Slide 1

Welcome, once again, to this teleconference on Outsourcing Technology Services—A Management Decision.

To enable you to follow the session, we have provided you with a handout that contains slides, and we will be referring you to them periodically.

As Comptroller Hawke indicated, outsourcing technology is a management decision. It is not a new activity. For many years, banks have used third party servicers to provide their customers with an array of products and services. So, that being the case, you may be wondering why, then, are we focusing on outsourcing?

Some of the reasons for this teleconference include the following facts, which by the way are not listed in any specific order of priority or risk:

First, the nature and types of outsourcing activities are expanding. Banks are outsourcing whole business processes in addition to IT services.

Second, there is an increasing trend of outsourcing in item processing due primarily to upgrades necessary to comply with Check 21.

Third, the emergence of new technologies, products, and services is resulting in more banks becoming reliant on third parties. For example, there is increasing reliance on a new type of service provider – Manage Security Service Providers. To these, banks are outsourcing their perimeter security and / or their internal network security.

Fourth, technology service providers, like the banking industry, are merging with or acquiring either competitors or other service providers to diversify or to broaden their product offerings. The resulting consolidation and potential concentration of servicers may limit your banks' choices and could result in changes to the servicer's levels or quality of service.

Fifth, service providers are either existing companies delivering new technologies or new companies that have appeared within the last five years to provide emerging products and services. Often, these latter companies are dealing with new security and control issues, and some are servicing banks for the first time. These companies may lack control standards or their inexperience may lead to weak controls affecting a servicer's entire customer base.

Sixth, financial weaknesses in new or fast growing providers can increase the risk of service interruptions resulting from business failure or control breakdowns that can be caused by distracted management or overworked personnel. And,

Seventh, new legal requirements are being introduced which reinforce your responsibility for managing outsourcing relationships.

So, if you turn to the agenda in slide #2, you will note that

Slide #2

We will begin with a brief overview of frequently outsourced activities and highlight the most common outsourcing relationships.

We will identify relevant regulatory guidance and expectations.

We will discuss the risk management process, including: risk assessments, due diligence, the importance of the contract, and ongoing monitoring.

We will highlight what you can expect during an examination that addresses outsourcing, and

We will cover two items we consider hot topics:

- Foreign outsourcing and the special risks you should address
- And intrusion and incident response. Here, we will discuss how unauthorized access to customer data maintained by service providers should be addressed in your bank's incident response programs

And, finally, we will recap our presentation and reserve time for a question and answer period.

Now let me turn over to Bob Wicksell who will talk about frequently outsourced activities.

Slides #3 & 4. Thank you, Aida.

Banks are increasingly relying on services provided by other entities to support various business and technology related functions. The decision to outsource can be driven by various factors. For example, banks may outsource for economic benefit, to gain operational efficiencies, to enable increased management focus on core business functions, to obtain specialized expertise, and accelerate new product delivery.

Commonly outsourced services include those listed in slides # 3 and 4. Others include IT or back-office operations like: the origination, processing, and settlement of payments; information processing related to customer account creation and maintenance; call centers; security monitoring and testing; system development and maintenance to name a few.

Banks have utilized technology service providers for years and have generally managed these relationships in a reasonable fashion. The rapid growth, in terms of the number of banks opting to outsource, AND, the new services being provided, direct us to highlight some of the risks involved.

Additionally, as Aida pointed out, new legal requirements are being introduced to reinforce bank management's responsibility for managing outsourcing relationships. As we will discuss in detail, Section 501(b) of GLBA imposes specific obligations on bank management with respect to the security of customer data that is outsourced to service providers. Further, many banks will be directly or indirectly subject to the requirement under section 404 of Sarbanes- Oxley that they assess and report on their internal controls. This obligation will extend to the adequacy of their controls over third party service providers.

Some historically well-managed banks have found themselves faced with unanticipated problems because bank management underestimated the need to manage, monitor and control the bank's outsourcing relationships and activities.

But, before we move on to risk management associated with outsourcing, let's look at the most common types of technology service providers.

Let's turn to **slide # 5**.
Technology Service Providers included, but are not limited to:

- Other financial institutions,
- Non-banking providers, regulated or non-regulated,
- Non-banking providers affiliated to a bank or independent, and
- Of course any of theses may be domestic or foreign-based.

Under federal law, the OCC and other federal banking agencies have clear authority to regulate and examine services performed for banks.

In regards to regulatory guidance, **Slides 6 and 7** highlight OCC and the other FFIEC agency issuances relative to outsourcing.

All of these highlight the board of directors and bank managements continued responsibility for the oversight of outsourced activities. They also mandate that these activities be conducted in a safe and sound manner and in compliance with applicable laws and regulations.

The guidance emphasizes that banks should have a comprehensive outsourcing risk management process to govern their technology service provider relationships. The process should be conducted in a manner that is commensurate with the risk tolerances and abilities of the bank.

Now, Debbie Fussell will discuss risk management

Thanks, Bob. Ok. I am on **slide 8** and this is the beginning of our discussion on the risk management process.

Regulatory guidance requires that banks adopt a risk management process to identify, measure, monitor, and manage the risks associated with outsourcing. Generally, four steps are recommended and are outlined on slide 8.

These are: a risk assessment that addresses both business and IT-related risks, due diligence to identify and select the servicer, a written contract that outlines duties and responsibilities of both parties, and on-going oversight of the arrangement.

The process is not a "one-size-fits- all approach," however. Each bank's risk profile is unique and requires a tailored risk management process. You should consider the scale and complexity of the outsourcing arrangement, materiality of risks identified, and your bank's ability to manage the risks.

Slide # 9 addresses the first and perhaps the most critical phase of a good risk management process, and that is the risk assessment.

A key element you should consider is whether the proposed outsourcing activity is aligned with strategic goals of the bank. First of all, what is being outsourced? What will this do for the bank? How does the service provider help the bank achieve its goals?

Typically, risk assessments are conducted by management and personnel associated with the particular business line. In addition, representatives from security, business continuity, audit, compliance, legal, and possibly a consultant will help outline what risks will be introduced or changed.

Some aspects to consider include: Will the bank's current infrastructure support the proposed activity or will new or additional technology, such as new servers or telecommunications be required?

With respect to controls, will existing controls provide adequate security, integrity, and confidentiality of bank and customer data? Or will additional controls be needed. It is also important to determine who will implement and manage these controls going forward.

Another factor to consider is whether management has the expertise to understand and manage the risks associated with outsourcing. If not, how will you get appropriate expertise to assess risks and help you make an informed decision? All of these are important aspects that should be addressed during the risk assessment phase.

Slide #10 lists several common problems that can have significant impact on the success of your outsourcing project and ultimately to the bank's risk profile and return on investment.

Identifying risks and mitigating controls for technology outsourcing requires a clear understanding of the product and the proposed operational environment. A risk assessment should not be taken lightly and does take time to complete.

Moreover, the risk assessment should be conducted upfront. The analysis should also help frame performance criteria, reporting needs, and the basis for contract provisions. Surprisingly, we have seen many instances where management shortchanges itself by only performing limited reviews or not providing adequate resources. The financial, reputation, or operational risks resulting from poor planning can be significant.

Continuing with **Slide 11**,

Due diligence is critical to evaluating the servicer's ability to meet your bank's needs. Once you have thoroughly assessed the risks and decided to outsource, you can begin the due diligence and servicer selection process. The depth of the due diligence process will depend on the risks associated with the activity, the complexity of the operations, and how critical it is to the bank's business operations.

Many of the risk and control issues you identified in the first step, in the risk assessment, can be included in the request for proposal that you send to prospective technology service providers.

The service provider's track record in implementing and supporting similar activities can be a good indicator. You should consider contacting existing client banks or user groups. Other sources of information regarding performance are the Better Business Bureau and law enforcement agencies. You may also want to visit the candidate operations as well.

If the product, function, or technology is new to the industry or the service candidate, your evaluation efforts should focus on how well the candidates have implemented other products or technologies in the past. Additionally, you will want to get a good understanding of the candidates' risk management process and how they view the risks and controls associated with your proposed outsourcing initiative.

You should consider conducting background checks on company management officials and employees. Additionally, if the candidates you are considering rely on other parties or subcontractors, you will want to assess the adequacy of the candidate's own vendor management practices.

Due diligence considerations carry over to **Slide 12**.

You will need to thoroughly review the adequacy of the servicer's risk management process regarding internal controls, systems security, use of confidential information, contingency planning, and management reporting. To do this, you will want to look at audit reports, third party reviews, internal policies, procedures, and performance metrics.

Other aspects of the due diligence process include analyzing the financial condition of the servicer to ensure that it has the ability to meet its obligations and support the proposed activity.

Depending on the nature of the activities and the risks involved, you should require audited financial statements and perform a detailed analysis of the servicer's financial condition. This analysis should be similar to the type of credit analysis you would perform if your bank were lending to the servicer.

Another factor to consider is whether the servicer has appropriate IT insurance coverage.

The bottom line is that you need to be assured that the servicer is capable of fulfilling its obligations through the life of the arrangement.

This brings us to the contract slides. Jeff, would you like to cover this?

Certainly. Our six contract slides begin with **slide #13.** The contract is an important risk control device— it is your bank's prime opportunity to define the expectations and obligations of each party --- the contract provides the framework of how the arrangement is to work. A clearly written contract can prevent miscommunication and misunderstanding.

Slides 13 and 14 list topics you should consider when preparing written contracts with service providers. These points are fully discussed in OCC 2001-47 and the FFIEC Outsourcing Booklet. (BTW: these are two resources we recommend you use in preparing to negotiate your servicing contracts.) I will briefly discuss a few points here and then on later slides I will go into greater detail on a few select contract topics:

First, in your servicing contracts, it is very important to define the scope of the arrangement including the content, format, and frequency of the service to be provided. You'll have to be diligent in specifying what you need and what you expect, because servicers won't necessarily know. A good rule of thumb is "you get only what you ask for."

Part of scope is also the time length of the agreement. Banks should consider what is an appropriate "life-span" for the agreement, especially whether it involves an area where technology or business needs are changing rapidly.

Also, your contract should specify fees and compensation for the service provided – how much the activity will really cost – how much will you really pay. Which party will incur the costs for purchasing and updating software and equipment?

You should generally ensure that periodic internal or external audits are conducted of the servicer. In some cases, a bank may reserve the right to itself audit the servicer, or to engage an outside auditor to conduct an audit. Audit reports should include a review of the servicer's internal control environment as it relates to the service being provided to the bank. Again, "you get only what you ask for" in terms of reports and performance information from the servicer.

Consider including a clause on the servicer's responsibility for maintaining business continuity plans, including the testing of the plans.

The contract should emphasize that the bank owns the data and prohibit the use or disclosure of the bank's information except as necessary to provide the contracted services.

In **slide 14**, we provide more general topics to consider on your servicing contracts.

The contract should also define the servicer's responsibility for protecting the security of program and data files. In contracts involving access to sensitive customer data, 501(b) GLBA mandates that the bank's servicing contracts expressly address the security of this data.

As Debbie will later discuss, the contract should address the servicer's obligation to provide the bank with alerts regarding data intrusions and compromise events.

Finally, your contracts should provide that the performance of services by a third party for the bank is subject to OCC examination oversight.

OK – now lets get into some more detail on a few select topics.

The next four slides discuss in greater detail some key contract areas from an IT standpoint.

Let's start with **Slide # 15**

The first topic is data ownership. Since IT service providers rarely have a lot of physical assets, the data they hold and their software systems tend to comprise their largest value asset. If a technology service provider declares bankruptcy, this may be the only piece of the company that a trustee can use to generate value to pay off the creditors. If the contract does not specify that the data belongs to the bank, you may face unanticipated difficulties in getting control over your own information after a service provider goes into bankruptcy.

Your contract should address performance measures or benchmarks—commonly called "service level agreements" in an IT context. These are typically addendums to a contract that specify both the level of service that is expected **and** measures to provide the basis for monitoring ongoing performance. These addendums could, for example, specify acceptable ranges for response times, system availability, data integrity, and the timing of management report availability. Service Level Agreements might also address expectations updating systems and software to current technology. Service Level Agreements are an important area that is often missed, especially by community banks.

Going to **Slides 16 & 17**: Your IT contracts should also describe each party's responsibilities in certain key areas: customer complaints, intrusion detection/monitoring, security, and business continuity planning. Without defined responsibilities, it is very easy for these areas to fall through the cracks, as each party believes the other one is handling it.

As noted, if the servicer receives nonpublic personal information regarding the bank's customers, the contract must obligate the servicer to implement appropriate security measures designed to meet the objectives of the GLBA 501b guidelines with which the bank must comply.

Also, you should be clear on the servicer's and the bank's responsibilities for business continuity planning in order to provide for a smooth recovery from a disastrous event.

Your contract should clearly lay out responsibilities for providing and receiving reports and information. Reports should include a review of the servicer's internal controls, security, and business continuity programs. The contract should discuss the frequency and type of reports received, including financial and audit information, and should be sufficient to allow the bank to evaluate the performance of the servicer relative to the performance measures. You will need this information in order to assess the control environment at the service provider. If this type of information is not provided under the contract, it may be difficult for you to fulfill some of your responsibilities in the area of security over customer data.

War Story: Here's an example that illustrates what type of problems poor contracts can cause in this area. A community bank contracted with a third party to do their core processing --- signing the standard servicer contract. When examiners criticized the bank for not monitoring the servicer's financial and operational condition on a periodic basis, the bank went back to the servicer looking for current financial statements and audit reports. The servicer refused to provide this information, and since the contract did not address access to this information, there was no way for the bank to push the issue. As a result, management struggled to fulfill their responsibilities in this area.

The final specific topic I will mention are termination, penalty, and exit clauses listed on **slide 18**. It is important that the contract anticipate that the time may come when the bank needs to change to another servicer or to terminate the agreement.

Either party could go through a merger or acquisition that requires or warrants termination. What is the bank's ability to terminate for inadequate performance – will you be stuck in the relationship no matter how bad it is? What happens if your bank becomes subject to an OCC order directing rescission or termination of the contract?

Your contract should stipulate what constitutes default and/or grounds for termination of the contract. It should also identify remedies and allow opportunities to cure defaults. Look out for excessive liquidated damages clauses or termination fees.

The termination and notification requirements should provide time frames to allow for the orderly conversion to another servicer and without prohibitive expense. And, as we discussed, it should provide for the timely return of your bank's data and other bank resources.

Bob would you like to address the next area?

Thank you Jeff. I am now on **slide 19**. The fourth phase of the risk management process is the ongoing monitoring of the servicer with respect to its activities, performance, IT insurance coverage, and financial condition.

The formality of your oversight program will vary, depending on the nature of and risks associated with the outsourced activity.

Banks should establish on-going monitoring of their servicer's financial condition. To comply with its fiduciary responsibility, management should assess the financial viability of its servicer's on an annual basis. However, if monitoring indicates that the condition is declining or unstable, more frequent reviews are warranted. Analyzing the financial condition may be difficult, as service providers tend to have very different balance sheets. As mentioned earlier, the value in the company may reside in assets that are largely intangible. These may include the software they developed, the goodwill attained in a merger or consolidation, or the customer base currently under contract.

If you become aware of a servicer's deteriorating financial condition, you should initiate your contingency plan as even if that servicer remains in operation, its financial problems may jeopardize the quality of its service and possibly the integrity of the data in its possession.

Let's turn to **slide #20** to look at assessing controls.

To review controls, there are a number of potential resources. Several are listed on slide 20. Internal or external audit reports, consultant reviews, and industry certifications are some examples. User groups may also sponsor audit or other independent review activities.

For discussion purposes, an example of an independent review is SAS 70. SAS 70 reviews are typically initiated by a user group, the service provider, or by your banks management or audit group.

SAS 70 reports provide a description of the control environment at the service provider and include a review of the related policies or lack thereof. A Type II SAS 70 report includes testing of the controls and management interviews, in addition to the review of policies and procedures. Type II reports are substantially more costly and, unfortunately, service providers are not legally required to have them produced.

If a SAS70 Type I or Type II is performed, it is important to review the scope and control objectives to determine if they cover the functions or services performed for your bank. If the scope of the SAS70 doesn't relate to the services or functions you receive, the report is of little use.

Another aspect to SAS70's is that they usually include some specific controls that the provider expects the bank to implement. This information is helpful in guiding the assessment of your own corresponding internal controls.

In the network centric world of today, security testing or penetration tests can be effective ways to verify that IT controls exist and are functioning as designed.

You also have the right to request a copy of the examination report from the OCC, when applicable. However, you must keep in mind that the Report of Examination or ROE is not an audit and does not relieve the bank of the responsibility to monitor its service relationships.

You should review the scope, findings and the adequacy of the management responses to any weaknesses listed, regardless of the reporting mechanism.

Slide 21 addresses monitoring of service levels and support functions.

Service level agreements are needed to assess the quality of on-going service. They should be included as contractual requirements. Without specific metrics, it is difficult to measure service performance. Moreover, performance data should be reviewed on a regular basis to ensure the timely initiation of corrective action, when needed. The lack of specific performance criteria could limit your recourse in the event of a contractual dispute.

The servicer's performance should also be considered in terms of its ability to react to new market pressures or customer requirements. Bank could lose their competitive edge if a servicer cannot react to such pressures in an effective and timely manner.

Additionally, it is desirable to have the ability to review customer complaints. These could indicate a systemic situation that might adversely affect your bank.

You should evaluate the servicer's training commitment to its own staff and that of your bank. Poorly trained staff will have a negative impact on the servicer and bank's performance.

Let's look at **slide # 22**.

Although the board of directors may delegate performance of managerial duties to others, it has the ultimate responsibility for ensuring that the bank is run in a safe and sound manner. Effective management reports (MIS) are necessary to effectively manage the outsourcing process.

If you are to manage your service providers effectively, your oversight program should be properly documented. Proper documentation, reports to the board are one example, will include some version of the items listed on slide # 30.

The OCC expects Boards of Directors to be informed of outsourcing activities and the associated risks and controls. Also, the board should be informed as to whether the arrangement is compliant with bank policy. Documentation will vary based on the nature and volume of outsourcing.

When you are considering the outsourcing of a function or service to outsource, the analysis should be documented and include relevant material such as business plans that outline

management's strategic planning process and the service provider selection process. The analysis should also consider and document findings from the risk assessment, due diligence, requirements analysis processes, and conclude with a recommendation for the Board of Directors and, or Senior Management to consider.

For existing outsourced activities, reports or summaries that address the adequacy of service levels, internal controls, financial strength, and contract adherence will meet this requirement.

Again, Management and Board of Directors oversight activities must be documented. GLBA 501(b) requires Board's to review **a report on the** bank's Information Security program annually and as mentioned earlier today, this includes an assessment of service provider controls in relation to the safeguarding of customer information.

The Board of Directors / senior management should ensure that bank policy, regarding risk management, conforms to regulatory guidance. Independent audits or validation of key risks and controls is also required by GLBA. The scope of required reports and information will vary based on the type of outsourcing your bank is involved with.

For purposes of demonstrating compliance with GLBA 501(b), you should document your annual review of technology service providers' performance and report that to the board of directors.

Critical or high-risk activities may require quarterly or semi-annual reviews to appropriately manage the risks.

On **slide #23**, the risk management process is diagrammed. Note that this is a repeatable process, not a one-time activity.

Examiner Focus is detailed on **Slide # 24**.

Examiners will focus on and assess your risk management practices. Examiners will ask you about existing and any planned outsourcing activities. We will be looking to see if the Board of directors has implemented or has a plan to implement a comprehensive risk management program. Also, we will be looking for documentation to support the Board of Directors and senior management's actions. We expect that your risk management process will be well defined and applied consistent with the complexity and risk of the outsourced services or functions.

Aida, would you like to address the Hot Topics?

Slide #25

Yes, Bob, I will. For this presentation we selected two hot topics, which we would like to cover and they are listed on slide 25:

Foreign outsourcing

And intrusion and incident response.

Let's start with foreign outsourcing, on slide 24.

Slide #26

As we all know, banks are increasingly using foreign-based third parties. These include both foreign and domestic firms that subcontract with foreign entities or firms that have operations located offshore and which are subject to the laws of any country other than the U.S.

Use of these servicers is also a management decision. And it may be based on varied reasons; such as, an economic alternative to internal technology and data processing functions.

I must emphasize, however, that the same principles of a sound risk management process, which apply to a domestic service provider, apply to a foreign-based company although foreign outsourcing presents additional risks that the Board and you must manage appropriately.

OCC Bulletin 2002-16 and Appendix C of the recently issued FFIEC IT Handbook on Outsourcing are listed on slide 26. They describe regulatory expectations for the oversight of foreign-based servicer relationships.

One of these expectations is that your bank's relationships with foreign-based servicers must not limit OCC's ability to obtain the information needed to effectively supervise your bank's operations.

So, let's take a few minutes to discuss some of the risks you, as part of bank management, must address prior to outsourcing to foreign-based servicers. Please turn to slide 27.

Slide #27

Before entering into a cross-border contract, you should establish an appropriate risk management process that considers all of the risks associated with foreign servicers.

As listed in slide 27, these include the unique issues of country and compliance risks, which arise from the fact that the servicer is outside the US.

The Board of Directors and you are responsible for understanding and addressing the risks associated with foreign outsourcing. Furthermore, it is important that you assess these risks as well as perform due diligence prior to entering into contracts with foreign-based service providers. Additionally, as part of due diligence, you should assess the foreign servicer's culture, vision, and business style in relation to your bank.

The country risk factors you should consider include socio, economic, and political stability issues. They could adversely affect the servicer's ability to meet its contractual obligations or safeguard your customer data.

The Compliance risk factors that you should consider include the servicer's impact on your bank's ability to comply with foreign and US laws such as OFAC's sanctions and embargo provisions. Also, you must consider your ability to enforce the contract.

From a legal point of view, you should ensure that all legal and regulatory requirements of the bank could be met. It is possible that foreign laws may not be favorable to your bank in a dispute situation. Weaknesses in these areas could result in significant reputation risk to your bank.

Slide #28

With regards to Operational risks, mentioned on slide 28, you should ensure that bank and customer information ownership and accessibility is carefully considered.

Your ability to monitor and control overseas operations are critical and can be more of a challenge when dealing with foreign servicers than with domestic servicers.

For example, coordinating tests and results of your and the servicer's tests for business continuity and disaster recovery plans could be quite difficult.

Slide #29

Slide 29 highlights contract and monitoring considerations unique to foreign outsourcing.

These are in addition to those that Jeff discussed earlier during the Contracts segment of this teleconference.

Your contracts with a foreign-based service provider should address the legal question of jurisdiction and choice of law.

Your contract should also address the privacy and security obligations required by U.S. law, regardless of any conflicts with "local law."

Issues relating to ownership of bank and customer information must be thoroughly understood and appropriately addressed.

Performance and service quality information requirements must be articulated in your contract, as should the criteria for terminating the relationship should problems surface.

Finally, the authority of the OCC, as the U.S. regulator, to examine the performance of services provided by the foreign-based servicer should be explicitly stated.

Slide # 30

Your activities for monitoring the foreign-based servicers are included in slide 30.

Your oversight should be comprehensive and should address the servicer's financial condition, performance, and control environment.

An issue that you should consider, for example, is the fact that financial data provided by a foreign company may not be typical of information received from a U.S. based firm.

The quality of the data should be based on your standards to meet your effective operations and ensure your regulatory compliance.

You should consider whether geographical and time zone difference might impact the services to be provided. For example, geographic considerations should include the cost of travel to perform on-site reviews or to monitor the servicer's corrective actions. Time zones also may raise the levels of risk if time translations are not clearly specified in all aspects of the contractual relationship.

Slide #31

As stated in slide 31, the OCC's primary supervisory concern in relation to foreign-based outsourcing is whether your bank is adequately dealing with the special risks of the relationship.

The OCC will conduct reviews to assess whether your bank develops and implements a comprehensive risk management process to oversee foreign outsourcing.

To facilitate such reviews, access to the information is key. The information should be in English and should be available in a US office of your bank.

The OCC may seek information through the appropriate supervisory agency in the servicer's home country, if one exists. However, if circumstances warrant, OCC may exercise its authority to examine services performed by foreign-based service providers.

The other hot topic we selected for today is intrusion and incident response. And Debbie, will talk about it.

Thanks Aida. For this hot topic, we turn to **slide #32**.

Last August, the FFIEC agencies published for comment a proposed Interagency Guidance on Response Programs for Unauthorized Access to Customer Information. This guidance is intended to be a binding interpretation of section 501(b) of the GLBA and the associated guidelines. The agencies are in the final stages of considering the comments and final guidance should be issued soon.

As proposed, the Guidance will require every financial institution to have a response program to address any incident that results in the unauthorized disclosure, misuse, alteration, or destruction of "sensitive customer information."

The bank's response program will need to address compromises of bank customer data that occur at a bank's service provider as well as at the bank itself. Thus, banks need to plan how they will deal with events at their service providers that result in the compromise of bank or customer data.

The response program should be a key part of your bank's information security program. The program should be intended to help management to act quickly to incidents. The critical steps are listed on **slide 33**.

For assessing the situation, you should work with your service provider to determine the nature and scope of the incident and identify information systems and types of customer affected.

You should notify the OCC and appropriate law enforcement agencies of the compromise regardless of whether it occurs at the bank or at the service provider. A SAR or Suspicious Activity Report should be filed.

You should take appropriate measures to contain and control the incident to prevent further unauthorized access to or use of customer information, while also preserving records for forensics. Actions may include including shutting down particular applications or third party connections, reconfiguring your firewalls, changing computer access codes and modifying as needed physical access controls.

Once you understand the scope of the breach and have taken steps to control the unauthorized access, you need to make sure that both the service provider and you can take corrective measures to mitigate the impact.

Examples outlined in the proposed guidance include flagging accounts –for those accounts identified as compromised. You would monitor those accounts for unusual activity, and implement controls to prevent the unauthorized withdrawal or transfer of funds from customer accounts.

Additionally, when affected customers have other related accounts that use the same account number, PIN, or password, all accounts should be secured until such time as the bank and the customer agree on a course of action.

Finally, in appropriate cases, the bank should notify the affected customers so that they can take appropriate action to reduce their exposure to identity theft and other injuries.

On **slide 34**, we focus on the implications of the proposed guidance for service provider contracts.

Banking Bulletin 2001-47 advises bankers that service contracts should require service providers to notify client banks of any security breaches that result in unauthorized access to bank or customer information.

The proposed guidance would also mandate that servicer contracts have language requiring the service provider to fully disclose to the bank, information related to any breach in security at the servicer resulting in an unauthorized intrusion into the bank's customer information systems. This communication to the bank will enable the bank to quickly implement its own incident response program.

Finally, the proposed guidance stated that under its contractual obligations, the service provider should be required to take appropriate actions to address incidents of unauthorized access to or use of the financial institution's customer information to enable the institution to expeditiously implement its response program.

Aida, would you recap the presentation?

Slides #35 and 36:

I will be glad to, Debbie.

Slides 35 and 36 highlight what we covered today:

We stated several times that outsourcing **IS** a management decision. It can be a viable business practice **if** it meets your bank's strategic objectives and **if** you manage appropriately the related risks.

The Board of directors has the ultimate responsibility for ensuring that the outsourcing relationship is managed in a safe and sound manner.

The risk management process should be commensurate with the risks posed by the contractual arrangement and your ability to oversee the activity.

Outsourcing is subject to the same risk management, privacy, security, and consumer protection requirements that would be expected if your bank where conducting the activities internally.

Outsourcing to affiliated entities should be structured similarly to outsourcing to non-affiliated entities in terms of assessing risk, due diligence, pricing, contract, and ongoing monitoring.

The same principles of a sound risk management process for outsourcing to domestic companies apply to foreign-based third party services, with additional considerations of the controls necessary to mitigate the unique risks related to cross-border outsourcing, of course. And, as far as unauthorized access to your data is concerned, you need to review your information security program to ensure you have an adequate response program that includes customer notice.

Slide# 37:

As we invite you on slide 37, should you find after this presentation that you have questions regarding outsourcing, please contact your portfolio manager, Assistant Deputy Comptroller or Large Bank Examiner-in-Charge.

Slide 37 also includes the OCC website where you can find links to all the guidance we mentioned in this presentation, and then some.

Now, we would like to begin the question and answer segment of this teleconference.

Thank you, once again, for having made the time to join us today.

Question and Answer Segment

Now we would like to begin the question and answer segment of this teleconference.

Aida: Jack, I am turning it over to you for the response to the polling questions.

Jack: Aida, thank you very much. Exactly what I have is the results of the polling questions we started our program with, and you might be interested to know that there are a minimum of 407 listeners out there in 143 locations all across the country.

At this time now if you would like to ask a question or have a comment, all you have to do is press the star key and then the 1 on your phones touch tone keypad. This will put you into our phone cue, and then when your turn comes up, I will call on you by city and the first name of the person who registered at your location. If your question is answered when you are in line, pressing the pound sign will take you back out of the queue. I would like to encourage you take advantage of this interactive format to talk with our panel and have your questions or concerns addressed. Please ask only one question at a time and if you have additional questions, please re-queue by pressing star 1.

A couple of other tips: If you are listening in on a speakerphone, if it is at all possible, please pick up the handset when you ask your question. We will all be able to hear you much better that way, and when replacing the handset, remember to press and hold the speakerphone button so you are not disconnected. However, if that should happen for that or any other reason, just dial back in, reenter your pin number, and you will be immediately reconnected to the program. So, if you have a question, go ahead and press star 1 now. And, again, if your question is answered we will in line and pressing the pound sign will take you back out of the queue. Finally, for those of you who have joined us a bit late on the Internet, you can also send us a question by your Internet connection. To do so, just go to the Q&A panel on the lower right portion of your screen, type in the question where indicated and click on the Ask button. Your question will reappear on the box above and only you and the panelist will see the question. Please leave the destination of the question set on host presenter panelist.

I have three questions in the queue to get us started. Los Angeles, San Francisco and Washington, DC.

Jack: Los Angeles you are up first at Jackie's location. Go ahead please.

Jackie: Several of my vendors are law firms, and I wanted to know what type of confidentiality statements are required from law firms and should it be included in a retention letter between a law firm and my bank? Or should it be assumed under attorney client privileges?

Jeff: Jackie, Hi. This is Jeff Gillespie.

Law firms are sort of a special exception because of this long-standing ethical rule of the legal profession regarding client confidentiality. Generally, under section 501b of GLBA, you do not

need to include anything in your company's contract with its law firm to address the security of customer information.

Jack: Los Angeles, thank you for joining us. Next we go to San Francisco in Celene's location. Go ahead please.

Dave: Hi. My name is Dave and I have a question.
You guys talked about the report of the examination that the OCC performs on the service providers. Typically from whom should we request that report? Should we request the results of that report from the vendor or do we need to go back to the OCC?

Aida: Thank you for your question. This is Aida. You should ask for the copy of the report from your Supervisory Office. They will channel the request either through the district office or to our office at headquarters. I would like to take the opportunity to answer another question that is related, too. What if we ask the OCC for a copy of the FFIEC report on the company we use and OCC declines? This seems to contradict what you said today. Can you elaborate or explain?

First of all an institution is entitled to a copy of the report of the servicer if it has a contractual obligation relationship with it. If the bank has not entered into a contract with the servicer, it is not entitled to receive a copy of the report of exams. If, in your situation, the bank had a contract and you could not get a copy, I would appreciate your sending your request directly to me and I will look into it to make sure you will receive the report, which you are entitled to.

Jack: Aida, thank you very much. We have one remaining question in the phone queue right now so there is plenty of time and plenty of room for you. All you have to do is press Star 1.

Washington, DC: Go ahead please.
Hello. My question is what responsibility do we have to provide references to other financial institutions regarding a particular vendor's performance?

Jeff: This is Jeff Gillespie. You have no responsibility to do that. You can be a member of a user group but that is completely voluntarily on your part. There is no legal obligation to provide references.

Jack: Washington, thank you for joining us. That clears out the phone queue for right now. So, Star 1 will get you back in there to talk to our panel. In the meantime let me go back to Aida. Lamont, Illinois just queued in. We will get to you in just a minute. Aida, let me come back to you for one or two Internet questions.

Aida: Alright. One of the Internet questions is: Under what circumstances would OCC issue an order for a bank to terminate a contract? I will ask Jeff to address it.

Jeff: OCC has the authority, under12 USC 1818, to issue what is known as a recession order. That is an extraordinary remedy; generally we only issue them in situations where the relationship essentially is unsafe and unsound and cannot otherwise be dealt with. When we ask banks to put provisions in their contracts to address our orders to rescind a contract, that would

generally only be triggered in a situation where the OCC issued a cease and desist order with the recession clause under 12 USC 1818.

Aida: Thanks, Jeff. I will ask a question of Bob, since he addressed SAS 70. Could you read that question please?

Bob: Sure. We have a question from the Internet.

Bob: Some of our third-party vendors do not have SAS 70. In this case, what can we do? There are various options available to banks that find themselves in this situation. However, it is also dependent upon the cooperation of the vendors that you are doing business with. Certainly their internal audit reports, independent reviews of their operations by other firms if they will make those available to you, they can be useful in your assessment. If you have internal expertise, whether it be audit or IT-related, you can request to do an onsite visit, do your own interviews, and attempt to make your own assessment in that matter.

Jack: Very good, Bob. We have three questions in the phone queue. Now we go to Lamont, Illinois in Gregory's location. Go ahead please.

Lamont: Hi. Is Illinois on?

Jack: Yes, you are.

Lamont: We have a problem when we negotiate a contract with several of the major data processors. They have a boilerplate contract, and they are very reluctant to change anything in the boilerplate contract--especially, in the areas of liability in the event of negligence or dishonesty. The only damages that they agreed to be liable for are two or three months of data processing services. And yet the liability—the damages—could be in the hundreds of thousands if not millions of dollars if they refuse to provide a fidelity bond or any other type of insurance. Their answer is: "If you don't like it go to another data processor." I am wondering if other banks have had the same situation and if there is something that the OCC can do to put some pressure on data processors to be able to get some insurance coverage in this regard? Also, termination of contracts is a very serious issue. Most of the data processors want 80 percent of the remaining life of the contract on a declining scale. It is a very onerous provision if you decide that you want to terminate the contract because of improper service or their inability to meet regulatory requirements. In fact the contracts do not offer any type of warranty that the services they provide meet regulatory requirements. Maybe you can give us some advice as to how we can proceed in this area?

Jeff: Gregory, this is Jeff Gillespie and I think you have raised a very important issue. The disparity of bargaining power particularly between community banks and the large service providers, is one of the main reasons we put out the guidance; we wanted to provide additional negotiating leverage for you. OCC essentially has a four-step process for vendor management. It is assessment, risk assessment, due diligence, and contract negotiations. Basically, what we would like you to do is what you have done already--which is even before you start shopping, put together a list of the important points you are looking for with your risk assessment. The

second step is due diligence. We suggest that even before you start identifying the service providers you have identified, you should do due diligence and find out their position on the important issues. I understand there is really not much chance that you will be able to go to a major service provider and get them to change their boilerplate. But you can find out in advance what their boilerplate is. User groups are particularly useful there. Also some trade associations can give you some help with that. So, by identifying which providers have contracts that are most likely to meet your needs, you will know that going into the process. If you and the other small banks do that, ultimately the market will put pressure on the large service providers to provide the type of contracts that we need.

Jack: Back to the phones for questions. Christine Berg in Virginia is up next and then we will go to Glen Falls, New York and San Francisco.

Jack: Christine Berg in Mary's location, go ahead.

Christine: OK. What control do banks have if their servicer provider is purchased by a foreign company, and should there be something in the contract in regard to that?

Jeff: This is Jeff Gillespie. Remember we talked earlier about termination clauses and what would be grounds for termination? The acquisition of a company of the merger of a service provider could be specified in advance as grounds for termination. Additionally, if an overseas company acquires your service provider, then you may find that, if the services are being performed predominately overseas, the guidance on overseas outsourcing would apply, and you would begin to have to analyze and monitor that relationship in accord with that guidance. You're stuck with your existing contract unless you have a termination clause in there, but you should start deciding whether or not you want to remain with that service provider and begin to prepare to either transition away or to renegotiate the agreement so that it takes into account the additional risks that you are subject to.

Jack: And before we go to Glen Falls. New York, Aida, let me come back to you for another Internet question.

Aida: OK. Thank you, Jack. Bob, do you want take this one?

Bob: Sure, I have an Internet question. Would a servicer's audit report be similar to SAS 70?

Bob: The answer to this question is it would depend on the scope of the internal auditor's report. If it were an IT focused report on controls, then, yes, it would be highly similar to a SAS 70, and the results would be similar. In either case, what you would be looking for would be the issues that were to be identified and the management responses to those issues.

Jack: Alright, very well, we go to Glen Falls, New York in Peter's location. Go ahead please.

Glen Falls: Yes, Hi. This is Kathleen. The question is: Is there a process in place for reporting service providers to the FFIEC when we have identified a significant information security vulnerability and that company is audited by the FFIEC?

Aida: Yes, there is. This is Aida by the way. Your first point of contact is your Supervisory Office. Whether there is a senior in charge or whether there is an ADC, Associate Deputy Comptroller, who supervises your bank. Please contact them immediately, give them the facts, and they will take it from there.

Jack: Glen Falls, thank you for joining us today. San Francisco, we go back there for Celene's location. Go ahead please.

San Francisco: The question is: What is our responsibility to notify service providers, particularly in the contract, of the fact that they will be subject to OCC regulations and possible inspection, and are we required to notify them of that fact or is it merely the fact that they entered into a contract with us that puts them under regulatory review?

Jeff: Good question. This is Jeff Gillespie.
There is no legal requirement that you do so, but we strongly urge you to do so for three reasons: First, it makes our life easier. If the service providers know in advance that we will be knocking on the door, they are less likely to resist when we show up. Second, if you have this in your contract, it gives you a hook to compel them to cooperate with us and if they fail to do so, you can get out of the contract. Third, it is a quality control device. The good service providers --the experienced providers—know this in advance and are not afraid of it. The people who would resist on grounds that they would be subject to regulatory oversight—that's a red flag. So by bringing it up as part of the contract negotiation it's like a quality control device.

Jack: Jeff, thank you very much. Before we return to Illinois for our remaining phone question at this point, Aida, let me come back to you and let's do two of the Internet questions.

Aida: OK. Jeff, do you want to take the one you have? And then I will have another one.

Jeff: Yes. One listener asks: What is considered to be "adequate" IT insurance coverage for ongoing service providers. I will give you the lawyer's answer: It depends. It really depends on the risk exposure of the relationship in part. How much damage would the bank incur in the event that something happens and the service provider is liable? If the provider is a small company, there should be sufficient coverage so that the bank's risk is covered and is not dependent on the solvency of the service provider. On the other hand, a huge service provider is in a position where it can self-insure, and the issue of insurance becomes less important. So you should recognize that as part of your due diligence. You should know whether or not you are dealing with a service provider who has sufficient financial footings, then you really don't have to worry about insurance.

Jack: Thank you very much. Another Internet question, Aida.

Aida: Yes, thank you, Jack. Earlier I talked about the requests for the reports. I responded that the Supervisory Office is the point of contact, where you can obtain and clarify that a bank that has not entered into a contract with a servicer may not obtain a copy of the report of examination. The question is: Isn't Aida's response contradictory to the process? How can you

conduct due diligence on a potential provider, if you can't get an OCC exam report on a potential vendor?

The OCC's reports are not intended to be the 'Good Housekeeping Seal of Approval.' They are reporting a point-in-time examination of the performance of the servicer. They provide those who have contracted with the servicer with a condition report of how that is being accomplished. It will not address competitive areas nor any other information that you may be interested in obtaining when you are looking for a servicer in your due diligence process. Once you have entered into a contract, statutory requirement 1867 gives us the authority to examine the servicer. Then you will be entitled to a report. There are other ways for a bank to obtain information on a servicer, including visiting the servicer, communicating with the user groups, and getting referral information. The OCC report, or any of the other FFIEC agencies' reports of examination, are not intended to facilitate the due diligence in terms of shopping for a vendor. I hope that is responsive.

Jack: Very good. With 13 minutes remaining for questions, we return to Lamont, Illinois in Gregory's location. Go ahead please.

Lamont: Yes, I just want to follow-up. You mentioned that we should do our due diligence with different processors before we start negotiating with them. And that is exactly what we have done. We looked at the contracts from a number of large data processors, and we are due to review their contracts. They are very one-sided, and they are virtually identical in all major respects. There is not much difference between one data processor's contract than another's. The issue of insurance is of no avail, and the size of the data processor does not help us because they have us holding them harmless for any error that they may commit or negligence, unless it is a gross negligence. So, in order for your guidelines to be of any assistance to the big banks, we will have to have the thousand pound gorilla get into this game and urge or use our persuasive powers to convince their processors to negotiate in good faith and that is the OCC, the OTS, and other regulatory agencies. Please give me your comments on that. Because the negotiating power of the community bank is very, very minimal.

Jeff: Gregory: Hi. This is Jeff again and I appreciate your dilemma. I'd like to have some off-line discussion with you on this. If you could send me an email. I'll be in touch with you. I think my contact information is james.gillespie@occ.treas.gov

Jack: Lamont, Illinois, thank you very much. That clears out the phone queue, and Aida let me come back to you and see what we have for Internet questions.

Aida: Bob has another question, and he will take it.

Bob: I do have an Internet question. The question is: What is the OCC's guidance for outsourcing of remote 24/7 network security monitoring? I am not sure I understand the question. From one perspective, the OCC would certainly encourage all banks engaged in any form of networking to have a 24/7 network security monitoring. If that service is outsourced, and it frequently is, because it can be resource intensive it can be a very costly endeavor. Some of these firms have developed mechanisms and things that they can operate much cheaper than

an individual bank or even a group of banks. I think the key factors that you would be looking for are the completeness of the service. In other words, what are they monitoring, what are they not monitoring and then your ability to respond to whatever information they would provide you if there was a breach of your network. I think those are the key factors.

Jack: And with no questions within the phone queues at this time, let's keep up with the Internet questions that are coming in. Aida.

Aida: Debbie has one she will take.

Debbie: OK. The Internet question is: We are facing the decision of either hiring a full-time network administrator or outsourcing to a third party. We are a $240 million in assets with seven branches. What do you see other institutions our size doing?

Well, I see it both ways. Quite frankly I see a $240 million network administrator in-house. I also see it being outsourced to a third party. Again it comes down to what you have available in your area for an individual with expertise and a back up, and what is the cost to outsource? That is what I would suggest. It could go either way, but you need to take a look at what is available to you.

Aida: Thanks Debbie. Another Internet question says: If the OCC were to become aware of a safety and soundness issue with a vendor, would they contact banks known to use that vendor?

Yes, we have a process for investigating issues that are raised to us about a servicer. We will contact the servicer and, if necessary, will visit the servicer to obtain relevant information. We would communicate, through our Supervisory Offices, the issue to our examiners. Either we would ask that our examiners to contact the bank directly, or if necessary and if the situation is serious enough, we would contact the bank directly. In past situations, we have had servicers put under enforcement actions for different situations, such as declining financial conditions. We expect our banks to monitor the conditions of their servicer(s) on an ongoing basis and expect them to be aware of serious issues. As conditions warrant, we may ask the banks to start activating their contingency plans. I hope that answers that question.

Jack: Very good. Thank you. With eight minutes remaining the phone queue is still remaining empty. All you have to do is press star 1 and we can bring you right into the conversation. So, if you have a question or comment, don't hesitate. In the meantime, Aida back to the Internet.

Aida: Jeff has one question, and he will take it.

Jeff: The question is: Will the OCC review a contract prior to the bank entering into the contract to determine if it is adequate?
The answer is: No, we will not. Because we really cannot be in the business of usurping the position of management, and it is really management's responsibility to decide the basis of upon which they will enter into contracts. We will be happy to talk with the bank in advance about general issues, but the idea that we would actually look at a contract and sign on the dotted line with the bank, so to speak is beyond the proper role of the OCC.

Jack: Aida, any additional Internet questions there?

Aida: Yes.

Aida: Bob.

Bob: We have a question that states: You mentioned that the term of the servicing agreement is an item looked at by the examiners. The question is: What term would be questioned by an examiner? What is too long? What is too short?

That is a difficult question to answer, because without knowing all of the surrounding terms and conditions and clauses within the contract, it is difficult to assess. Generally, what are probably more important than length of contract are the provisions that Jeff talked about in his presentation, including the monitoring of the service agreement, the ability to terminate the agreement, and so forth. Generally speaking, agreements of two to three years are fairly common. I am sure that less than that would be probably some sort of transitional arrangement. But it is difficult, and I don't think the OCC would have a specific recommendation on a specific term for a servicing agreement.

Jeff: And Bob, let me add to that. I agree. The FFIEC outsourcing guidance has a footnote in the contract issue section that specifically addresses this issue. The point that we make is that the longer the term of the contract, the more flexibility you have to build into the contract, so that if things change, you can modify the contract or get out of it. As Bob pointed out, the acceptable term depends in part on the nature of the contract, what it is covering, how fast the technology and business needs are changing.

Jack: Gentlemen, thank you both very much. With four minutes remaining for questions, Fort Lauderdale, Florida is on the phone queue. We go there as Theresa's location. Go ahead please.

Fort Lauderdale: Yes, thank you. Our bank has a third-party vendor who supports our network and provides 24/7 monitoring capability. We had an independent company come in and do an intrusion test and a security assessment of that network. This independent company that performed this intrusion test wants to provide ongoing support and monitoring of the firewall. Our feeling is that that would not allow them to be independent enough to continue to do periodic intrusion tests, but they claim that that would not be that kind of conflict of interest, and I wonder what your thoughts on that might be?

Debbie: Well, this is Debbie speaking, and it does not appear that you are getting an independent assessment, if they are the ones who are configuring the firewall, and they are the ones who are doing the penetration testing. I don't see how you would have the independence.

Fort Lauderdale: Yes. I agree with that. Their comments were that they were doing this for 200 max and have never been cited by the examiners.

Debbie: That is not a guarantee of security.

Fort Lauderdale: I agree. I am glad to hear you say that.

Jack: Fort Lauderdale, thank you for joining us. That clears out the phone queue. And with two and one-half minutes remaining for questions, let me go back to Aida. Aida, are there any additional Internet questions that we need to cover?

Aida: Yes. The question is: When do you expect the final guidelines for the incident response program?

We have come to about a 99 percent conclusion of what we want to recommend to senior management in terms of the final guidance. We have taken into consideration all of the comments submitted by the industry and by community groups. We should, this month, be finalizing at the staff level, and then we have to follow up our process for a review by senior management and the principals. So hopefully, keeping our fingers crossed, we estimate that by September we should be issuing the final rule.

Jack: Alright, very good. We have about two and one-half minutes remaining here. Are there any more questions we can take care of or is it time to wrap up?

Aida: I do have one more question we can take. The question says: During negotiations, some servicers have been telling banks that GLBA does not apply to servicers. Are they correct? How should banks deal with this so they can comply with the 501(b) guidelines?

Jeff: The fact is that the FTC recently issued a rule implementing section 501(b) that has a very interesting provision in it. It basically makes service providers for banks subject to the FTC's 501(b) rule. Which is, although more general than the banking regulators' 501(b) guidelines, intended to be essentially the same. So, service providers are now subject to section 501(b) in terms of their requirement to have security programs that are effective to achieve the section 501(b)'s security standards. So when the bank pushes for a security provision in the contract, the provider should not be pushing back on the grounds that they are not subject to section 501(b).

Jack: I will go to Aida and our panel for our first few Internet questions.

Aida: Thank you, Jack. We do have an Internet question, and I will turn it over to Jeff.

Jeff: Yes, the listener asks: Could you please repeat where the contract points are detailed?

There are really three places. One is in OCC Bulletin 2001-47, which discusses service provider relationships. There is also a very recently released FFIEC IT Handbook on outsourcing. You can find that on the FFIEC Web site: www.ffiec.gov we will have it on our Web site eventually. The last is the Overseas Service Provider Bulletin that the OCC issued, 2002-16.

Jack: Jeff, thank you for getting us started with our first question. We now have one question in the caller queue. Lake Jackson, Texas. Sherry's location. Go ahead please.

Texas: Yes. We were wondering if it has ever been considered to have a certified vendor list?

Aida: Thank you. This is Aida and I will take that question.
If you are referring to the FFIEC agencies providing a public list of the servicers that we examine, that item is currently under discussion at the interagency level, but it has previously not been approved for publication.

Jack: Lake Jackson, thank you for the question. Aida back to you and the Internet questions.

Aida: Thank you. We have one that Bob will address.

Bob: The Internet question is: Some of my third-party vendors do not have the SAS 70 Report. In this case, what can we do?

Well, SAS 70 is an industry re-certification document. There are many other methods and means to perform an assessment of your vendor. If you have expertise in house yourself, you can perform the assessment. That may be as part of a site visit and as part of answering questions based upon some of the guidance that we have informed you about today. Certainly, you can review its internal audit reports, particularly if it relates to the IT function and the controls therein. And last but not least, you can hire a consultant to perform the review for you.

Aida: Thank you Bob. Jack, do we have a question over there?

Jack: Not at this time. Let's continue with what you have there.

Aida: Okay. We have a question: In the event of a security breach of a service provider, who is responsible to file the Suspicious Activity Report (SAR)? The national banks are the ones who have the obligation to file the SAR, so they need to obtain all of the information from the servicer to complete the form and submit it.

Aida: There is another question that Jeff can answer.

Jeff: The question is: If there is already a service agreement that complies with all the aspects of the requirements outlined today, except the mandate that the service provider notify the bank of an intrusion, what leverage can a bank apply to require the service provider to agree to add it? I would suggest that your contract probably already has a regulatory requirements clause in it. And, you can use that clause, because you can point to the provision in 2001-47, which says that the service provider should notify the bank of the intrusion. Second, when the interagency intrusion response guidance comes out, I expect it will incorporate such a requirement under the 501(b) guidelines. So, again, that would trigger the regulatory requirements clause. I hope that is responsive.

Aida: Thank you. We will continue with another Internet question.

Debbie: Yes. The Internet question I have is: What process or procedure should or can a bank use to do a background check on a perspective or a current outsourcing provider and its management?

As we talked about in the discussion, if it is a service provider, you should be able to talk to other banks and people within a user group. As far as background on the company, you can get information from Dunn and Bradstreet, Moody's, Standard & Poor's or you can do a credit report on the business. As we indicated, you cannot get regulatory reports until after you have signed a contract. We also talked about law enforcement agencies. Lexus Nexus would be another source for getting information on the background check on a business or persons within that business.

Aida: There is another Internet question that I will try and answer. Can service providers provide copies of regulator examination reports or must the banks request these reports directory from the regulator?

The report of examinations are confidential property of the FFIEC agencies. They should not be disclosed by the service provider. Banks that are interested in obtaining a copy should contact their primary regulator and go through their Supervisory Office. This would be the best approach to get the report.

Jack: Aida, thank you very much. We will go to New York City and Kathleen's location.

New York: My question deals with the foreign outsourcers. We know there are all these special risks because of the fact that they are indeed not in the U.S. We were wondering, when you were talking just a few minutes ago, about the background checks on the potential outsourcer what you can do. Some of those alternatives might not be available in a foreign country, such as law enforcement or other checks. What would you suggest? Do you have any suggestions for vetting any potential foreign outsourcers?

Aida: Thank you for that question. I know that some countries are trying to establish processes similar to what we have. They might not have them to the extent that we have but, for example, in India, their Chamber of Commerce (NASCO) is in the process of developing information on the technology service provider employees, such that they can meet the needs of a United States background check wherever it is possible. There may be other countries making similar efforts with which I am not totally familiar, but nevertheless, through the central banks or other regulatory entities that exist overseas, information could be obtained by the process which they use internally to validate the background of a person.

Jack: Thank you Aida. Back to the Internet for whatever you have there.

Aida: Thank you. Jeff will take another question.

Jeff: I actually have two related questions. They relate to what type of entities are considered to be service providers for the purposes of today's presentation.

One person asks: Are correspondent banks covered?

Another asks whether or not it includes an ATM network that provides switching of transactions.

The guidance that we are providing on outsourcing actually can cover a wide range of third-party relationships where the bank is having services performed for them that they would otherwise have to do for themselves. In fact, if you look at the general guidance in 2001-47, that speaks very broadly of "third-party relationships." So, the type of advice that you find in those issuances, and also in today's presentation, would apply to correspondent banks and to a provision of switching services by ATM networks. I hope that is responsive.

Aida: There is another Internet question that Bob will take.

Bob: This Internet question is: At what point does a bank require a vendor to obtain SAS 70 report?

Well, the SAS 70 report is talking about the control environment of the service provider. As part of your risk analysis, risk assessment, and due diligence process, you would need that information up front prior to the contract to make an effective risk-based decision. In terms of SAS 70 or other audit reports or review reports, ideally reports should be available prior to the contract negotiation phase.

Jack: Bob, thank you very much. We have one more question in the phone queue from Charlotte, North Carolina. Edmond's location. Go ahead Charlotte.

Charlotte: Thank you. When we have a relationship with a domestic partner, and they choose to send the work offshore, but still within the same company-it is not being reassigned, are there any regulatory constraints to that? We are not actually going to an off-shore outsourcing partner we have our domestic partner, they have just within the confines of their own business moved it over to one of their other facilities. How is that addressed?

Jeff: This is Jeff Gillespie. If you look at the OCC Overseas Outsourcing Guidance 2002-16, there is a footnote there that basically says that the guidance applies not only to companies that are located overseas, but also to domestic companies to the extent that they themselves outsource the activity to a firm that is located overseas. Basically, what we are saying, is that the types of risk analyses and risk controls that one would apply to a purely overseas service provider should also be considered for a domestic provider who does a considerable amount of overseas outsourcing. Is that responsive?

Charlotte: What you are saying is: If I own a company and I had a factory here and a factory in Spain, the same company, the same employees, and we just moved the work from here to there that is considered outsourcing. Well, it is a reassignment of work?

Jeff: Let me ask you a question? Are we talking about where the bank owns an overseas facility? Or, are we talking about a third-party service provider that is domestic but also has overseas operations?

Charlotte: The latter.

Jeff: The latter. Okay. Then my answer stands.

Charlotte: Thank you.

Jack: Thank you very much. Back to Aida.

Aida: I have a question. If the OCC were to become aware of the safety and soundness issues with a vendor, would they actively contact banks known to use that vendor?
And the answer is yes. First of all, we would investigate the situation that has been reported to us as part of our portfolio management responsibility, more than likely onsite at the servicer. Depending upon the seriousness of the situation we would notify our banks through the Supervisory Offices. We will communicate with the other agencies, too, so that they can inform their regulated institutions. There have been situations in the past when we may have had formal actions against service providers primarily because of financial situations that hinder their ability to perform under contract. In those situations we have contacted the banks directly and required them to work on their contingency plans. So, the answer is: Yes we would.

Aida: I have another question I will ask Debbie to address.

During negotiations, some servicers have been telling banks that GLBA does not apply to the services. Are they correct? How should banks deal with this so that they comply with the 501(b) guidelines?

Debbie: This question came up yesterday as well – whether GLBA applies to service providers. The Federal Trade Committee has recently established a regulation that indicates that service providers have responsibilities for safeguarding customer information that is basically the same as GLBA. So under the Federal Trade Commission when the service providers would fall under that jurisdiction, it does apply, so it is basically the same thing.
Aida: Thanks Debbie.

Jeff: An Internet question. What is Lexus Nexus?

Lexus Nexus is a commercial database that is available for on-line searches. The Lexus database is essentially legal components. It has judicial cases, regulatory materials, law review articles -- that sort of thing. All subject to keyword-in-context searches. Nexus is a broader database of commercial data including the 10Ks, business journals, and some academic business journals. It is an extremely expansive database.

Jeff: Another Internet question. If we are using the same third-party service providers as our affiliated company, and we are also using our affiliated company to do some of our IT processing, would you please address the role of our affiliated company?

Basically, if you are receiving services from an affiliate, the standards that we would apply are similar--identical really-- to the nonaffiliated service provider. The 501(b) guidelines on security certainly do apply to affiliated entities. 2001-47 also applies to affiliated entities. But there is also a special requirement that applies to affiliate relationships under the sections 23(a) and 23(b) of the Federal Reserve Act. Specifically, it says that transactions with an affiliate must be on terms and circumstances that are substantially the same, or at least as favorable to the bank, as those prevailing at the time for comparable transactions with or involving non-affiliated companies. So, if you are receiving services from an affiliate, you should make sure that your contract and other terms are at least as favorable to the bank as what you would get on the open marketplace.

The other question is: Can you rely upon an affiliate to oversee or monitor the services that your bank is obtaining?

The basic answer is to some extent you can. But, your management is still required to oversee the overseers. You want to make sure that the holding company or the affiliate is doing the same sort of monitoring and control that we would expect if the bank were overseeing the relationship directly. That was a long answer but I hope it was responsive.

Bob: I have another Internet question. This one relates to the length of contract. The question is: You mentioned that examiners would look at the length and terms of the contract. What would be too long? What would be too short?

From an OCC perspective there is no specific answer to that question. The term of the contract would be or should be consistent with your business plan, with your strategic objectives, and so forth. Clearly a contract that exceeds three, four, five or six years in a dynamic technology world could create problems in terms of responding to new technology and new product delivery. The basic answer is: It should be consistent with your business plan and your objectives.

Jack: Newark, Delaware just queued in Scott's location. Go ahead.

Newark: I am trying to get a little further clarification on what service providers would be applicable. There are a lot of industry-wide vendors out there--electronic activity networks, CCN, the exchanges, and the Swift. Do you have different expectations for them or would they fit within the requirements that you have defined here?

Jeff: We intentionally give broad guidance. What is key is that the guidance starts with the risk analysis. So, I invite you to look at the specific relationship: what service is being provided and what risks you can identify based on that relationship. Then look at the guidance to determine which risk controls described in the guidance are appropriate to apply to that relationship. For example: you might have a snow removal service. Very few of the risks we have identified in 2001-47 will ever apply to that. But, on the other hand, a switching or image exchange network clearly gives rise to some of the risks, but not necessarily all of them. So our approach here is not rigid. It is more that we invite you to look at the specific risks that are in the relationship and then manage those risks, and we try to provide some suggestions in terms of how that might be done.

Jack: Newark, did that help?

Newark: Just a quick follow-up. When you answered the related question, you talked about services that you would or could provide yourself. I am just trying to get a sense of how that would play in there?

Jeff: Sure. There are really two questions. Not to get overly legalistic here. One is: What relationships does the OCC and the FFIEC Outsourcing guidance apply to? The sort of risk-oriented answer I gave you is addressed to that.
The second question is a narrower, legal question about what sort of relationships are subject to our examination and supervision authority under the Bank Service Company Act, that is 12 USC 1867(c) which gives us the authority to examine and regulate the performance of "services." And generally, 1867(c) applies to the type of services that the bank would or could provide for itself. So I am really addressing two different questions. And you are right to call me on the fact that I wasn't totally clear about that.

Jack: Newark, thanks for your question. Jeff thanks for your response. Aida back to you.

Aida: I will ask a question to which I would like Jeff to respond. Some of the servicers have boilerplate contracts and are not willing to change them, especially in the areas that deal with liability. Do you have any advice for the banks?

Jeff: This is probably the single most difficult challenge that community banks in particular face with respect to vendor relationships. They are dealing with large entities that tend to take a take it or leave it approach. We have described in the outsourcing guidance four steps that we would like the bank to take. First, is to look at the services and identify the risks. The second, is to conduct due diligence based on that, and the third, is contract negotiation. We would suggest that when the bank, particularly the community bank, does its risk assessment, it put together a shopping list of the provisions in its contract that it would like to have based on its risk assessment. Then when it gets to the second step which is due diligence, begin to identify the service providers that are most likely to offer boilerplate contracts that will meet that shopping list. A good way of doing that is to talk with other banks at user groups. Occasionally the service providers will give you advance copies of their boilerplate. But the idea is trying to identify the service providers that are most likely to be responsive and receptive to your issue list rather than to enter into negotiations and then try to get them to change their boilerplate, because that, particularly for a small community bank, can be very difficult.

Aida: Thank you, Jeff. I think we have another question.

Jeff: Yes, an Internet question came in: What is to be considered "adequate" IT insurance coverage for a service provider? We don't have precise guidelines for that. Basically, it depends in part upon the nature of the service, and it also depends upon the nature of the service provider. One nature of the service, you would want to look at the potential exposure of the bank. What is the amount of claims that the bank would likely need to assert against a service provider if the

service provider screwed up? So, obviously, that would establish the outer limits in terms of coverage that you would want to see.
The second would be the nature of the provider itself. Some service providers are large enough that they can self-insure. They don't need to go out and acquire third party insurance, and you would determine that as part of your due diligence where you would look at the financial footings of the service provider.

Aida: Thanks Jeff. Other questions. Jack?

Jack: Woodland, Texas just popped up. Lets go to Woodland.

Woodland: When you are negotiating a contract with a servicer and you go through all of the due diligence that we have talked about here and you do your job right, what happens in a year or two down the road when there is consolidation between two companies? Typically, the new company picks up the contract and honors it, but I am just wondering if there are any problems with that if we see some consolidation within servicers.

Jeff: I think you are right. There can be problems in two different ways. One is that the merger of the servicer might change the nature of the entity enough so that you no longer are secure that you actually want to do business with this entity. That is one of the reasons why we suggest that you take a close look at your contract in terms of the termination clauses. Have you reserved a right to terminate the agreement if there is a merger or acquisition that could affect you? More generally, the problem is that as the service providing industry becomes increasingly concentrated, the number of entities out there become fewer and fewer. It becomes harder for community banks to find alternatives and that raises the question that we talked about before. How does a community bank negotiate with a huge service provider? So, I think you raise an important issue.

Jack: Woodland, Texas, thank you for joining us. Aida, do have any questions?

Aida: No, we don't have any over here.
Jack: We have about 30 seconds. Aida, I understand you have a closing thought.

Aida: Yes. We would like to thank you very much for taking the time to join us on this teleconference. Also, for all of your pertinent questions. As I invited you earlier, if after this teleconference you have other questions you would like to pose, please pass them through your ADC, your portfolio manager or your Large Bank examiner-in-charge, and we will be glad to address them. Thank you once again.

Jack: Very good. Thank you, Aida. And with that, we conclude today's program: Outsourcing Technology Services: A Management Decision, brought to you by the Office of the Comptroller of the Currency and well presented by Aida Plaza Carter, Bob Wicksell, Jeff Gillespie and Deborah Fussell.

To sign up for the OCC email service on educational announcements, you can go to the OCC Web site shown on page 2 of your handout material. We, also, encourage you to fill out your

evaluation form that came with your materials, using only spaces indicated and fax them to the number shown on the form using the fine or superfine setting on your fax machine. Your comments and suggestions are important to us, since they help us provide you with future quality programming. When I end the program on the Internet, you will have a small window pop up in the center of your screen telling you so. Just click on the OK button and your computer will go to an OCC Web site for your review.

Thank you for joining us today. Please enjoy the rest of your day and you may hang up now.