 percent) from our original sample of 349 had provided complete responses. We did not verify the information provided by survey respondents.

To accomplish our first objective, we asked each respondent whether the bank offered or planned to offer on-line banking to retail or corporate customers and the reasons for offering or not offering on-line banking. In addition, we asked these officials about the types of on-line banking services their banks offered. We found that 185 of the 277 banks we contacted reported they offered on-line banking services. We found that many of those banks were affiliated and a single official was able to provide on-line banking information on several banks in our survey. Thus, we interviewed only 93 bank officials who were able to provide information for the 185 banks that reported offering on-line banking in our survey.

Our estimates of the (1) overall numbers of U.S. banks offering or intending to offer on-line banking and (2) specific services offered are projected to the entire population of approximately 10,520 U.S. banks we estimate to have been active at the time of our survey. To arrive at 10,520 banks from the original population of 11,507, we adjusted the original number on the basis of the number of ineligible banks we found during our review. To make such estimates, we assigned each completed survey questionnaire a mathematical weight proportional to the number of other unsampled banks in the stratum that the sampled bank was to represent. We assigned a weight of 1 to banks previously identified with on-line banking systems, as they were not drawn at random to represent a larger stratum of nonsampled banks. For example, to arrive at our population estimate of 4,220 banks that do not currently offer any on-line banking services but plan to offer at least 1 such service by December 1998 (see app. I, ques. 3), we multiplied each of the 36 sampled banks that gave us this answer by a weight, ranging from 1 to 336, depending on which size stratum each was drawn from. Because we surveyed only a sample of

banks, these estimates have a sampling error, which is a measure of the precision with which the estimated value approximates the actual value. Sampling errors are calculated at the 95 percent confidence level for each weighted estimate made and are reported in the text.

To accomplish our second objective, to determine the experiences reported by banks in implementing their on-line banking systems as well as efforts to mitigate associated risks, we based our results on the responses of the officials we interviewed and did not project the results to all active banks in the United States. We obtained information for 185 banks on (1) the channels used to deliver on-line banking services, (2) the reasons for implementing on-line banking, (3) whether on-line banking met or exceeded expectations, and (4) the electronic links that banks had with other payment systems. We limited certain information obtained from these officials to the banks they directly represented. Specifically, these officials provided information for 93 banks on (1) problems experienced, (2) risk identification, and (3) risk mitigation efforts.

The difficulties of conducting any survey may introduce other types of “nonsampling” errors that affect both the weighted and unweighted estimates. For example, differences in how a particular question is interpreted, or in the sources of information that are available to respondents, can introduce unwanted variability into the survey results. Although we did not verify the survey results, we took various steps to reduce nonsampling errors. Prior to designing our telephone questionnaire, we interviewed information security experts and federal agency officials to identify the types of potential risks and problems that could be associated with on-line banking as well as basic security features that could help prevent the occurrence of such problems. We also reviewed relevant documents and technical literature on these issues. We then solicited expert opinions on the wording and structure of our questions, and we pretested the survey instrument with several banks.

All data collected during our survey were keypunched and verified during data entry, and computer analyses were performed to identify additional inconsistencies or other indications of errors. All computer analyses were checked by an independent analyst.

In this study, we did not attempt to determine the effectiveness of security measures that banks implemented to prevent the occurrence of on-line banking problems. To do so would have required us to look at numerous

factors, such as particular computer system architectures and banks' policies and guidance.

In addition, we interviewed information security experts from Lawrence Livermore Laboratory; Science Applications International Corporation; Advanced Programming and Development, Inc; the Department of Defense; and the National Institute of Standards and Technology to identify potential risks and problems associated with on-line banking as well as basic security features that could help prevent such problems. We also discussed these issues with officials from the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the Department of the Treasury. We further contacted officials from the Federal Bureau of Investigation, the President's Commission on Critical Infrastructure Protection, the American Bankers Association, the Bankers Roundtable, and the California Bankers Association.

We conducted our review between October 1996 and October 1997 in accordance with generally accepted government auditing standards. We provided a draft of this report to the Federal Reserve System, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, and the Department of Justice for comment. The four regulatory agencies provided written comments, which are reprinted in appendixes III through VII. In addition, these four regulatory agencies and the Department of Justice's Federal Bureau of Investigation provided technical comments, which we have incorporated where appropriate in the report.



# Comments From 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

CLYDE H. FARNSWORTH, JR.  
DIRECTOR  
DIVISION OF  
RESERVE BANK OPERATIONS  
AND PAYMENT SYSTEMS

November 14, 1997

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

Dear Mr. McCool:

We appreciate the opportunity to comment on the General Accounting Office's (GAO) draft report on Electronic Banking: Experiences Reported by Banks in Implementing On-line Banking. Electronic banking is an important issue, which the Federal Reserve is addressing through a variety of initiatives. The draft report provides further useful insights into this rapidly evolving area. We believe, however, that the draft report would benefit from better distinctions in two areas.

See comment 1.

First, we believe that the report's definition of security problems (or security difficulties) with on-line banking systems overstates the extent to which real security problems may exist with these systems. The draft report's definition of a security problem includes all "unauthorized attempts" to access a system, even if the attempts were unsuccessful or were the result of inadvertent errors by authorized users. In contrast, the federal criminal statute that relates to computer crime (18 U.S.C. 1030) and Federal banking supervisors define computer-related security problems as those related to the actual theft of funds, theft of information, or disruption of computer services.<sup>1</sup> According to the draft report, eighteen of the nineteen unauthorized access attempts identified in the survey were categorized as unsuccessful (and there is no information on whether the successful attempt was adequately contained by other security measures). In our opinion, these unsuccessful access attempts do not indicate a "problem" or "difficulty" as characterized in the report.

See comment 2.

Second, it would be useful if the draft report would differentiate between problems caused by hardware, software, or operational failures and those caused by attacks on systems. The draft report states that 69 percent of banks reported that they

---

<sup>1</sup> For example, see Supervisory Letter SR 97-28, Guidance Concerning the Reporting of Computer-Related Crimes by Financial Institutions, issued on November 6, 1997, by the Division of Banking Supervision and Regulation, Board of Governors of the Federal Reserve System.

---

**Appendix III  
Comments From the Federal Reserve  
System**

- 2 -

experienced service availability lapses, security problems, or operational problems with their on-line banking systems. These are quite different problems and we question the appropriateness of aggregating them for statistical presentment. It is not clear from these broad categories of problems, for example, whether the "problems" were due to operational difficulties, attacks on systems, or errors on the part of authorized users. In particular, the draft report should clarify its use of the terms "denial of service" and "disruptions" or "breakdowns" in service. The former term suggests an intentional interruption of service due to an attack, which is quite different from a breakdown or disruption in service due to a hardware or software problem. Given these presentation problems, we were not able to interpret the data sufficiently to determine the underlying causes of the issues identified in the survey, and we are concerned that others might misinterpret the statistics or take them out of context.

We also have some additional technical comments on the draft report, which we have provided directly to your staff. Thank you again for the opportunity to comment on the draft report. We hope these comments are useful to the GAO in the development of its final report.

Sincerely,



Clyde W. Lewis

---

The following are GAO's comments on the Federal Reserve System's letter dated November 14, 1997.

---

## **GAO Comments**

1. FRS commented that the draft report overstates the extent to which real security problems may exist due to the inclusion of unsuccessful unauthorized attempts to access a system or inadvertent errors by authorized users. In order to eliminate any confusion, our discussion was changed to comment only on the number of banks reporting unauthorized access attempts and, thus, excludes the one bank that classified a customer error as an unauthorized access attempt. The purpose of our survey was to obtain information on the problems reported by banks and thrifts that offered on-line banking, and the scope of the work did not include an assessment of the significance or underlying causes of the problems each institution experienced.
2. FRS suggested that we clarify our use of the terms "denial of service" and "disruptions in service." We did not differentiate these terms in the question we posed to the banks. Our question was directed to whether the bank was unable to provide service regardless of whether it was due to a malicious intent or breakdown in the hardware or software supporting the system and thus cannot be used to determine underlying causes.

# Comments From the Comptroller of the Currency



---

Comptroller of the Currency  
Administrator of National Banks

---

Washington, DC 20219

November 21, 1997

Mr. Thomas J. McCool  
Director, Financial Institutions and Markets Issues  
General Government Division  
United States General Accounting Office  
Washington, D.C. 20548

Dear Mr. McCool:

We have reviewed your draft audit report titled [ELECTRONIC BANKING: Experiences Reported by Banks in Implementing On-line Banking](#). The report is the first in a series of reports on electronic banking to be issued in response to congressional request.

The report correctly points out that on-line banking exposes customers and the bank to risks from electronic interception, data corruption and fraud, as well as other risks. Moreover, the survey data indicates that some banks may not be conducting appropriate risk assessments prior to implementing these systems. This is consistent with our analysis of the current situation. We are addressing this problem and are currently developing appropriate guidance on these issues.

However, we think the report's conclusions about system availability, security and operational problems may provide a misleading picture of the extent of these problems. Our basic concern is that the survey questions do not sufficiently distinguish between significant problems and relatively minor problems. It is impossible to draw firm conclusions about the significance of these issues without additional information. As an example, in the section on security problems, there is no distinction between inadvertent mistakes by customers entering passwords or personal identification numbers, and actual efforts to gain access for illicit purposes. These are two very different events and without more information, it is difficult to discern the level of security risk.

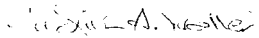
We agree with the basic thrust of the report that banks face challenges when implementing and maintaining on-line banking services. Your report is helpful in assessing the extent of the market in on-line banking, as well as identifying weaknesses in bank approaches to managing risks associated with this activity.

---

**Appendix IV  
Comments From the Comptroller of the  
Currency**

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

Sincerely,



Judith A. Walter  
Senior Deputy Comptroller for Administration

# 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

November 17, 1997

Mr. Kane Wong  
Assistant Director,  
Financial Institutions and Markets Issues  
U.S. General Accounting Office  
301 Howard Street, Suite 1200  
San Francisco, CA 94105-2252

Dear Mr. Wong:

Enclosed is the FDIC Division of Supervision's response to the United States General Accounting Office draft report to Congress entitled, "Electronic Banking: Experiences Reported by Banks in Implementing On-line Banking". We appreciate the opportunity to respond to the draft report. If you have any additional questions, please feel free to contact Elroy Holden, at (202) 736-3036.

Sincerely,



Vijay Deshpande  
Director

Enclosure

cc: Dennis F. Geer (w/o attachments)  
Paul L. Sachtleben (w/o attachments)  
Simona L. Frank (w/o attachments)  
James D. Collins (w/o attachments)  
Grace Sakoda (GAO)

**Appendix V**  
**Comments From the Federal Deposit**  
**Insurance Corporation**



**FDIC**

Federal Deposit Insurance Corporation  
550 17th Street, N.W.  
Washington, DC 20429

Division of Supervision

**ELECTRONIC BANKING: EXPERIENCES REPORTED BY BANKS IN IMPLEMENTING ON-LINE BANKING**

The following summarizes the FDIC's comments on the November 1997 report, Electronic Banking: Experiences Reported by Banks in Implementing On-line Banking. The opportunity to review and comment on the report is greatly appreciated. The report contains meaningful findings regarding the number of banks currently offering online banking and forecasts significant future growth in online banking. In general, these findings are consistent with FDIC's observations and expectations. The report also outlines significant concerns regarding system security and banks' controls over online banking programs. These findings merit serious attention; however, our degree of concern depends somewhat on additional information that was not provided in the report. FDIC has taken proactive steps to address these emerging concerns which include our recently issued examination procedures for electronic banking, examiner training programs, and development of technical electronic banking specialists. We continue to regard this dynamic area as one of increasing importance that merits close monitoring.

**General Comments on Scope and Content**

The following general comments pertain to the scope of the survey, the surveyed population, and the information contained in the report.

See comment 1.

The survey of online banking activities focused entirely on systems involving personal computers. Telephone banking was not addressed in the survey. While telephone banking has been deployed by many banks for several years, these systems involve the same communication networks as dial-up PC banking and may involve similar risks and concerns. While the functionality of telephone banking systems may be more limited, they generally facilitate applications similar to PC banking such as account access, funds transfer, and bill-payment. The security of these systems and their integration with other bank systems should be considered within the scope of online banking.

See comment 1.

The survey targeted a sample of banks and thrifts, and the findings were projected to reflect the entire U.S. bank and thrift industry. It may be useful to also consider the online activities of the credit union industry. Currently, credit unions are more active in deploying online banking (particularly Internet) systems than their bank counterparts. Over 80 credit unions maintain transactional Internet sites and it is expected that a much larger number offer direct dial-up PC banking programs. Given the significant and growing number of credit unions that are involved in online banking, their system security and connectivity to Fedwire may be worthy of review.

See comment 2.

While the size of the surveyed bank population was rather small (349 banks surveyed with online banking activities reported by 185), a further breakdown or analysis of the results organized by

the asset size of the bank might provide useful insights. It is recognized that risk exposure and control methods will be quite different for multi-billion dollar regional or national banks in comparison to smaller community institutions.

One important item that was not included with the report is a copy of the questions that comprised the survey. This information would be particularly helpful in understanding and interpreting the responses. It is recommended that a copy of the survey be included in the appendix of the report or as an addendum.

#### **Current and Future Trends in Online Banking**

The observation that approximately seven percent of U.S. banks (770 institutions) currently offer online banking is consistent with the FDIC's observations. However, while significant and rapid growth in online banking is expected, the forecast that 47% of U.S. banks will offer online banking by the end of 1998 seems high. Additional information as to how the projected numbers were arrived at would be helpful. The number of banks offering direct dial-up and Internet home banking (Table 2) appears reasonable and consistent with our observations. Currently, the majority of institutions offering online banking utilize direct-dial up channels; however, a trend toward Internet systems is developing. FDIC has also observed an increasing number of institutions deploying multiple systems concurrently (e.g., telephone, direct dial-up, and Internet). It would be particularly helpful to view a breakdown of the surveyed banks' plans for deploying dial-up versus Internet systems.

The finding that only 58% of the surveyed banks had conducted formal risk assessments is viewed with concern. FDIC has also observed that many banks rely heavily on third party vendors and may be less than fully aware of the security features that protect their systems. The FDIC's safety and soundness examination procedures instruct examiners to discuss this issue with bank management and evaluate the institution's risk management techniques for electronic banking activities. The quality of the risk assessment is of particular importance and receives close attention by examiners. (Reference is made to the *Planning and Implementation* and *Administration* review areas of the electronic banking examination procedures.)

The projected growth of online banking is significant and warrants close monitoring. FDIC has been proactive in developing programs to remain abreast of industry trends and has issued examination procedures and instituted training programs to prepare examination staff for these developments.

#### **Security Problems and Controls**

The finding that 69% of the bank officials surveyed reported problems with their online banking systems (particularly security related problems) is viewed with great concern. Particular attention is directed to the observation that within the surveyed population there had been 19 unauthorized access attempts (of which one was successful). In order to fully comprehend the significance of these findings, it would be most helpful to review the context of the survey

See appendix I.

See appendix I.



question. A follow-up question on whether the incidents were reported to the appropriate regulatory agency and law enforcement would be helpful in evaluating the extent of the suspected problem that financial institutions are failing to report breaches of system security.

While it was reported that 85% of the surveyed banks had contingency plans, FDIC is concerned that the remaining 15% did not have such plans. FDIC's electronic banking examination procedures specifically address the need for contingency plans, emergency preparedness, and well-trained response teams. The examination procedures were made available to the industry to provide guidance on important concerns, such as contingency planning, that should be addressed in the early stage of system development. Examiners are directed to review contingency plans and preparedness measures at each safety and soundness and information systems examination.

The large number of reported unauthorized attempts to access banks' systems (20%) and system disruptions (35%) merit serious attention. FDIC's examination procedures state that banks should institute programs where system logs are reviewed regularly and programs are developed to prevent, detect, and contain system intrusions. Suspicious activity should also be reported to law enforcement and the regulatory agencies. To address system availability concerns, ongoing evaluations of capacity and stress testing are advised. The importance of system security is emphasized in examiner training programs and information systems specialists are currently undergoing training to enhance their knowledge of emerging technical solutions.

#### **Linked Systems**

On page 27 of the report, "electronic links" between banks' online retail banking systems and other banks' systems are discussed. The report expresses concern that these links could potentially endanger multiple systems, if one is successfully attacked. While electronic links with vendors and business partners are generally expected, FDIC finds it surprising that 15% of the surveyed banks reported electronic links between their online banking programs and Fedwire. In the FDIC's experience with regular onsite examinations, we have rarely encountered such linking. In the majority of situations, we have observed that banks' online banking systems are maintained separately from critical systems such as Fedwire. Generally, the systems are physically separate and disconnected. It may be possible that the wording of the survey question caused the banks to report that they have linked systems when in fact they have multiple systems, but they are not directly connected. Also, in our experience, very few banks offer their customers the ability to directly transfer funds to other banks. External funds transfer appears generally limited to electronic bill payment and automated clearing house (ACH) transfers.

#### **Other Comments and Observations**

It was interesting to note that employee sabotage, or internal attacks, represented such a low percentage of reported problems (only 1%). This finding was somewhat contrary to recent reports by the Computer Security Institute and the Federal Bureau of Investigation that insider attacks continue to comprise the largest share of computer crimes.

The GAO is commended for its excellent job in selecting questions that covered the primary

Now on p. 16.

See comment 3.

See comment 4.

areas of security and concern. A couple of additional aspects of online banking security that are suggested for possible future reviews include nonrepudiation and access control. The use of passwords and PINS remains the most common method of access control and user authentication; however, such provides only a limited degree of security. FDIC is monitoring developments in these and other areas related to system security.

**Summary and Conclusions**

In general, the findings and conclusions related to the current number of banks offering online banking and projected growth in this area are consistent with the FDIC's observations and expectations. The noted failure of many banks to perform risk assessments and develop contingency plans is viewed with concern. However, FDIC's examination procedures direct examiners to evaluate risk management techniques and contingency plans for electronic banking, at a minimum, in the course of a bank's safety and soundness examination.

The fact that a significant percentage of the surveyed population reported security and operational problems merits serious attention. However, the severity of the problem would depend on how the questions were phrased and how they were interpreted by the respondents. For example, if the respondents included their experience during pilot tests, the results may be distorted and concern would be mitigated. It is clear that this area deserves significant attention during regular examinations. Through our electronic banking examination procedures, and development of technical specialists, FDIC has taken proactive steps to address this emerging area, and will continue to closely monitor developments in online banking.

Please contact Examination Specialist Cynthia A. Bonnette at (202) 898-6583 if you have any questions.

---

The following are GAO's comments on the Federal Deposit Insurance Corporation's letter dated November 17, 1997.

---

## GAO Comments

1. FDIC stated that the survey results in our draft report did not include telephone banking or the experiences or efforts of the credit union industry. Although we agree that these are important subjects to cover, they were beyond the scope of our work.
  
2. FDIC commented that it would be useful to provide an analysis of the survey results by bank asset size. An analysis of survey results organized by asset size of the banks would be helpful. However, we were not able to project distinctions between asset size categories because of the size of our sample.
  
3. FDIC commented that it had rarely encountered an electronic link between banks under its review and other systems, including Fedwire. It commented that it may be possible that the survey question may have been ambiguous. In addition, FDIC said it has seen very few banks offer their customers the ability to directly transfer funds to other banks. We specifically asked the banks whether their on-line banking services were electronically linked to Fedwire and other systems. In addition, we recontacted one bank that examiners told us they believed was not linked to Fedwire, and bank officials told us that in fact the bank did have an electronic link to the Fedwire system. In regard to transferring funds between banks, we specifically asked the banks whether their on-line systems allowed customers to authorize or perform interbank funds transfers. We did not validate whether customers could actually perform these transfers, and we presented the information as it was reported to us.
  
4. FDIC stated that the number of reported experiences of employee sabotage and internal attacks was low and contrary to other recent reports. We recognize that internal attack is one of the biggest threats to on-line banking. However, we were limited to presenting the number of experiences that the banks reported to us. Although the FBI had information that insider attacks constitute a large number of computer crimes, FBI officials told us the information is not specific to the banking industry. See page 14.

# 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, D.C. 20552 • (202) 906-6590

*Ellen Seidman*  
Director

November 17, 1997

Mr. Thomas J. McCool, Director  
Financial Institutions and Markets Issues  
U. S. General Accounting Office  
441 G Street, N.W.  
Washington, D.C. 20548

Dear Mr. McCool:

We appreciate the opportunity to review an advance draft of the report *Electronic Banking: Experiences Reported by Banks in Implementing On-line Banking*. We have found the information to be useful and offer the following comments:

Throughout the report, risk assessment issues were addressed. The Office of Thrift Supervision (OTS) and Federal Deposit Insurance Corporation have issued guidance for institutions to adequately assess and mitigate the risk involved with the use of information technologies such as on-line personal computer banking.

OTS issued guidance to thrift institutions on retail on-line personal computer banking in June 1997 (CEO Memo 70). In this statement, we encouraged institutions to evaluate the risks associated with personal computer banking and implement sound controls. In October 1997, OTS issued Regulatory Bulletin 32-6 updating examination guidelines for the use of information technology. The October guidance puts heavy emphasis on thrifts adopting a risk management program. In both documents, OTS suggests that an institution's effectiveness in controlling risks inherent in the use of evolving technologies has a direct impact on its overall safe and sound operation. Therefore, OTS advises institutions that use information technology to create a safe, sound, and secure infrastructure that is adequate to evaluate and mitigate risks associated with electronic activities. The OTS guidance suggests that the infrastructure should include adequate planning; controls for deployment, operation, and user acceptance; and an internal audit function. Specifically, controls should address information security, contingency planning, conversion project management, change control management, input and output controls, training and outsourcing.

In addition to these guidelines, OTS issued an advanced notice of proposed rulemaking on April 2, 1997 soliciting advice as to whether OTS has any rules that stand in the way of implementing technology in the thrift industry and recommendations for rules we should adopt to enable their use of technology. After reviewing the 22 comment letters, OTS issued a notice of proposed rulemaking on

See comment 1.

**Appendix VI  
Comments From the Office of Thrift  
Supervision**

November 17, 1997  
Page 2

October 3, 1997 proposing a rule that would permit thrift institutions to use technology to deliver any banking services the institution is authorized to deliver through more traditional means. Comments are due by December 2, 1997.

Finally, GAO's projections for the growth of on-line banking services are not adequately explained and appear very aggressive based on currently available data. While OTS does not collect data on thrifts offering on-line electronic banking services, the FDIC does report some data for banks and thrifts based upon information they obtain from internet search techniques and from data collected by field examiners during exams. The field examiners' data suggest that several hundred banks and thrifts currently offer direct phone line connections using PC software. There are far fewer institutions providing interactive transactional services through an internet web site. At the end of the second quarter 1997, FDIC estimated the number of banks and thrifts with web sites to be 1100. However, only 56 of those sites offered transactional services by the end of the third quarter 1997 (and this number had increased to 75 by early November).

Although GAO's estimate that there were 770 banks and thrifts offering "on-line electronic banking services" in June 1997 appear roughly consistent with FDIC data, a projected six fold increase to 4990 institutions by the end of 1998 may be overly optimistic. The FDIC numbers do indicate that the number of interactive transactional web sites is rapidly increasing, but it is unlikely that almost half of the banking and thrift industry will be offering such services within the next 13 months, i.e., by the end of 1998. An explanation of the GAO projection methodology in the data appendix would help to resolve the reasonableness of the forecast.

We have included additional comments on specific issues in the report as an attachment to this letter. Thank you for providing the opportunity to comment on this draft document. I hope these comments are of assistance to you and your staff.

Sincerely,



Ellen Seidman  
Director

Attachment

cc: Kane Wong, Assistant Director  
General Accounting Office

We did not reproduce the attachment.

---

**Appendix VI  
Comments From the Office of Thrift  
Supervision**

---

The following is GAO's comment on the Office of Thrift Supervision's letter dated November 17, 1997.

---

**GAO Comment**

1. The Office of Thrift Supervision described its agency's efforts in providing guidance to thrift institutions on retail on-line personal computer banking. We have added to the report OTS' expectations that thrifts providing services over the Internet evaluate and mitigate risks to their on-line systems. See page 9.

# Major Contributors to This Report

---

**General Government  
Division, Washington,  
D.C.**

Carl Ramirez, Senior Social Science Analyst  
Delois Richardson, Computer Specialist

---

**San Francisco Office**

Denise Callahan, Evaluator-in-Charge  
Grace Sakoda, Evaluator  
May Lee, Evaluator  
Gerhard C. Brostrom, Communications Analyst

---

## 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.

### Orders 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 touchtone 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 an e-mail message with "info" in the body to:

[info@www.gao.gov](mailto:info@www.gao.gov)

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

<http://www.gao.gov>



---

**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**

---

