Comptroller of the Currency

Administrator of National Banks

Internet Banking Security:
Safeguarding Customer Information

Thursday, July 19, 2001

9:00 a.m. – 10:30 a.m. EST

Presented by:

John D. Hawke, Jr.
Clifford Wilke
Carter Messick
Joan Bryant
Jeff Gillespie
Deborah Katz

Mr. Dalton: Today's Comptroller of the Currency Administrator of National Bank's program is Internet Banking Security: Safeguarding Customer Information. At this time it is my pleasure to turn the program over to the 28th Comptroller of the Currency John D. Hawke. Jerry, welcome to the program today.

Mr. Hawke: Welcome to the fourth in a series of OCC telephone seminars to the banking industry. When we launched these seminars last fall we did so with the idea that they would serve as a convenient and effective means of communicating with you on pressing supervisory issues. The enthusiastic response we have had to each of them proves that we are meeting the need for real-time information and for opportunities to engage in that dialogue with OCC experts who happen to be among the nation's leading experts in these areas. I know that you will benefit substantially both from the presentations and the question and answer session that will follow. I cannot think of a more urgent issue before the banking industry than Internet banking security. And I cannot think of five more qualified people to discuss it than the OCC experts who are with us today.

Leading the seminar will be Cliff Wilke, our director of bank technology and one of the nation's most respected experts on bank technology supervision. After Cliff's introductory remarks, you will hear from Carter Messick and Joan Bryant, two national bank examiners with extensive experience in conducting IT examinations. When they are done, Cliff, Carter, and Joan will be joined for the Q&A session by two senior members of the OCC's legal team, Deborah Katz and Jeff Gillespie. Deborah was a major participant in drafting our guidelines for safeguarding customer information. Jeff, in his capacity as assistant chief council, is responsible for the management of special projects, particularly those involving electronic banking. If one of these five people cannot answer your questions on Internet banking security, I am not sure that anyone can.

You have read about Internet security issues all the time. Some of you may have experienced security problems with your own systems, and you know that problems in this area can seriously affect your bank's reputation and its relationship with customers. Concern about information security is perhaps the foremost reason why so many Americans are still reluctant to bank electronically, a primary obstacle to a bank's reaping the benefits of the information revolution. Until your customers achieve that level of comfort and confidence in the security of their personal information, banks will be unable to take full advantage of the potential efficiencies and marketing opportunities that the new technology makes available. Understanding the threats to your information systems and how to protect against them, is one of the central topics we will cover today. Our presenters will also address the issue of supervisory expectations, particularly for the information security requirements set forth by the Gramm-Leach-Bliley Act of 1999. Joan and Carter, in particular, will talk about what they have encountered in the IT area as they have carried out technology exams around the country. With that insight, you will have a better idea of what constitutes an effective information security program and what to expect when your IT examiner comes calling. It promises to be an interesting and worthwhile session. Thank you for deciding to be part of it.

Mr. Dalton: Thank you, Mr. Hawke. And now we will conduct our second polling question of the day. We are curious how many people are listening in at your site today. And again using your touch-tone keypad, if you are the only one in the office listening to today's program, simply press 1. If there are two of you in the room, press 2. If there are three in the room, press 3. And so on up the line. If by chance there are nine or more people listening in at your site today, simply press 9. And thanks for participating in our second poll question. Now you can turn to page 12 in your materials, and we will begin. It is my pleasure to turn the program over to Clifford Wilke. Hi Clifford.

Mr. Wilke: Good morning. Thanks, John. First, I would like to thank each of you for participating in our call today. It is our intention and goal that you will gain additional information on the risks that you could use immediately to reduce the risks associated with Internet banking. Only by working together and addressing the security issues proactively will we reach our goal of providing the safest and most secure delivery channel to our customers. To bankers this is not a new equation. It is a fundamental cornerstone of our industry. Our goal is to provide you with informal discussion by OCC staff on the issues we see banks facing today. During the teleconference, we will include some hypothetical factual cases that will be used to illustrate certain points. And these cases are not intended to represent any actual occurrences.

In addition during the call, we will take some more informal polls. It is our intent to see that the results are confidential. In addition, the OCC cannot identify the response of any one person. However, technology has made this feature available, we want to be able to take advantage of it to provide you with the most beneficial information.

Following the prepared remarks by myself, Carter, and Joan, we will have a question and answer session. It is our goal to answer these questions on the subjects that we are discussing today. However, we do want to let you know up front that the answers are “unofficial opinions of the OCC staff involved in the call” and, secondly, we will not discuss any particular questions regarding a specific institution, service provider, or occurrence.

Having said that, the first question you may ask is: Why do we focus on Internet security and authentication? There are three reasons. First, based upon what we have seen in recent Internet banking examinations at our banks, the risks are greater with emerging technologies, some technologies with which you may not be totally familiar.

Secondly, we have seen a lot more activity in the area of Internet fraud and hacking attempts. One cannot pick up a paper these days and not read about the occurrence of an Internet event.

And, thirdly, with the provisions of the GLBA Financial Modernization Act, taking effect on July 1, the requirements for privacy and security that are the critical elements for compliance, our goal is to provide you with suggestions of where to start, what to address, how to monitor the risks, and how to check to ensure that you are in compliance. In addition to discussing direct risks, we will address the unique risks that exist when using a service provider. Included in the appendix review is a copy of the guidelines for safeguarding customer information.

The next slide highlights the recent developments in the areas of emerging technologies. The developments have enabled financial institutions to provide new products and services to their customers at a pace that has never been seen before in the industry. Today the Internet has reached critical mass proportions in the United States and at a rate never seen before. For example, if you will look back, radio took 38 years to reach critical mass proportions. Television took 14 years. I think we can count on one hand how many years it has taken the Internet to reach these same critical mass proportions. The challenge that bankers and regulators face together is how to keep pace with the technical developments. The nature of the network Internet environment alone provides instant access globally to information, products, and services. The Internet, not only presents great opportunities, but also provides some unique challenges, and a whole new set of expectations from the customer's perspective. I like to use the analogy that as the front door of your bank faces Main Street in the town where you live, with the Internet your bank has a window to the world. Yes, this cannot only provide opportunities, but it can also present the potential for unique challenges and risks that must be monitored and addressed.

The next slide reflects the projected growth of Internet banking. The experts may differ in their exact figures. However, one fact remains. The market is growing. In my opinion, the growth of Internet banking users will be directly relational to the number of Internet users. However, we may see a faster growth rate especially if new products and services enter the marketplace.

The following slide highlights the innovation in financial services. According to industry experts, the primary driver to get more customers to use the Internet delivery channel may be the lure of these new products and services. When you look at what new feature may drive the marketplace it is anyone's guess at this point. However, I see a few products on the horizon. Products may provide comprehensive online account history, one-stop shopping via account aggregation, bill presentment and/or bill payment, electronic authentication and digital signatures to verify the customer's identity, or Web site hosting.

One enticing horizon, and moving fast, especially outside the United States, is the anyplace, anywhere, anytime features that the wireless delivery channel can provide. However, to gain the customer's trust and overcome the primary concern that many customer surveys have noted - the security issue - banks must ensure they are following and establishing the highest standards of safety and soundness. However, when you think about it, it is no different than customers' current expectations about physical security faced at banks today.

The next slide shows the growth of national banks currently offering transactional Internet banking. We see the number of institutions continue to grow. However, be aware that the majority of the large banks today are currently offering transactional Web site capabilities. When we look at the total picture, we see that currently 69 percent of the 2,342 national banks have a Web site. When we look at future projections for national banks, we see that 52 percent expect to offer transactional Internet banking by year-end versus 21 percent only two short years ago.

At the OCC we have taken a multifaceted approach to supervising the risks associated with Internet banking. In 1999 we issued a comprehensive Internet banking handbook. The handbook focuses on risk analysis, measurement, controls, and monitoring consistent with the risk tolerances associated with the delivery channel. We have performed numerous risk-based examinations of banks and third party service providers, which include onsite examinations and quarterly reviews that focus on safety and soundness issues and targeted reviews of banks with transactional Web sites and e-banking service providers. In the last year alone, the OCC has provided basic IT training to all 1,800 OCC field examiners. In addition, we provided targeting Internet banking training to almost 600 examiners and even more advanced Internet or security-rated training to more than 300 OCC field examiners. I share this with you, so that you are aware that we are in the same position as you and realize that we must focus our attention on providing proper training internally. Through industry outreach, Meet the Comptroller Meetings, and other events, we have successfully raised the bankers' awareness of the risks. We have also published guidance to new organizers and the enhanced application process.

The next slide focuses on security self-assessment. When you look at your bank, you should ask yourself the following questions: Is information security a priority for your bank's directors and senior management? Are you confident in the effectiveness of your written security program? Are you and your service providers ready to respond to security incidents? Only by asking the questions and providing honest answers can you truly establish a strong starting point to assess these risks.

Earlier I mentioned we would take polls throughout the Telephone Seminar, but be assured the results are confidential, and we cannot identify any individual response. So John, I will turn it back to you for our first polling question.

Mr. Dalton: Thanks, Clifford. Our first polling question is, "Does your bank provide customers with access to account information through the Internet?" Press 1, if yes. Press 2, if no. Press 3, if not a banker. Again the question, "Does your bank provide customers with access to account information through the Internet?" Press 1, if yes. Press 2, if no. Press 3, if not a banker. And now at this time I will turn the program over to Carter and Joan. Welcome to the program.

Mr. Messick: Good morning. Today's topic and Cliff's introductory remarks make it evident that the OCC expects information security to be a priority at your bank. In today's presentation, we focus on Internet banking security for three reasons. We start the discussion on page 18 of the handouts.

First, we have seen a sharp increase in the amount of fraud and security incidents reported by national banks. The FBI's National Infrastructure Protection Center sent out several alerts related to increased e-commerce and e-banking attacks. The OCC responded to this increase with OCC alert 2001-4, which advises banks of eight key actions that you can take to reduce your risk exposure to network security vulnerabilities.

On the fraud side, the Federal Trade Commission has recorded a large number of identity theft victims. In fact, they are currently logging about 1,700 complaints and inquiries a week. The ease of access and the sense of anonymity increases the likelihood that criminals will continue to look for ways to use Internet connectivity to threaten banks and your customers. Strong security reduces your exposure to what we now see as real threats.

The next two slides illustrate the increasing trend in security incidents. The first exhibit shows the increasing number of reports from all Internet sites to the Computer Emergency Response Team Coordination Center or CERT. The chart shows only events reported to CERT, and you would expect actual numbers to be much higher. The second exhibit shows an increase in the number of actual security incidents reported by national banks to the OCC. Since our numbers are based on what our banks have reported to us, they do not reflect necessarily an increase in actual events, but are due maybe in part to increased reporting.

On page 20 of the slides, we look at the next reason why the OCC considers security to be a priority. Our examination findings have supported the need for additional risk management efforts for Internet banking. As of March 31, 956 national banks offered Internet banking services. By the time of our presentation, all of those banks should have received an initial Internet banking examination, and dozens of additional banks will have rolled out Internet banking.

Service providers exercise a major role in most of our banks' Internet banking efforts. In fact, more than 75 percent of national banks outsource their Internet banking applications to a service provider. These companies often provide a cost-effective way for community banks to deliver a new service, while benefiting from additional expertise and experience that they can offer. However, even if you are serviced, your bank remains accountable for safeguarding your customer information. You can outsource the day-to-day duties related to technology, but the bank is responsible for the oversight of security and controls.

Let us move to the bottom of page 20 and discuss a few of our exam findings. Based on our examinations, we have identified eight key success factors that result in strong risk management. Most of those factors have direct or indirect security implications.

Today's presentation will discuss some of those issues in more detail, but I wanted to highlight specifically two key factors, because they really do ensure that all the other factors are addressed. First, active vendor management is essential for Internet banking, because of the degree of reliance you must place on third parties. Few banks are alone in their Internet banking efforts. Internet banking software developers and servicers, bill paying providers, Internet access providers, network security consultants, and others can affect your security. Given the high degree of access to the bank's system and to the customer's information, none of you want to be the weakest link.

Second, strong security is critical to your bank's reputation and to your customer's confidence in your Internet banking system. Security must be a concern at the board of director level. Both of these issues are key elements in today's presentation. On the next slide on page 21, we had a regulatory reason to prioritize security. In February, the OCC issued, OCC Bulletin 2001-8, that distributed the interagency guidelines for safeguarding customer information required under GLBA's Section 501(b). These guidelines require banks to implement a comprehensive written information security program. The requirement provides community banks with some flexibility by using a language appropriate to the size and complexity of the bank's operation. But really all banks must have a documented risk assessment and an adequate written security program consistent with the objectives contained in the guidelines. Despite the Internet focus of today's presentation, these guidelines are not confined to Internet banking only or even to information technology. The risk assessment and the security program must address all aspects of your operation. We use Internet banking as an example of one area that you need to address.

Now for examination coverage for most community banks, our examiners will integrate the examination of compliance with these guidelines into the normal supervision of your bank. For most banks, the procedures will be incorporated into the community bank's supervision handbook with three or four questions or procedures. For some banks, expanded Internet agency procedures may be used. These expanded procedures should be published probably by the end of this week.

At the bottom of page 21, our slide provides a brief outline of what is required by the 501(b) requirement. For some security-conscious banks, the guidelines may require doing a little more than you have always done. But most of you must revalidate your existing security programs at least with a risk assessment. You must also include any additional controls, training, and testing. The guidelines describe a process and not specific controls to implement. We included an excerpt of the news release with the guidelines in the Appendix on page 42. Essentially in a *Reader's Digest* version of a bank's efforts to comply with the guidelines: you must involve your board of directors in the development, approval, and maintenance of the program; assess the risk to your environment; manage and control those risks by considering controls in eight different categories; train your staff and adequately test your controls; effectively oversee your service providers and adjust the security program for changes in the risk and sensitivity of your systems and information; and finally, report to the board at least annually.

So to recap quickly, computer crime, OCC examination results, and the new regulatory requirements related to customer privacy all make security an important issue and underscore the need for board involvement. Internet banking provides increased opportunities for unauthorized access to nonpublic customer information and often to the bank's payment system. You must include Internet banking and Internet connectivity in your security risk assessment process. That point makes a good transition to Joan's next section.

Ms. Bryant: Thanks, Carter. In this section, I will discuss the security risk assessment process and common security controls. But first, let us focus on what it takes for an information transaction to be considered secure. As you can see on the bottom of page 22, two security objectives exist for 501(b), confidentiality and integrity. Secure transactions must possess integrity, meaning the transaction was not altered while being transmitted. Without integrity, there is no guarantee that the message your customer sent to the bank matches the message that the bank actually received. Secure transactions must also possess confidentiality, meaning the context of messages remain private as they pass from the customer through the Internet to your bank. Without confidentiality, anyone can view the transaction message and gain private information. A confidential transaction requires a transaction to be authenticated, meaning you know who sent the transaction. Authentication is one element of confidentiality. And without good authentication techniques, you have no way to be sure that the person sending the transaction's instructions is the person they say they are.

In addition to privacy, achieving confidentiality and integrity would yield the added benefit of nonrepudiation, meaning that both the sender and the receiver of a transaction agree that the information exchange took place. Without nonrepudiation, the customer can easily say they never sent the message or initiated the transaction.

So to recap briefly, if you know the message has not been altered, and you know the message remained private throughout the transmission, and you know who sent the message, you have achieved privacy and nonrepudiation. Achieving these security objectives requires a combination of processes as well as technologies.

So with these concepts in mind, let us talk about where to start. Before you can manage and control risk, you must conduct a risk assessment. Where are the threats and vulnerabilities within your environment? How significantly do they affect the confidentiality, integrity, and availability of your bank's systems or the customer's need for privacy. In terms of security, risk is a function of threats, exploiting vulnerabilities that affect your bank's assets.

So what is a threat? A threat is something, such as a person, thing, or event that poses danger to an asset's confidentiality, integrity, or availability. Threats can be deliberate, such as a hacker attack, or operational, such as someone sending a message to the wrong address.

So what is a vulnerability? A vulnerability is a weakness in your control system or the complete absence of a control. You can think of threats and vulnerabilities as being similar to the potential for your car being stolen. The threat of your car being stolen exists, and there is not really much you can do about that. But if you leave your car unlocked and sitting at the mall for hours, it is much more vulnerable to being stolen than sitting locked in your garage at home. The effect would be the difference between having your dirty gym socks in the back seat or your wallet sitting on the front seat. Each piece of your technology infrastructure possesses vulnerabilities that are exploitable by threats. Security is not about any one control. It relies on a layering of multiple controls that often overlap each other. Over reliance on or overconfidence in a single control, such as a firewall, often ignores other easily exploited vulnerabilities.

So now that we have discussed threats and vulnerabilities, let us move to the risk assessment process. The new 501(b) guidelines specifically require risk assessment that includes three factors. These are listed on the bottom of page 23. First, you must identify the threats to customer information. On the top of page 24, we have listed some examples of Internet banking threats and types of attacks. This is not an exhaustive list, but only some of the more obvious threats and types of attacks. So now moving back to the bottom of page 23, once you have identified the threat, you should assess both the likelihood that your environment would be affected by the threat as well as its impact, I want to emphasize that this exercise should not concentrate solely on dollar losses. In fact, dollar losses associated with attacks have been relatively minor to date. However, the privacy breach can harm, not only your bank's reputation, but also your customer's acceptance of Internet banking. It could also result in identity theft for your customer. As a past victim, I can tell you that that is a huge hassle and its effects can linger for a long time. Lastly, you should evaluate the adequacy of your controls. And we will discuss controls in greater detail shortly.

On the bottom of page 24, we have listed only some of the issues to consider when completing the risk assessment. I am certain you will develop some of your own criteria. Obviously, every bank is different. Some community banks still have closed networks with dedicated connections to service providers, including their Internet banking service provider. For those banks, you want to focus primarily on application security, information handling, and end-user guidance. But your security responsibilities expand as your environment grows more complex. Everyone should approach this process with the review of both their automated and manual controls. You must also educate yourselves and your staff about potential threats.

A common question we have received at the OCC is, “Is risk assessment a one-time process?” As you can see on your slide, “No.” This is not a one-time event. The 501(b) process is a dynamic one that requires continuous monitoring to adjust the program as necessary. The risk assessment process is one component of the overall 501(b) process, and it should be updated whenever significant changes are made to your technology environment. In a stable environment, you will want to update the risk assessment at least annually. Keep in mind that new ways to exploit technology weaknesses are discovered each day. Your risk assessment could become dated fairly quickly depending on the technology platforms you use and the external parties to which you may be connected.

I believe we have a polling question now. And John will tell you about it.

Mr. Dalton: Thanks, Joan. You will see our next polling question on page 25, “Has your bank completed a security risk assessment?” Press 1, if yes. Press 2, if no. Press 3, if you do not know. Press 4, if not a banker. Again the question, “Has your bank completed a security risk assessment?” Press 1, if yes. Press 2, if no. Press 3, if you do not know. Press 4, if not a banker.   Now I will turn the program back over to Carter and Joan.

Ms. Bryant: Now let us discuss what should be included in your security program. Once you have completed the risk assessment and have a better handle on the threats facing your bank, the next thing you must do is review your written security program. For most banks, this will be to update their existing security program. However, some banks actually may need to develop the program. For any products or service, the security program should cover all aspects of the bank’s operations, not only the IT department, and it should include or at least reference your existing administrative, physical, and automated security controls.

In the next several slides, we will provide examples of these controls and illustrate their importance in some case studies. Listed on the top of page 26 are several administrative controls, with which I am sure you are all familiar. I have a few suggestions for you to consider in examining these controls from an Internet banking perspective. You should expand your existing security awareness programs for your employees, contractors, and Internet banking customers. If you do not already complete employee background checks and require your employees to sign a user security agreement, you should. Annual training and security updates, followed by a signed user agreement are effective tools in preventing mistakes and prosecuting violations, should that become necessary. Many banks also provide security awareness information, when customers enroll for the service. You should also provide this information continuously through your Web site, statement stuffers, and other regular customer communication. You also should ensure that security configurations are current, and that changes are documented, approved, and tested. We cannot emphasize this control enough. The OCC recently issued Alert 2001-4 on network security vulnerabilities to target this issue.

You should designate someone at the bank to be responsible for monitoring for new vulnerabilities. They can accomplish much of this through e-mail subscriptions, notification services, or Web sites. With this information, they can assess the risk of the new vulnerability and implement a fix if that is necessary. They should use multiple sources to get this information. You also must make sure your changes are not made quickly without proper testing or review and approval of the fix. You must also ensure the fix comes from a trusted source.

At the bottom of the slide, we have listed some effective policies we have seen in our banks. Because of the number of people using your Internet banking technology, and its distributed nature, you must assign responsibility formally and communicate clearly your standards and expectations. You should develop formal policies or update the ones you have if you have not done so already. As we have said earlier, we have some case studies to discuss. Carter is going to walk us through the first one.

Mr. Messick: Thanks, Joan. Today's presentation has four case studies. The case studies are a composite of various situations that the OCC has encountered, and we will use these hypothetical cases to illustrate the principles we discuss.

The first case on the bottom of page 26 is an example of poor administrative control. We have a bank that prints customers' social security numbers on their bank statements. The bank also uses the last four digits of the social security number as the default password for the initial login to the Internet banking application. One of the customers who has never logged onto the Internet banking system moves without changing his/her address. The new resident receives the bank statement and is able to use the customer's social security number to transfer funds from the customer's account. Weeks go by before the customer detects the theft.

Now turn to page 27 and we will talk about how this type of problem could be avoided. The most obvious lesson is that you should not put a customer's social security number on your bank statement, and you should discourage customers from even recording it on their checks. You should stop using a common identifier, such as a social security number, as a part of the initial login process, when possible. It is also much smarter to require customers to request activation of Internet or telephone banking services during an application process, rather than automatically activating all your customers. You could also establish initial customer setup procedures, including password distribution similar to the way you handle ATM PINs. One option would be to give customers the ability to setup their own initial passwords during an encrypted Internet session or at the bank to enhance the confidentiality of their passwords. This example also highlights the importance of adequate authentication of new Internet banking users, which leads to Joan's next slide.

Ms. Bryant: Although we were talking about administrative controls, I wanted to emphasize the importance of authentication, that is, verifying who you are dealing with. Because physical contact with the customer may not be part of your Internet banking process, you may need to develop alternate means to verify new customers who want to open a deposit account or obtain a loan online. In the last case, the bank did not adequately authenticate the customer before allowing online account access. As you can see, sound authentication controls are critical to the security of your systems and your customer's privacy. I believe we will issue at the end of this week an interagency guidance on authentication controls. Essentially, the guidance requires authentication techniques to be commensurate with the level of risk associated with the transaction or information. IDs and passwords may not provide enough protection, and you should evaluate this.

On page 27, we have listed some events where sound authentication controls should be implemented. To be effective, authentication techniques require good administrative control. Some questions to consider include: What information do you obtain for a new Internet banking customer? Do you require written documentation or proof of identification? And how do you verify this information? Automated services exist to run customer applications through third-party verification services. But you must set the standards for acceptance, rejection, or additional verification. That is, if information from the customer's application does not match the external verification services database, does it result in a rejection of the customer's application? When would additional verification be required?

Another issue to consider: What personnel at your bank have the capability to establish online account access for your customers? Is there a process to review this activity? Does this duty conflict with other responsibilities they may have? Also, what are the authentication controls required for funds transfer and bill pay? How are they different from those used to allow customers to view account information? And what about reporting and monitoring online transaction activity? Are you doing this at all?

Lastly, do your employees obtain adequate information before providing customer information or password resets over the phone? Could someone fool them with information stolen from a wallet or a bank statement? How many databases have your customer's mother's maiden name?

Our next case provides a good example of the importance of authentication. Carter will present it.

Mr. Messick: Now let us look at a second case for an example of poor authentication procedures. This case is on page 28. In this example, an employee at Bank A for whom the bank had never done a background check, steals account information about Bank A's customers and uses it to open up fraudulent accounts online at Bank B. Bank B has a person-to-person payment system that uses the ACH system to allow new customers to fund their deposit accounts more quickly. The employee transfers funds from the customer accounts at Bank A into his fraudulent accounts at Bank B. The employee continues to initiate transactions for several weeks. Eventually one of the customers detects large withdrawals and notifies Bank A. What can banks do to avoid this type of problem?

First you should, as a part of your hiring procedures, perform thorough background checks on employees who have access to sensitive information. You also should have effective authentication procedures in place before permitting accounts to be opened online and before initiating Internet-originated ACH transactions. Online account origination requires additional fraud detection controls. As Joan mentioned, some banks have used third-party verification services to validate application data immediately and to help reduce the likelihood of identity theft. New ACH rules placed the authentication burden more clearly on the ACH originator and required that Internet-initiated ACH transactions be labeled with a WEB or web transaction type. The additional flag can help you review these transactions for suspicious activity.

Now we will turn the microphone back to Joan to discuss physical controls.

Ms. Bryant: As Carter said, I would like to emphasize the importance of physical controls and to stress that they should not be overlooked. On the top of page 29, we have listed some physical control issues to consider. These are not new concepts, but things that you should keep in mind as you introduce new equipment into your environment. As you know all of the automated controls designed into the technology can be easily circumvented if you have weak physical controls.

We will now move onto the discussion of automated controls that begins at the bottom of page 29. When talking about Internet security, most people think about automated controls, such as firewalls, in fact firewalls are only one of many automated controls that should be included in your program. Essentially, these controls provide a way to automate a manual control, so that it is simpler, more effective, and more reliable. But remember automated controls can be worthless without strong management support, security expertise, and administrative policies and procedures. Some of the many controls that should be considered in a security program are listed on the bottom of page 29.

But I have a couple of quick points. At exams we often see where management may not have activated all the security features that are available in the application. Banks should review security settings and ensure that the appropriate combination that is featured has been activated. You should also ensure that default IDs and passwords are removed. Also if you do not need a particular file or service, remove it because it contains vulnerabilities that can be exploited. Encryption techniques provide confidentiality when implemented correctly, but they also add another layer of security if customer information is breached. Bear in mind, 128-bit secure socket layer, supported by most browsers, provides encryption protection only while the information is being transmitted. It does not provide protection when the data is stored. In fact, many banks are moving to virtual private networks to further secure communications.

Virus protection. We all know viruses can bring down the system. Some of us have learned that the hard way, but they can also provide a hacker with the means to access your system remotely. There is also the risk of spreading the virus to your customers. Additionally, as a vendor-hosted website, you should ensure the vendor also is protected against viruses.

Lastly, if you have connected your bank's network and core banking systems to the Internet as part of your Internet banking solution, you know that a firewall is an essential control. A firewall is a combination of hardware and software that monitors Internet traffic into and out of your network. Firewall software can limit access to unauthorized users, prevent the transfer and sending of files to or from your servers, and prevent the sending or receiving of e-mail messages with file attachments. So you can see how firewalls serve to restrict access between your network and other public networks, and that firewalls are an essential element of security.

On the top of page 30, we have listed some key items to consider to ensure that your firewall is well controlled. Regardless if your firewall is hosted in-house and your staff is managing it or if you have outsourced this responsibility to someone else, you must ensure that these items have been addressed. Firewalls do not come ready to install out of the box. They must be configured and managed. You should know who has high level access to the firewall. You also must have a basic understanding of the rule sets, that is: What traffic is allowed? Firewall rule sets fall into two basic categories. The first, denies all traffic, except that which is specifically allowed, or allows all traffic, except that which is specifically denied. Obviously, the first rule set provides greater security. The latter of these is much more difficult to manage and control. Clearly, a strong process to manage and track firewall changes is essential. An unauthorized change here

can undermine your entire security program significantly.

I want to emphasize that having a firewall alone is not enough. It does not provide any protection, if it is not well monitored and well managed. Many things can work together to weaken the effectiveness of a firewall. This includes limited functionality, poor firewall placement within your network, the lack of firewall policies or management practices, and inadequate staffing. Although firewalls control Internet traffic into and out of your environment, they do not provide any protection for access achieved via traditional methods, such as modems dialing directly into your system. Many third party providers often use this access method to support your Internet banking system. Appropriate controls should be implemented for this type of access, including controls for activating the line, configuring the modems appropriately, callback procedures, logging access, and routinely searching for unauthorized modems in your environment. Now here is Carter to discuss our next case.

Mr. Messick: This case, on the bottom of page 30, is an example of poor automated controls. A bank hosts its own Internet banking system, using a purchased software application; a hacker scans the bank’s web server, using readily available vulnerability assessment software. At the time the bank is unaware of the scan. The hacker exploits a vulnerability picked up by the scan and is able to download the bank’s password file on some customer account information. Even though the passwords were encrypted, he could have potentially run password-cracking software to obtain clear text passwords. When investigating the incident, the bank learns that a patch was available that could have fixed the vulnerability several months earlier. The vendor distributes a patch to the bank for installation.

We can take several lessons from this case. First, if you have an in-house Internet-connected system, you must implement a process to track your hardware and software for new vulnerabilities and install security patches as soon as they are available and tested adequately. If you have in-house Internet banking applications, you probably will be able to monitor adequately only for intrusion and test intrusion-detection controls by implementing an automated intrusion detection system. You or your service provider should periodically perform vulnerability assessments and penetration tests to identify weaknesses more proactively.

In the next section starting on page 32, I will discuss intrusion detection and vulnerability assessment in more detail. As the title indicates, this section focuses on methods to monitor security risk and test controls. We will discuss system monitoring or security audits to full-scale penetration tests. The need for these methods and their scope of use should be determined by your bank's risk assessment.

First, *system monitoring*. Most of you have always done some level of security monitoring for core banking applications. Internet banking system security must be closely monitored. You can start by reviewing the activities of privileged users and security exception reports, failed access attempts, and even verifying account maintenance. Most Internet banking providers have begun to add more monitoring reports for banks to use. For banks with in-house Internet operations, newer generation firewalls provide reporting and real-time alert capability for certain types of access attempts. There is also security management software available that can automate security policy enforcement throughout your network. Another form of monitoring is the logging and review of all program changes.

Intrusion detection is another form of monitoring that we will discuss on the next slide. Intrusion detection systems can evaluate incoming and outgoing traffic more thoroughly than a firewall. Firewalls must allow certain traffic through for legitimate purposes. Hackers and hacker attacks often seek to exploit that. An intrusion detection system can analyze packets of data for known attack signatures similar to the way virus detection software works. As with virus software, an intrusion detection system must be kept updated for new types of attacks. Intrusion detection software tools can reside on specific servers to detect intrusions to your hardware software or at various locations inside and outside a computer network. It then analyzes the network traffic moving through different network segments and alerts you to predetermined events. The OCC issued OCC Bulletin 2000-14 that underscores the importance of considering the need for intrusion detection systems in your bank. It also provides guidance on an appropriate intrusion response plan. Intrusion detection systems provide an additional layer of filtering beyond the firewall. To some extent, those systems can also help test the adequacy of firewall rule sets. But one of the primary benefits of an intrusion detection system is that it allows you to respond more quickly to problems.

That point leads us to our second slide on page 33. This slide reviews the key issues to address in your intrusion response plan. These points are contained and more thoroughly discussed in the guidance that I mentioned. One important reminder from this slide is that the OCC recommends that all successful intrusions be reported on a suspicious activity report by the bank. You can also see that the slide includes two questions.

"Do serviced banks need a response plan?" Absolutely. Serviced banks that offer Internet banking must have at least a basic intrusion response plan. It probably would not be nearly as detailed as what an in-house bank might prepare, but it could address the steps you would take in terms of vendor and customer communication, evidence handling, mitigating steps that would limit a repeat intrusion, and information sharing. Reviewing and understanding your vendors' intrusion response plan in communication policies would also be important.

"Why notify customers, if no money is lost?," because of the potential effect on your reputation and the possible legal liability. Regardless of the dollar losses, if a customer's information is breached and they are susceptible to identity theft, you should inform them. Many companies have found that the reputation damage is much greater when they conceal an intrusion, and it is discussed, than when they communicate it more proactively to their customers. By concealing a privacy breach, you may also create potential legal liability if your customers become victims of identity theft.

We also encourage banks to report security events to information-sharing organizations. If they act as trusted clearinghouses for new threats and recommended responses, they can better protect the industry as a whole.

On page 34, we change the subject to discuss the use of audit coverage. Obviously, a bank's internal and external audit coverage should include the security associated with Internet banking systems. Audit coverage that includes verification procedures is one of the most basic ways to test security controls consistent with the

501(b) guidelines. If you provide Internet banking and your audit does not review security controls, you should expand the scope. Even for banks relying on Internet banking service providers, the audit scope should include physical security governing record handling and access to information and systems; payment systems or funds transfer security; application security, including user access levels for employees; password composition and administration; network security, emphasizing Internet access controls; and controls over remote access to your bank's system.

Looking at the bottom of this page, vulnerability assessment provides an excellent additional verification method for security practice. Vulnerability assessment is merely an attempt to identify known weaknesses that could be exploited. It would be difficult for any bank with Internet-connected systems to test its patch process in configuration management without periodic vulnerability assessment. The most common site to which we refer when talking to bankers is network-based and includes a scan of the network from the outside in to look for known vulnerabilities in firewall rules or network configurations. Another type of vulnerability assessment software actually resides on the specific host or server and can periodically scan that server or operating system for security weaknesses. Vulnerability assessment is only effective, if it is conducted periodically with additional use after you make changes to your systems. Some banks use these tools in-house, but others establish contracts with third parties. Commercially developed and supported products are the most likely to be updated and maintained for new vulnerabilities. But numerous products certainly are available for free on the Internet.

Lastly, the assessments are absolutely no good, if their findings do not receive prompt follow-up, risk assessment, and correction.

From vulnerability assessment, we move on to penetration testing. The two are easy to confuse and in our next slide we will discuss the difference. Penetration testing actually subjects the system to real-world attacks. It really is the ultimate test for an in-house system, but it does increase your cost. It tests the effectiveness of security controls and provides an excellent means to test your intrusion detection and response plan. A penetration test may start with using vulnerability assessment software. The testing personnel use any identified security weaknesses to attempt to gain access to the system. It will typically use additional means to identify potential weaknesses like phone calls or e-mail looking for modems. You must determine the extent of security testing based on your bank's risk assessment. But the OCC issued early Internet banking guidance that required penetration testing for banks with an in-house Internet banking system. These banks account for about 25 percent of our banks with Internet banking. In those cases your systems are subject to unauthorized penetration attempts everyday, and you have no control over the scope or timing. Penetration testing becomes an essential method to identify proactively correct new risk exposures before an unauthorized penetration attempt succeeds.

The testing personnel do have the potential to gain access to your system. Banks can control that risk by selecting reputable third parties, defining an appropriate test scope and obtaining nondisclosure agreements. That concludes this section. An important final point is that policies and controls can lead you to a false sense of security if you do not have adequate monitoring and testing. You must use your risk assessment to determine the necessary scope and level of monitoring and testing needed for your system. This will help ensure that your policies and controls are implemented effectively.

Now John has our last polling question.

Mr. Dalton: Thanks, Carter. And our last polling question is,“Has your bank or service provider experienced a security incident that resulted in a potential privacy breach?” Press 1, if yes. Press 2, if no. Press 3, if you do not know. Press 4, if not applicable. Again the question, “Has your bank or service provider experienced a security incident that resulted in a potential privacy breach?” Press 1, if yes. Press 2, if no. Press 3, if you do not know. Press 4, if not applicable.

We will have the results on all polling questions shortly. And I will now turn it back to Carter and Joan.

Ms. Bryant: Thanks, John. We know that oversight of service providers is not a new concept to bankers. Given the growing trend with outsourcing, the OCC has issued some recent guidance on service provider oversight. We have listed two of these issuances at the bottom of page 36. A common problem that we have seen at exams is management, not including Internet banking service providers and their established vendor management programs. You must ensure that your program includes your Internet banking servicer, your Internet service provider or ISP, your bill pay provider, and your Web site host. You also must make sure that your contracts with service providers include provisions detailing the responsibilities to protect customer information as required by 501(b). You have until July 1, 2003 to get existing contracts into conformance. However, contracts originated after March 5 of this year should already comply.

On the top of page 37, we have listed reports you should receive routinely from your service providers in addition to the annual financial information you normally obtain. These reports will help you monitor how well your servicer protects your bank's and your customer's information.

We have also included some pointers to help you assess the adequacy of SAS 70 audit reports. If you are not familiar with SAS 70 reviews, these are external audits that provide some level of assurance about the control environment at your servicer. They come in two types. Type one reviews provide assurance that policies, procedures, and internal controls exist. They do not provide verification and testing of internal controls. Type two reports include the actual testing of the controls. Because servicers control much of the scope of these reviews and their timing, you should review these reports to ensure that all material controls have been tested reasonably often. Also depending on the nature of the service provided, you should review your servicer's security assessments, penetration tests, and security incident reports. You must document your conclusions from these reviews and report your findings to the board.

On the bottom of page 37, we have listed some issues to consider when selecting a service provider. The OCC's advisory letter 2000-12 on the risk management of outsourcing provides a much more comprehensive list of factors to consider and is really an excellent resource.

Our final case appears on the top of page 38. Once again Carter will review it for us.

Mr. Messick: This last case is an example of why banks must oversee their service providers. When a customer calls to question a transaction, a bank will report to its service provider that it realizes that some wire transfers initiated by one of its customers were fraudulent. The service provider’s investigation finds that in each case the proper IDs and passwords were used, but the customer insisted that they did not initiate the transaction. The investigation concludes that the system was breached. They find proof that the hacker had been in the system, but they are unsure how he/she broke in. To make matters worse, the servicer confirms that the user ID and password files were among those copied by the hacker.

Here are some of the controls to better address this situation. Your bank is responsible for securing customer information, and your reputation is on the line. You can outsource security management and IT services, but you must continue to oversee the relationship. You should ensure that your vendor firewall and security controls are tested independently, then evaluate the adequacy of those tests. You may need to establish more conservative password composition standards and use more conservative security settings built into the Internet banking system.

A bonus recommendation, not appearing on the slide, would be to monitor Internet-originated transactions for suspicious activity. Ultimately, even banks and service providers with good security controls and testing may still experience a security breach, so communication with service providers becomes critical. Banks and their providers should discuss their policies on communicating information on security events. You should ensure that your service provider will inform you of any security event that has jeopardized your customer’s information. Now please turn to page 39.

We have reached the conclusion of our presentation and over the last hour we outlined the case for security being a priority at your bank. We explained the importance of starting with risk assessment and provided a basic description of what to include in your security program. We also described the key ways to monitor and test your security controls, and Joan related these issues to your service providers. Because today's information was fairly basic I will quickly provide a few additional resources before we move on to the Q&A portion of the presentation.

First, the OCC has issued guidance in a number of security-related areas, many of which we have referenced in today's presentation. Some of the most important issuances to read include: Infrastructure Threats and Intrusion Risks, OCC 2000-14; Risk Management of Outsourcing Technology Services, Advisory Letter 2000-12; Network Security Vulnerabilities, Alert 2001-4; and, at the top of the list, Basel Committee Report Outlines Risk Management Principles for Electronic Banking (News Release 2001-42). The latter provides an excellent primer for senior management and directors and 14 key risk management principles. It can be found on the OCC's Internet banking Web site under international electronic banking supervision. Despite the international label, it provides excellent guidance to community banks as well as large banks, as does the final document, Guidelines Establishing Standards for Safeguarding Customer Information or the 501(b) Guidelines in OCC 2001-8. The guidelines require you to have an effective security program. We used Internet banking today as an example of one aspect of your operations that you should consider.

On page 40, we have a screen shot of the OCC's Internet banking Web site. It is a good starting point to look up any of these issuances and additional regulatory information related to Internet banking. It is clearly referred to and easy to navigate.

At the bottom of the page, we have provided some additional Web sites that are good sources for security resources and information. The Purdue site will allow you to enter your hardware and software by name and version and provide you with a list of potential vulnerabilities by product.

So, in conclusion, Internet banking security is a priority, and there are many motivators to move banks to action. Regulatory expectations are only one of them. But it should not be your primary motivator. We leave you with two action items. First, you must ensure that you complete a security risk assessment. It provides the foundation for your security program. Then you must implement a comprehensive security program that includes board involvement, adequate internal controls, continual monitoring, testing, and third party oversight.

That concludes our prepared remarks. I will now turn the presentation over to John to discuss the polling results and begin the question and answer portion of our call.

Mr. Dalton: Thanks, Carter. Here are the results of our polling questions. First, we have more than 900 people listening to today's program.

On our first poll question, "Does your bank provide customers with access to account information through the Internet?" 68 percent voted, yes, 26 percent voted, no, and 7 percent voted, not a banker.

On our second polling question, "Has your bank completed a security risk assessment?" 60 percent voted, yes, 28 percent voted, no, 5 percent voted, don't know, and 7 percent voted, not a banker.

On our third poll question, "Has your bank or service provider experienced a security incident that resulted in a potential privacy breach?" 24 percent voted, yes, 51 percent voted, no, 17 percent voted, don't know, and 8 percent voted, not applicable.

Now I would also like to welcome Deborah Katz and Jeff Gillespie to our Q&A session. If you would like to ask a question, you can do so merely by pressing number 1 on your touch-tone keypad. This will put you into the queue. When your turn comes up, we will call on you by city and by first name. If you are listening on a speakerphone, please pickup the handset when you ask your question. We will be able to hear you much better that way. If your question is answered while you are in line, you can press the pound (#) sign. This will take you out of the queue. So if you have a question, go ahead and press 1 now. You can do this at any time during this Q&A session. Again if your question is answered while you are in line, pressing the pound (#) sign will take you out of the queue before your turn comes up. So press 1 to get in line. Press pound (#) to get out of line. The fax number for questions is 715-833-5469. We can accept only one question from each site. We will go to Joseph's site in Kansas City with our first question. Go ahead.

Kansas City: Can you tell me on the risk assessments, if you see those more on a business aspect or a technical aspect. And how detailed do they get?

Mr. Wilke: We had a hard time hearing you. Could you please repeat the question again? Perhaps try to get a bit closer to the phone.

Mr. Dalton: Yes, pick up the handset please.

Kansas City: OK, I will shout. On their risk assessments, do you see those being performed more as a business analysis or a technical analysis, how detailed are they getting?

Mr. Wilke: I will ask Carter to please address this question first.

Mr. Messick: I would say that really the risk assessments will vary, but I think it will be a combination of both. You will have to look at your business processes and then at the specific technical aspects of your systems and how they affect risk. And I would expect the scope of those risk assessments to vary quite a bit based on the size and complexity of the bank. A small bank lacking an Internet connection or much complexity to its system might have much less detail than a larger bank. But as you bring more and more systems in-house, more and more technology in-house, I think you will have more technical risk assessment.

Ms. Katz: I would like to chime in. This is Deborah. Do not forget that the risk assessment must also address physical controls.

Mr. Wilke: OK, John, next question.

Mr. Dalton: Alright, we have two other callers left in the queue. We will go to Sandy's site in Elk River, Minnesota. Go ahead. Sandy, are you there? Is your mute button on?

Elk River: Yes, we are here.

Mr. Dalton: Go ahead with your question.

Elk River: We only wanted to know the Web site again where we could put our information systems, and it would lead us to our potential problems.

Mr. Messick: Oh, yes, this is Carter again. It was on page 40, www.cerias.purdue.edu. Basically, it is a nonprofit organization that has a product called Cassandra that will let you track vulnerabilities in your software.

Elk River: OK, thank you.

Mr. Messick: You bet.

Mr. Wilke: These are provided for you as references. Please be aware we are not recommending any particular site or one site over another. This is only a list of different ones available today for you to use as a reference.

Mr. Dalton: OK, we will go to our next caller. Four callers are now in the queue. Brenda's site in Huntsville, Texas. Go ahead.

Texas: Yes. I have a question about background checks on employees. Is it really necessary to do a background check on all of your employees or can you restrict that to only your DP operators and those kinds of people?

Mr. Wilke: I would like to ask Carter to please address that.

Mr. Messick: Yes. That would be something you would look at, what the employee has access to, and what systems they will access. Certainly in most community banks, a network administrator has access to the bank's systems and its information. That would be someone who, that as you hire someone new, you should conduct a background check on. Many banks have call center when they become larger, and customer service employees have access to information there. You might have a lot of turnover in that staff, and background checks would be important. I think Deborah has something to add.

Ms. Katz: Yes, this is Deborah. Are you only talking about Internet banking or are you talking about banks generally?

Texas: Generally or how do you mean it? Do you mean it only for Internet banking or for all of our employees?

Ms. Katz: No, even tellers can have access to sensitive information about customers. In the example that Carter gave, a bank employee could use information about an individual customer to transfer funds into another bank. So, although it is probably a business decision on your part, we would encourage you to perform background checks for all employees that have access to sensitive customer information.

Texas: OK, that answers my question. Thank you.

Mr. Dalton: We will move to San Francisco. To Thomas' site.

San Francisco: Yes, what are the special considerations for an Internet bank that wishes to enter into a service provider relationship with a company offshore in a developing nation?

Mr. Wilke: I will ask Jeff Gillespie from the legal department to address that question.

Mr. Gillespie: This is Jeff Gillespie. I would be happy to answer that. The most important issue is the questions that arise about ensuring that the bank has access to the information transferred abroad. That can actually be more difficult than what you would expect, because the issues of choice of law and choice of jurisdiction can be quite technical. You really should get your lawyers involved any time that you are looking at using an overseas service provider. This will depend on your time frames, because if you will be using a provider in the next several months, we have been focusing on this issue, and hope to issue some guidance on it, probably in the next two months or so.

San Francisco: That would be really good, because our horizon is short.

Mr. Gillespie: We are aware that with increasing globalization more and more banks are thinking of using offshore service providers. We should issue guidance on that soon. But you must make sure that you do not run inadvertently into problems with choice of law and choice of jurisdiction, and lose control over your data. I think that is the best I can do for right now.

San Francisco: Thank you.

Mr. Dalton: Three other callers are left in the queue and 17 minutes are left in the program. Press 1 to get in line, if you have a question. We will go to Owing's Mills, Maryland, to Melanie's site. Go ahead. Melanie are you there? Is your mute button on?

Maryland: Yes, we are. Actually, I am not Melanie. I am George and our question pertained to risk assessment. A comment was made earlier that risk assessments will vary in how they are conducted. Do you plan on issuing additional guidance on risk assessments, so that there will be more consistency throughout the entire Internet finance sector?

Mr. Wilke: Let me turn it over to Carter to start.

Mr. Messick: I know we have looked at that, and there has been within the agency some pilots on or some drafts of the risk assessment guidance. So that may be something that we can issue guidance on. I do not think there is any formal effort to issue guidance right now, but it is certainly a good recommendation and an area where we could provide some additional information. I wish I could provide more. Is that responsive?

Maryland: Yes, thank you very much.

Mr. Messick: You bet.

Mr. Dalton: We will move to Sheila's site in Las Vegas with a question. Go ahead.

Las Vegas: Yes. I am reiterating what the last caller said. We are in the middle of doing a risk assessment today and are at a point where we cannot stop drilling deep. It seems as if everything we look at we should be drilling deeper and deeper. I would really like some help that would give us a little more guidance on what the hard buttons are? What should we be pushing hardest? My second part of this question is how often should an extensive risk assessment like this be conducted? I understand that it is a living document and will be addressed daily, but how often should a complete risk assessment be done?

Mr. Wilke: I would like to ask Joan to address that please.

Ms. Bryant: I definitely sympathize with your frustration or process in which you find yourself drilling deeper and deeper. I can understand exactly how you could find yourself doing that. And I guess my response to that would be is that you should focus on systems by criticality and how sensitive it is. You want to focus more on sensitive customer data.   To help you know where to focus, I would suggest you know what you are doing with data classification and to rank your systems according to criticality. The second part of your question, how often? You acknowledge that it is a living document. How often should you go back and review it completely? Basically, we are saying that for stable environments, you want to complete a risk assessment annually or at least review it annually. Does that answer that question? Clearly, the more complex your environment, the more rapidly things evolve and the more often you will have to do that.

Las Vegas: That is fine. I appreciate it.

Mr. Gillespie: This is Jeff Gillespie. I just want to emphasize something that Joan said that an annual assessment is fine. But at the time you begin to initiate new systems you should engage in an assessment. Say, for example, that you decided to offer account aggregation services when you were accepting PINs from your customers for third-party sites, that is clearly the kind of database that has a high degree of sensitivity and should have adequate security and controls. You would want to be sure of that.

Mr. Messick: This is Carter. I had one more thing and we will let this one move on. I think it is difficult to throw a rope around the risk assessment process. I think it will be something that the bank has to work through. Maybe this will be a learning experience, especially when you do it the first few times. But one thing I have seen a bank do, as Jeff said, is that anytime that it had a new system, the bank took a risk assessment worksheet or form and went through it and checked off common considerations that the bank would ask itself each time it changed the system. I think that is a good process to help speed up the updating of the risk assessment. Each time you change your environment, you have already done this little quick process, when you are doing your due diligence of the change you were making, and you can add that to your annual review that you do.

Mr. Dalton: OK, we will move on to our next caller, which is Daniel's site in St. Paul. Go ahead.

St. Paul: Hi, my name is Pete Johnson. I have a question more toward the board of director involvement. Typically, the question arises about how formal should be the actual approval of the security program and/or its presentation. That is the first question. The other is: Do I have to get a written signature or is being on the board of directors' agenda and presenting enough?

Secondly, can the entire board of directors, a committee of the board of directors, or a designate of the board of directors approve a bank's security program? Let's say if your CIO is a vice chair and reports into the board, is that level appropriate for approval of the security program? It seems to me fairly vague and not so clear on how far we need to take that.

Mr. Wilke: I will ask Deborah to take a first shot at it, please.

Mr. Dalton: Deborah, is your mute button on?

Ms. Katz: With respect to your first question about whether you have to obtain signatures. As long as board approval is recorded, that ought to be sufficient. For example, it could be recorded in minutes of the board. And second, with respect to involvement of the board, our security guidelines say the board of directors or an appropriate committee of the board can approve the bank's written information security program and conduct the oversight. Do you have some additional questions about that?

St. Paul: Well, not really. I think you know we have an audit committee on the board of directors that would probably be the appropriate place from which to get that direction. But the other piece is in GLB itself. It says that the board of directors must designate an owner of the overall security program. And, again, does that have to be somebody that is actually on the board or could it be an employee within the actual enterprise?

Ms. Katz: Yes, we were expecting that that would be an employee. We do not expect the board to be engaged in day-to-day oversight of the bank's operations. But we do expect that someone will and that would be someone employed by the bank.

Mr. Wilke: I think the real intent was to ensure that security is looked at as critically as other important aspects of the bank, including credit, risk, etc. And it is supposed to be part of the overall program with regard to the importance of how important security is today, not only the Internet, but also the physical world.

Mr. Dalton: OK, we will move on to our next caller. We have one caller left. Again press 1 to get in line. We have about nine minutes left. We have time for a few more questions. Robin's site in Lyons, Nebraska. Go ahead.

Nebraska: Yes, the OCC performs examinations of service providers, of which we can get and read the results. My question is how often do you do that and are those results on the Web site?

Mr. Wilke: I will ask Carter to address that.

Mr. Messick: We generally will examine the service providers at least every 24 months. They have to be a certain size and have a certain number of customers before they represent enough risk for us to go in and examine them. But most of the Internet banking providers have received interagency examinations. The reports are available from the OCC typically by requesting a copy from the district office in which your bank is located. Availability from other agencies differs slightly among them.

Nebraska: And we did that. I only wanted to know if it was on the Web site.

Mr. Messick: No, it is not on the Web site. And we have to be pretty careful with that, because we only provide that report to customers of that service provider, current customers. It is not something you can use in your due diligence efforts or anything. But if you are currently serviced by that company, you can request a copy of a report, and if we verify that you are a customer, we send a copy to you.

Nebraska: Thank you.

Mr. Messick: You bet.

Mr. Dalton: OK, one more caller again. Back to Thomas in San Francisco. Go ahead.

San Francisco: My question has to do with the organizational placement of information security. Does the OCC have any opinion on where that can be most effective? Whether within technology or at a higher level within the organization? Any input there?

Ms. Bryant: Hi, this is Joan. We do not have a formal opinion on where that function needs to reside. I think it will vary by bank and what you will be doing. I have seen a lot of different placements X having the technology department divided on lines of business, so that the platforms of support retail credit report to the head of retail credit. I have also seen centralized IT functions. I think its success or failure will depend on the culture of your corporation. I would say that for such functions as technology risk management-type practices, vendor management, information security, technology audit, we see a variety being centralized or decentralized. It comes back again to the fact that you need a coordinated effort to perform vendor management or information security. So often you may see that the corporation that has a centralized technology risk management function to handle vendor management or information security has better success than one that does not.

Mr. Messick: This is Carter. I will add something quickly. One knows that the larger the bank, often the more separate and distinct is the information security department. And you might move it up into a report into risk management along with the business continuity person. But the smaller the community bank, the harder it is to separate the security function from the information technology staff.   I think that to the extent that you can, it is good to have that independence, and it is a prudent practice at least for someone to oversee and review reports who is outside the information technology area. But I think it has very much to do with the size and complexity of the bank and the extent that you can actually separate that out from the IT area.

San Francisco: Thank you.

Mr. Messick: You bet.

Mr. Dalton: OK, two other callers are left in the queue. Five minutes are left in the program. We will go to John's site in New York. Go ahead. John are you there? Is your mute button on?

New York: Yes. Sorry. It is Maria. Did I understand correctly that there would be new guidance coming out the end of this week on administrative controls, authentication, and passwords.

Ms. Bryant: You did understand me correctly. There is interagency guidance pending on authentication. However, I made a mistake when I said it would be the end of this week. I confused it with the examination procedures that will be issued at the end of this week. The interagency guidance on authentication is under development, and I think is nearly finished. So it should be issued soon.

New York: Is soon two months or six months?

Mr. Gillespie: This is Jeff Gillespie. I would say we are talking about a matter of weeks. I would be surprised if it took us more than four weeks to get it out.

New York: Great. Thank you.

Mr. Dalton: Alright. Back to Las Vegas, to Sheila's site. Go ahead.

Las Vegas: Yes, this is Gary again. Getting back to the complexity and drilling deep, I am trying to make sure that we are on the right track in understanding that the OCC has limited resources. Are there any suggestions about who could review our plan to make sure we are on the right track, about risk assessment? We have internal auditors. I am not sure that they are knowledgeable about exactly what we should be looking for. Are there any suggestions you can give us to help someone who is looking at our plan so that he/she could make sure that the assessment has been complete.

Mr. Wilke: Hi, this is Cliff Wilke. I think you have a number of different options available to you. I think some of your accounting and auditing firms are looking at these kinds of functions today. There are also specialized security firms that are examining the security issues. Actually, some of the third party providers provide that as part of their service to you. Carter, do you have any other ideas?

Mr. Messick: I think it is always possible to send in a third party for an advanced look to your portfolio exams. If everybody is sending those in and trying to get feedback, it would probably be overwhelming and something we could not do, but I am sure that, in some cases we could certainly take a look and review those exams and see if you are on the right track. It may not be right away, but it is something we might be able to do over time. But in the exams when we actually go in and look at these, hopefully, we should be working with you to help look for ways that could improve the risk assessment as well.

Las Vegas: That is great. Thank you.

Mr. Dalton: OK, we have time for one more caller. Back to Thomas in San Francisco.

San Francisco: Hi, this is Kathryn and I am the vendor management administrator. My question is, I actually have three, but they related. Number one is, Can we get a transcript of the presentation? Number two is, do you provide or have any resources or could you direct us to resources that would provide us with the general outline of solid risk assessments at the company level? And the third one is, do you have any suggestions, we are having some difficulties with some of our smaller vendors and getting this level of data security documentation from them as in the SAS 70 information. Do you have any suggestions for some of these smaller vendors and how to encourage them to meet with them in compliance with OCC guidelines.

Mr. Wilke: Hi, this is Cliff. I will be glad to answer the first question for you initially, and then I will have to turn to the rest of the panel for the second and third questions you asked. With regard to the transcripts, yes, they are available. And you can request them through the vendor KRM that conducted the conference today. Carter, second question?

Mr. Messick: Yes, as far as sources go, about the information on how to fill out a risk assessment or format, the resources that we provided were nonprofit Web sites. We were not really endorsing those. But from my standpoint, they are potential sources to find some information about security program or risk assessment. There are a number of other commercial sites to which you could probably go to a search engine and find. But it would really be more difficult than going to a third party and having them assist you in developing it. It would be difficult to give you a lot of other links on the Internet that would not be some kind of an endorsement of someone else's product or service. But the links that we have are a good start. Certainly the sans.org is a good site for information on security programs.

Ms. Katz: And on the third question, you should try to handle obtaining reports through your contracts with your servicers and require that before you start doing business with a servicer that they agree to get your reports. Because your servicers today do not do that, you might consider finding a servicer that will give you access.

Mr. Dalton: OK, Clifford we are out of time and I will turn it over to you for some closing remarks.

Mr. Wilke: Thanks, John. In summary, it has been our true pleasure to share with you our perspective on Internet security issues associated with Internet banking. Only by working together can we proactively address the issues to ensure that the highest standards of safety and soundness are achieved. It was our goal to raise the awareness and the issues on this important topic. I hope that we achieved this goal. On behalf of Comptroller Hawke, Carter, Joan, Jeff, Deborah, and myself, thank you very much for participating. Have a great day.

This program continues with the Q&As from the second session.

Mr. Dalton: OK, and thanks. Before we get into Q&As, we will cover those polling questions. First, we have more than 800 people listening in on this morning's program.

To our first polling question, "Does your bank provide customers with access to account information through the Internet?" 75 percent, voted yes, 18 percent, voted no, and 7 percent voted, not a banker.

To our second polling question, "Has your bank completed a security risk assessment?" 52 percent, voted yes, 32 percent, voted no, 10 percent, voted don't know, and 7 percent voted, not a banker.

And to our final polling question, "Has your bank or service provider experienced a security incident that resulted in a potential privacy breach?" 25 percent, voted yes, 50 percent, voted no, 17 percent, voted don't know, and 8 percent voted, not applicable.

I would also like to welcome Deborah Katz and Jeffrey Gillespie to our Q&A session. If you would like to ask a question, you can do so merely by pressing number 1 on your touch-tone keypad. This will put you into the queue. When your turn comes up, we will call on you by city and first name. If you are listening on a speakerphone, please pick up the handset when you ask your question. We will be able to hear you much better that way. If your question is answered while you are in line, you can press the pound (#) sign. This will take you out of the queue. So if you do have a question, go ahead and press 1 now. And you can do this at anytime during this Q&A session. Again if your question is answered while you are in line, you can press the pound (#) sign. This will take you out of the queue before your turn comes up. So press 1 to get in line. Press pound (#) to get out of line. Again the faxed number for questions is 715-833-5469. We already have four callers. Let us first go to Fairfield, Texas to Pam's site. Go ahead.

Texas: Yes, a question about security on the Internet on e-mail. Can you address whether we are using a product that helps secure e-mail communications?

Mr. Wilke: Hi, this is Cliff Wilke. Unfortunately, we will not address any specific products or technology. So that is something that you probably want to discuss with your vendor and ask them how are they keeping it secure and really addressing it that way.

Mr. Messick: As applied to communications, you want to make sure in your communiqués with customers or with other third parties that your e-mail is secure, if you are relaying nonpublic customer information or sensitive information to the bank. So having encrypted e-mail would probably be a good idea. Is that responsive?

Texas: Yes. Can you hear me?

Mr. Messick: Yes.

Texas: I understand you cannot address the specific products, but in general do you have a good solution to encrypting e-mails since that is a nonsecure channel?

Mr. Messick: We do not, other than with your customers, you cannot. You may have some of your corporate customers sign up or subscribe to encrypted e-mail, and install an encrypted e-mail package, but a safer policy with retail customers, especially to make sure you have policies that restrict your employees from e-mailing nonpublic information between the bank and your customers.

Mr. Wilke: Joan, your thoughts?

Ms. Bryant: I only had one really quick point about how often we see within the retail Internet banking application an e-mail communication capability that allows the customer to e-mail back directly to you without going outside of your actual product or network. So that also provides a safer mechanism.

Texas: OK, thank you.

Mr. Dalton: OK, we will move to Gerard's site in Evelith, Minnesota. Go ahead.

Minnesota: Good morning. Many of us have only started the process of selecting the third-party service provider. Without recommending a specific vendor, is it possible for you to provide us with a list of vendors that meet your guidelines and have passed third party reviews and/or have passed reviews on site in banks.

Mr. Wilke: I will ask Jeff Gillespie from the legal group to take a first shot at this one.

Mr. Gillespie: And since you are talking with a lawyer, you know the answer.

Minnesota: I know.

Mr. Gillespie: We would wish we could pass that on to you, but government ethics prohibit us from providing endorsements for particular firms. But if you undertake the due diligence process outlined in advisory letter 2000-12, we are quite confident you will find a good vendor.

Minnesota: Thank you.

Mr. Dalton: Alright. Two callers are left in the queue. Again, merely press 1 to get in line. We have 20 minutes left in this Q&A session. We will go to Larry's site in Miami. Go ahead.

Miami: Hi, I hope everyone is doing well. It is a very informative seminar, and we appreciate it. I had a particular question about the differences between vulnerability testing and penetration testing. We have had our penetration testing done, and I wondered if that covered our aspect of the vulnerability testing at least as far as our Internet banking is concerned?

Mr. Wilke: Let me toss that to Carter.

Mr. Messick: Anytime we talk about testing, we return to the risk assessment that the bank must support to the scope and the level of testing that you are doing. But a penetration test probably first included vulnerability testing in order to know what types of attacks the bank wanted to try on the system. I would also encourage banks to consider vulnerability assessment as more ongoing than the actual penetration test. But again the frequency, scope, and the level of testing, whether it is only a vulnerability assessment or it extends to a penetration test must be decided by the bank based on risk assessment. So you must support a vulnerability assessment. Then you can talk to the examiner about its scope and frequency. But certainly it would be valuable to schedule interim assessments between penetration tests.

Mr. Wilke: Joan, your thoughts?

Ms. Bryant: I only have a point about penetration tests. I think the scope can vary widely from where they were able to get in to where they actually went further toward the vulnerability assessment spectrum for possible social engineering or a network architecture-type analysis. A difference on the vulnerability assessment side of the spectrum would be that the bank might be looking at and evaluating its security policies and identifying its critical assets and vulnerabilities rather than merely performing limited penetration tests.

Miami: OK.

Mr. Dalton: Alright. Our next caller is Karen's site in Austin, Texas. Go ahead.

Texas: Thanks. Much discussion about the due diligence on the third party processors dealt with the actual servers and ISPs, etc., but many community banks have joint marketing arrangements with an array of third party vendors, such as securities firms and annuities products and those who also have Web sites. Is it appropriate in the analysis and the due diligence to ask those third party vendors for their technology assessments, such as an SAS 70 audit, etc?

Mr. Wilke: This is Cliff again. I think part of your due diligence process is the normal business conversation of asking them: How they are doing it? What will be their procedure for doing certain things? How do they react to certain occurrences? What are their normal standard operating procedures that they use daily? If you are working with third party vendors in a business relationship, you have a joint interest in ensuring that the activities are being done with the highest levels of safety and security.

Carter: Your thoughts?

Mr. Messick: Yes. It will probably happen, if a bank's service providers outsourced different aspects of its operations to another company, and the bank did not actually have a contract with that company. So the service providers may have to support the bank's efforts to comply with 501(b), by conducting their own risk assessment, that is, by getting their own information from the companies that support them and distributing it to their banks. So I think that it is reasonable for a bank: (1) to ask a service provider about its due diligence process with the companies that it relies on; and, (2) to get a listing of those companies. If those companies will be handling your bank's data, you must be able to identify them and their privacy practices and know that their security will be solid. It is reasonable to expect your service providers to do that.

Mr. Gillespie: This is Jeff Gillespie. I would like to add another thought. You have to look at the legal configuration of the joint marketing relationship. Some of them involve actual servicing relationships, when the joint marketing party actually performs services on behalf of the bank, in which case Advisory Letter 2000-12 would apply. But occasionally you have only a pass off, when the bank essentially transfers its customers to the third party. In that case, more of a disclosure issue exists, in terms of making sure that the customers know that they are being transferred, and that they must worry about the third party's security and privacy policies. For guidance, we have recently issued a bulletin on web linking. Although the discussion addresses web linking specifically, it can be applied more generally to joint marketing relationships when there is a referral. And Deborah has an additional thought.

Ms. Katz: Hi, this is Deborah. Speaking specifically about the 501(b) security guidelines. Those specifically state that a bank's review of controls of the servicer should also include a review to ensure that any subservicer used by the service provider will be able to meet the objective of the guidelines. That is all I have to say.

Mr. Dalton: OK, we will move on to our next caller. We only have one left in the queue. Again, merely press 1 to get in line. David's site in La Jolla, CA. Go ahead.

La Jolla: Has there been any change by the OCC in reviewing audits relative to our reliance on the SAS 70 provided by the vendors in a servicer environment?

Mr. Wilke: Carter?

Mr. Messick: I do not think there has been a change, but merely receiving a SAS 70 will not always be sufficient. I mean looking at the scope of the SAS 70, that is, looking at the operations evaluated by the audit firm and the level of independence. I would encourage user banks, certainly if it is a large user group to become involved in looking at the scope of a SAS 70 review and providing their own input. I make this suggestion, particularly, if the banks want certain areas examined, because some of the security-related issues may not have been included within the verification procedures that were part of the SAS 70. So a SAS 70, by itself, may not be in default, but it must be reviewed and evaluated. You may also want to ask your service provider to perform additional testing.

La Jolla: Can I ask an additional question?

Mr. Messick: You bet.

La Jolla: Is there guidance in one of these issuances that would tell us what should or not be included in a SAS 70, so we would know if it met the standards?

Mr. Messick: Again, we do not have a standard for SAS 70 themselves. I mean that is contained in the accounting rules. But the scope of the review will be negotiated between the service provider and the audit firm doing the SAS 70 review. It is based typically on their existing policies and procedures.

Ms. Bryant: Yes, there is no specific laundry list of controls that should be included within the SAS 70. It will vary by company, based on what they are doing. So management, in conjunction with the external audit firm, will determine the critical controls and how to proceed with testing. Generally management details those controls, so that is the main distinction between a type 1 and a type 2 report. A type 1 report addresses the controls that management has outlined for the auditors, and the auditors have commented about whether those controls are designed to meet the control objectives.

Mr. Messick: A SAS 70 review usually would not include a penetration test. It might or might not include a source code review for security issues within the source code of the Internet banking application. There may be some companies that are providing subservicers, such as a bill payment provider for an Internet banking vendor, and the bill payment aspect is not included within the SAS 70 coverage. So only going through and looking and seeing whether the key areas, and key controls are addressed.

La Jolla: Right.

Mr. Messick: Is that responsive?

La Jolla: Yes. In the vendor that we are using, it appeared that they did have a level 2, and they discussed penetration testing and vulnerability testing and the other controls that you mentioned. So I have been relying heavily on that SAS 70 in evaluating this vendor, and I only wanted to make sure that there was not something else that the OCC could provide to assist me.

Mr. Messick: I think largely you are right. The SAS 70 will provide you with good assurance that they have found internal controls and that they have been tested to a degree. And so you can look to the SAS 70 as one source of assurance.

La Jolla: Yes. Thank you very much.

Mr. Messick: You bet.

Mr. Dalton: OK, two other callers are left. Let us go to Susan's site in Kansas City. Go ahead.

Kansas City: Hi, this is Marshall. My question is related to the interagency guidelines. The guidelines require that a risk assessment be performed. On page 46 of your handout section C3, the last sentence says that, "Tests should be conducted or reviewed by independent, third parties or staff independent of those that develop or maintain the security program. If the program includes the risk assessment, does this mean, therefore, that the internal or external audit firm that is performing the independent tests that the risk assessment cannot be relied upon by management for purposes of compliance with the guideline?

Mr. Wilke: Deborah?

Ms. Katz: I think that if you are using the third party, you can rely on them. It is only that we wanted a party who is not involved in the day-to-day operations of the bank to review the results of any tests that were conducted. You do not need a third party necessarily to review your risk assessment. The reference to third parties was really to having someone conduct tests or review tests separate from those involved in the operations of the bank.

Kansas City: I think my question is more, can the tester be the risk assessor? Or does this have to be management's representation of its risk or its self-assessment as was referred to at the beginning of the presentation?

Ms. Katz: In other words, you are asking, can you hire a company to do your risk assessment and can you hire the same company to do your testing?

Kansas City: No. The question is: If internal audit performs a risk assessment, can management rely on that risk assessment solely or do they have to attest somehow to it and to its completeness in order to comply with these guidelines?

Ms. Katz: There should be a separation of function. I do not know if anyone else wants to chime in, but I do believe that the board has to be involved in reviewing the bank's information security program and cannot delegate its responsibility to internal audit.

Mr. Wilke: Joan, do you want to give us another perspective on it?

Ms. Bryant: Yes. I would say only from an internal audit function, I have been doing risk assessments for years to help determine the scope, frequency, and timing of their reviews. I would say generally you do not see a translation of risk assessment into business risk and the effect of vulnerability on the operational side or the business side. So I think you might have an issue and some independence conflict there. If you are relying solely on the auditor's risk assessment, and they and you are using it as your risk assessment I can see some problems with that.

Mr. Dalton: OK, we will move on to our next caller. Follow-up from Pam's site in Fairfield. Go ahead.

Fairfield: This is Ron. Yes, thank you for letting me call in twice. I have two questions. One is related to the discussion you had with the SAS 70 report. Our provider provided a fairly exhaustive SAS 70 report, as I am sure the other callers did. Along that line, although the vulnerability testing report was merely a letter of certification from the CPA firm that they performed the review. No scope and no test results were given. Should we require more of the vulnerability testing scope and test results or can we rely on a big 8 CPA firm's certification that it was adequate?

Mr. Wilke: Why do not we go ahead and let Carter address your first question. Then we will return to your second one. So Carter, why do not you jump in for the first question?

Mr. Messick: I do not believe that only a statement of certification is sufficient, if you do not know the criteria and the scope of the assessment. The criteria and scope really enables you to know or to verify that the risks are managed properly. If your risk assessment says that this service provider furnishes a service that must have more frequent annual penetration testing or vulnerability assessments, then the service provider must be a little more responsive to customers. The servicer could provide a report that, at least, shows the basic scope and the key findings of the assessment. Many service providers say that they do not want to provide confidential information that could be contained within the results of the penetration tests. But they can easily remove that kind of information and place the scope and key findings in an executive summary, which would reveal the issues and management's response to them. I think that is an extremely reasonable request that deserves follow-up as part of security practices when we look at a service provider. You should forward those issues to your examiners.

Fairfield: Thank you. I had a second question, but you sounded like there was someone else to whom you wanted to address something.

Mr. Wilke: Go ahead with the second question.

Fairfield: OK, sorry. Regarding the risk assessment process, certainly new technologies would be done on the Internet banking, etc. But how much risk assessment should we expect the Internet service providers to perform? Keeping in mind that they have a lot of contracts and third party connections to provide the connectivity of the Internet service, and it has been around for about five or six years on a Web site, using basic e-mail and maybe postcard-type Web sites. What level of risk assessment do we need to do with them?

Mr. Dalton: Excuse me, this is John. We have 30 seconds left to answer that question.

Fairfield: Alright.

Mr. Messick: This is Carter. As far as the risk assessment of a service provider, they would not perform a 501(b) risk assessment, but they should have a security program and risk assessment as a part of that. There are many ways that a service provider can support a bank's efforts to comply with their 501(b) requirements. One way would be to conduct their own internal security risk assessment and provide a summary of that to the bank.

Mr. Dalton: OK, we are about out of time. Clifford, you have 30 seconds to wrap up the program.

Mr. Wilke: Thanks, John. In summary, it has been our pleasure to share with you this morning our perspective on the security issues associated with Internet banking. Only by working together can we address proactively the issues to ensure that the highest standards of safety and soundness are achieved. It was our goal this morning to raise the issues and your awareness on this important topic. I hope that we achieved this goal. On behalf of Comptroller Hawke, Carter, Joan, Jeff, Deborah and myself, thank you very much for participating.

Mr. Dalton: A quick reminder to everyone. We encourage you to fill out and fax in your evaluation sheet. You will find that that phone number is listed on your evaluation form. Your comments and suggestions are important to us and help us to provide you with future quality programming. That is all the time we have this morning. Thank you for joining us and enjoy the rest of your day everyone.