Comptroller of the Currency
Administrator of National Banks

Risk Management Principles for Third-Party Relationships

Wednesday, August 21, 2002
2:00 p.m. – 3:30 p.m. EDT
and
Thursday, August 22, 2002
11:00 a.m. – 12:30 p.m. EDT

Presented by:
John D. Hawke, Jr.
Kirk Spurgin
Greg Isaacs
Mike Koll
James F.E. Gillespie, Jr.

Mr. Tatera: Welcome and thank you for joining us for this telephone seminar, "Risk Management Principles for Third-Party Relationships," sponsored by the Office of the Comptroller of the Currency. I'm your moderator, Ted Tatera, coming to you from the operation center at KRM Virtual Seminar Services. We provide production support for distance education programs. Our presentation will run 90 minutes. You will have an opportunity to ask questions. I'll give you instructions on how to be placed in the audio queue when we begin our question-and-answer session. You can send your questions to me via fax also, 715–833–5469. Jot down your questions, fax your questions to me at any time during the program, and we will address those questions during the Q&A session.

Before we get under way I have a few points of information. The audience is in a listen-only mode throughout the program except when an individual line is opened to ask a question. If you're calling from a speakerphone and it has a mute or mic-off button, it'd be a good idea to press it now, because some speakerphones do have a tendency to clip off the incoming audio if noise or conversation is detected in the room. If for some reason you're disconnected from the program, simply call back. Your PIN will be reactivated. Included with your written materials is an evaluation form. Please take the time to fill out this form and fax it to the number listed on the page. The information you provide is important to this, as well as future, programs. And I should also mention that this program is being recorded.

At this time I'd like to introduce our presenters for today. First we have Kirk Spurgin. Kirk is a national bank examiner and core policy development analyst in the chief national bank examiner's office.

Next we have Gregory J. Isaacs, a national bank examiner and credit risk specialist for the chief national bank examiner's office.

Mike Koll is a national bank examiner and information technology lead expert with the Midwestern district of OCC.

James F.E. Gillespie, Jr., is the assistant chief counsel in the law department for the OCC.

And at this time I'd like to introduce the Comptroller of the Currency, Mr. John D. Hawke, Jr.

Mr. Hawke: It's a pleasure to welcome participants from around the country to the OCC's telephone seminar on risk management for third-party relationships. This is the latest in the series of telephone seminars that the OCC has sponsored over the past couple of years. Literally thousands of people have found them to be a useful and cost-effective way of obtaining up-to-the-minute guidance on a variety of supervisory issues. Indeed, some of you are back with us for the second or third time, and we sincerely appreciate your interest.

One of the most interesting industry developments in recent years has been the increasing ability of community and mid-sized banks to match the product and service offerings and the operational sophistication of their large-bank counterparts and do it without investing in new staff or expensive technology. Instead, they've come to rely on third-party providers to do much of the legwork for them. Through such third-party relationships, banks can fulfill their customer's demand for a broader range of nonbank financial products, and so prevent those customers from becoming someone else's customers.

Of course, many banks have for years used third-party providers for a variety of routine, back-office management and support functions, and have found that by contracting out, they can usually get those services performed on a more cost-effective basis than if the bank tried to handle them on their own. But today third-party providers are doing much more than routine bookkeeping. They're offering Internet banking services, bill payment, bill presentment, account aggregation, digital certification, merchant processing activities, customer call centers, and many other services. The list of functions currently being carried out by third-party providers, especially those functions that call for advanced technology, is an extensive one. Indeed, some providers will offer turnkey programs of a fairly sophisticated nature that may hold out enticement to a community bank to get into such activities as securitization and secured credit cards. Where such relationships are appropriate for the bank and are carefully built and monitored, they can be a source of significant bottom-line gain for the bank. Ultimately, they can help to safeguard the competitive viability of the community bank franchise itself.

With benefits, however, come risks. Risks that must be weighed and measured—both before and after a bank enters into such relationships. If the third-party provider performs badly, it's the bank's reputation with the customer that's hurt. The customer will have no idea who's really responsible for the bad performance. If products offered through a third party don't meet the applicable legal or ethical standard, it's the bank that must answer for the deficiencies. If a third party fails to fulfill contractual responsibilities, it's the bank that must make good on them. And if a bank acquires a loan from a third party that's been poorly underwritten, it's the bank's capital that might be exposed.

Unfortunately we're finding that many community banks don't fully appreciate these risks and are not devoting sufficient attention to managing third-party relationships. As we've also found, such neglect can prove to be extremely costly. That's certainly been the case with such sophisticated activities as securitization and secured credit cards.

One of the most troublesome of all third-party relationships is the practice of "charter renting." This is the term we use to describe a relationship in which a national bank authorizes a third party to conduct business in the bank's name, seeking in effect to transfer the advantages of the national bank charter to that third party. In such cases, the third party is usually far more than a mere service provider. They become the principal, for all practical purposes, with the bank simply receiving a fee for the use of its name.

While such relationships may not be inherently abusive, they often are. In several recent cases, national banks have attempted to transfer their immunity from certain state and local laws to nonbank payday lenders, for example, whose motivation has been to evade regulatory restrictions that would otherwise apply to them. This not only exposes those banks to reputation risk but also to significant potential safety and soundness problems. We've been vigilant about scrutinizing such arrangements to determine whether the national banks involved are capable of managing those relationships effectively.

To assist national banks in managing the risks associated with third-party relationships, the OCC, late last year, published a bulletin, OCC Bulletin 2001–-47, that provides industry best practices

and other guidance. This is a lengthy document, but I would strongly recommend you read it if you're involved in or considering getting involved in a third-party service arrangement. But what it boils down to is this: banks' risk management systems must reflect the complexity of its third-party activities and the overall level of risk involved. For some banks that may call for sophisticated risk management processes. But for others, whose risk exposure is limited and whose management may be thoroughly familiar with a third-party provider, our guidance may entail less formal procedures. In this respect, as in all others, our supervisory expectations are geared to the varying complexities of the banks we supervise.

Today's teleconference will focus on outsourced technologies and credit products. For that purpose we've brought together some of the OCC's leading experts to discuss a variety of legal and supervisory questions. The information you'll receive and the discussions in which you'll take part should help you see to it that your institution's third-party relationships are conducted safely and profitably.

Thanks once again for participating, and we hope you enjoy the program.

Mr. Tatera: And thank you, Comptroller Hawke. Before we continue, I would like to conduct a quick poll to get an idea of how many participants we do have with us today. Using your touchtone telephone keypad if you would please, press the number one if there is one of you listening right now. Press the number two if there are two listening. Press the number three if there are three listening. Four, press number four. All the way up to number nine. If there are nine or more of you currently participating in this telephone seminar, please press the number nine. Example, if there's a dozen or 15 or 40 in your room right now, please press the number nine. Please make your selection now.

Once again, press the number one if there is one of you. Two, if two. Three, if three. Four, if four. All the way up to number nine. Nine or more of you, please press the number nine. And I do thank you very much for your participation.

And now to continue with our program, I'd like to introduce Mr. Kirk Spurgin. Kirk?

Mr. Spurgin: Thanks, Ted. I'm Kirk Spurgin, a national bank examiner and policy analyst assigned to the chief national bank examiner's office. I'd like to join Mr. Hawke in welcoming you to this session on managing third-party relationships. But before we proceed, I refer everyone to the handout. Several pages into it you'll find some slides that pretty much follow this presentation. So hopefully you won't have to take many notes. We'll frequently reference the slide number to help you follow along.

Last year the OCC issued Bulletin 2001–-47, "Third-Party Relationships: Risk Management Principles." It's included at the end of the handout. As Mr. Hawke said, many banks are using third parties to conduct banking functions on their behalf or to provide new products and services for their customers. If a vendor hasn't already approached you with a pitch to offer new products or services, sooner or later one will.

Turning to slide 2, you'll see that we'll address why we issued the guidance and talk some about the kinds of activities subject to the guidance, but we'll spend most of our time walking through the points of a sound risk management process. My comments will pertain broadly to most types of third-party activities. But Greg Isaacs and Mike Koll will speak specifically about two areas in which we are seeing increasing use of third parties—credit-related products and services and outsourced technology services. The risk management principles in 2001–47 aren't particularly new. And slide 3 lists just some of the policy guidance we had already issued on specific types of third-party arrangements, and these issuances remain the primary guidance for those particular types of arrangements. OCC Bulletin 2001–47 is intended as umbrella guidance that draws many of the risk management guidelines from these earlier issuances, so they can be applied broadly to most types of third-party arrangements. And at the outset I should say that vendor isn't a dirty word. We don't want to leave you with any impression that we're against the concept of using third parties to offer products and services. So, on the contrary, we recognize that third-party relationships can offer banks a variety of legitimate and safe opportunities to gain a competitive edge and to improve financial performance. But—and there's always a but—we are hearing with increasing frequency from our examiners that some banks aren't properly monitoring the risks of third-party arrangements, and, in some cases, have essentially

relinquished control of the activity to the vendor. This lack of oversight has resulted in sizable financial loss. And has even led to the need for capital restoration of some banks. So we issued these guidelines, or industry best practices, for banks to consider when implementing and managing their third-party activities—whatever their nature.

Let's talk about the different kinds of third-party relationships that are subject to the guidance. They fall roughly within two categories as shown on slide 5.

First is a situation in which a third party performs a function on behalf of the bank, what we commonly refer to as outsourcing. This includes data processing services, internal audit, internal loan review, and similar banking functions. Technological advances has resulted in new types of functions being outsourced, like Internet banking. The other broad category is when third parties provide products and services that the bank itself doesn't originate. An example of this is a situation in which bank customers are offered insurance or nondeposit investment products made available by an insurance agency or a brokerage firm. Or a situation in which a nonbank vendor provides services such as payday lending, credit repair products, and check cashing through a bank. Later we will use information technology (IT) and credit-related vendor arrangements to illustrate the principles in the guidance.

Since reliance on outside parties lessens management's direct control, third-party activities can significantly increase a bank's risk profile. As part of the OCC's supervision-by-risk framework, we've identified the principle risks typically associated with third-party activities as reputation, strategic, compliance, transaction, and credit risk. Although we won't discuss these risks in detail today, slide 6 briefly describes how third-party activities can affect these risk categories.

But I would like to reiterate Mr. Hawke's comments about reputation risk. Often customers have no idea whether they're dealing with a bank employee or a third-party vendor in obtaining a product or service. It simply doesn't matter to the customer, for whom everything that happens is a reflection of the bank, not some unseen technology provider or loan marketer. So it's important that a third party's products and services meet the expectations of the bank's customers regarding quality and suitability.

As noted on slide 7, the main point of the guidance is that OCC expects banks to manage their third-party relationships in a safe and sound manner. The underlying controls of the activities should be the same, no matter whether the bank is performing the function directly or through a third party. Using a vendor doesn't wash management's hands, so to speak, of the responsibility to manage the risk associated with the activity. Management and the board of directors remain responsible for ensuring that appropriate controls and risk management processes are in place.

But having said that, we recognize that each bank's risk profile is unique, and we aren't suggesting a one-size-fits-all approach to the process. As with other activities, OCC expects banks to adopt a risk-based approach in its use and oversight of third-party arrangements. The risk management process should reflect the bank's ability to identify, monitor, manage, and control the risks posed by the third-party activity. We realize that from a practical standpoint, banks can have dozens of vendor relationships that present different kinds and levels of risk. We would expect that the risk management processes implemented would reflect these differences. In other words, the more complex and risky the activity, the more comprehensive and structured the risk management process should be. But in practice, community banks with relatively low risk exposures should be able to get by with a less-structured approach.

A risk management system is a four-stage process as shown on slide 8. The first step is taking a hard look at the proposed activity to identify the risks involved and to determine that it can aid the bank in achieving its strategic goals. The second step is selecting the qualified vendor. Followed by the third—entering into an appropriate written contract with the vendor. The fourth and ongoing stage is monitoring the third party with respect to its activities and its performance.

Now I'll briefly discuss each stage, and then Greg and Mike will provide more information specifically about credit and IT vendor relationships.

As indicated on slide 9, it's essential that management has a clear understanding of the objectives and the requirements of the activity by making an assessment of the risks posed by it, a determination that the activity is clearly integrated with strategic goals and supported by

adequate capital. Is the product or service part of an identified customer need? Does management have the expertise to properly manage and control the risks posed by the activity? And it's critical that management identifies upfront the infrastructure necessary to manage the risk. It's at this time that management should identify performance criteria, reporting needs, internal controls, and contractual requirements.

We've seen banks suffer sizeable financial losses because they didn't properly assess the risks and establish an effective risk management process. The financial risks posed by poor planning are potentially much larger than any short-term profits or cost savings achieved. So any profit or cost-savings potential in the short term should be measured against the long-term stability and viability of the activity.

We want to try to drive home some of these points by putting them into context. So now Greg will discuss aspects of the risk assessment phase from a credit perspective. And then Mike will speak from a technology services perspective. Greg?

Mr. Isaacs: Thanks, Kirk. The items Kirk described may sound basic, but you may be surprised how many times strategic planning and risk assessments are not completed prior to introducing a new, third-party credit relationship. This step should not be taken lightly. You may refer to slides 10 through 14 to follow along with this discussion.

Management needs to have answers to the fundamental issues Kirk posed on expertise, resources, and controls prior to entering into an arrangement. A little homework in the planning and risk assessment process can significantly save the bank time, cost, and headache. Plus it offers the bank a greater chance of success in the activity.

There are several common problems that banks may encounter in the planning and risk assessment phase. These include: entering credit relationships that are outside management's lending experience, failing to recognize and mitigate the risk, underestimating the risk involved in the particular third-party endeavor, and failing to devote the resources to a particular activity prior to implementation.

Entering loan arrangements through third-party channels—whether it is loan participations, syndicated loans, or broker or indirect originated loans—can result in more difficulties than benefits when the loans are outside the bank's experience or outside the bank's market area. Let me provide some examples, starting with slide 11.

Take the community bank that began making ocean-going vessel and airplane loans through commercial broker and indirect channels, only to find out that many of the liens were not perfected. The bank did not understand that the process was different from obtaining a title or filing a basic blanket security agreement. The result? Millions in unsecured or questionable collateral values. This doesn't count the time and resources expended trying to track down, repossess, and liquidate the collateral.

Or take the example on slides 12 and 13 of a bank that decided to diversify and grow their commercial portfolio by entering into an agreement to purchase truck and trailer leases generated throughout the United States from a third party. Within 12 months the bank funded leases equivalent to 100 percent of capital, and shortly thereafter the portfolio began to deteriorate. The leasing company, which had been collecting and remitting the lease payments to the bank, curtailed this service. The bank obtained delinquency reports indicating over half the portfolio was 30 days delinquent. During the repossession process, the bank found that the residuals had been set significantly higher than market values and also discovered titling problems.

Although the strategy failed for several reasons, the most important was that the bank did not understand the leasing business. The bank did not have a formal servicing agreement, did not review the documentation, and was not familiar with the trucking industry.

The preceding example also illustrates a factor that hits closer to home for many banks—expanding outside the trade area using third-party loan arrangements. Many times banks have entered into the indirect dealer and broker business, outside the bank's normal trade area, without factoring in potential increases in the cost of repossessions, dealer reputation, or loss severity.

Just because a bank is familiar with a type of loan in their local market does not mean that the same type of loan will perform the same outside this market. Each market is unique.

Another thing to keep in mind, as listed on slide 14, is resource considerations. Just because a third party may be doing much of the work, as regulators we expect the bank to have the risk management resources to analyze and monitor the process, as well as the loss reserves and capital to adequately support the activity. That means planning for potentially new systems, management information systems (MIS), and staffing is needed in some cases.

Before we move on, let me reference two documents that can provide banks additional guidance. These issuances are specifically related to third-party loan arrangements and the associated credit risk of those arrangements. OCC Banking Circular 181 (or BC 181) describes prudent loan purchase and loan participation practices. OCC Advisory Letter 2000–9 describes key components of third-party risk management and provides several good examples of the importance of sound risk management principles.

Mike, I'll turn it over to you now.

Mr. Koll: Thanks, Greg. I've listed key information technology (IT) issues in this area on slide 15. Once the bank has determined that outsourcing fits into their overall strategic plan, the first issue they need to consider is expertise. They must answer the question, "What level of internal expertise is needed to properly manage this new relationship?"'

Also, any product or service provided by a third party must integrate with the bank's existing technology infrastructure. This would include services already being contracted for from other third-party providers. Can key management information systems reports be shared seamlessly with other systems? Or will management need to develop a process to move the information from one system to another? Will the company's existing technology infrastructure support the product, or will management need to invest in additional technology, such as more bandwidth, or a more complex, more robust server, to allow for the integration of systems? All of these questions should be part of the initial planning process when looking at a third-party provider.

When doing their risk assessment, management needs to consider the potential impact of this product on their control environment. Expanding into transactional Internet banking, for example, increases the risk of external attacks on the bank's systems. Management will need to determine how their control environment would need to change in order to accommodate the change in risk profile. Will existing controls provide adequate security, confidentiality, and data integrity? Or will new controls need to be developed? What controls should be included with the product, and which ones will management be responsible for? With the emphasis on security, privacy, and confidentiality, another key factor to consider is the responsibility for compliance with the Gramm–Leach–Bliley Act, Section 501(b). How will this product fit into the bank's existing 501(b) information security program? Who will be responsible for day-to-day compliance with the program? What changes will be needed and how will they be communicated to the board of directors for their approval? All of these factors should be considered early on in the risk assessment process.

Other strategy-related IT issues to consider include, "What is the durability of this product?" Is it a temporary, hot product, one that will require constant changes to stimulate customer demand, or it a long-term seller that will require little customization or revision in the years to come? Strategically speaking, bank management needs to have answers to these questions, as they will be a factor in choosing the right vendor to provide this product or service. Kirk?

Mr. Spurgin: Now I'm on slide 16 of the handout. Once the bank has thoroughly assessed the risk, it can begin the vendor selection process. Of course, the formality of the due diligence process will depend on the complexity of the activity and how critical it is to the bank's operations. One part of the due diligence process focuses on the vendor's track record in implementing and supporting the proposed activity. The bank should contact other bank clients and user groups about their knowledge of and experiences with the vendor, and should consider consulting the Better Business Bureau, state attorneys general offices, and state consumer affairs offices. If the product or service is new to the company, evaluating the satisfaction of the existing clients may not be easy. Without a track record on that company, it may be hard to assess the company's ability to support the activity. If you're one of the first banks to contract

for the service or product, you may find yourself relying on the company's reputation for providing other types of services.

You'll need to thoroughly review the adequacy of the company's risk management system regarding their internal controls, systems security, use of confidential information, contingency planning, and management reporting by reviewing audit reports and internal policies and, if available, regulatory reports. You should also determine the extent to which the vendor subcontracts any of the work to be performed.

Other aspects of the due diligence process include analyzing the financial condition of the third party to ensure that it has the financial ability to meet its obligations and support the proposed activity. Depending on the nature of the activities and the risks posed, the bank may need to require audited financial statements and perform a detailed analysis of the vendor's financial condition, similar to that which it would conduct if it were extending credit to the party. The bank should also ensure that the third party has appropriate insurance coverage. The bottom line is, the bank needs to assure itself that the vendor will still be around in two or three years, still providing quality service.

Now Greg will provide some additional information about selecting a vendor.

Mr. Isaacs: Thank you, Kirk. As indicated on slide 17, depending upon the arrangement, this is the time to review the quality of loans being acquired and the processes of marketing, origination, and servicing. It is also the time to scrutinize the third party's financial strength and reputation. It is not the time to be hesitant about asking questions or complacent about checking out the operations. Two questions worth asking on any arrangement are: "Would my bank make a loan to this company based on its operations, reputation, and financial wherewithal? And if we do this deal, how easily and timely will it be to discontinue operations, if found unsatisfactory once into the arrangement?"

OCC Banking Circular 181 provides a great baseline for critical elements of many third-party arrangements where loans are purchased and particularly with regard to due diligence. The five basic tenets listed in the guidance and in your handout on slide 18 are:

1. Written lending policies and procedures governing transactions
2. Independent analysis of credit quality by the purchasing bank prior to purchase and throughout the life of the loan
3. Agreement by the obligor to make full credit information available to the seller
4. Agreement by the seller to provide available information on the obligor, and
5. Written documentation outlining the rights and obligations of each party

Let's move to slide 19 and build on the basic premise from BC 181—independent analysis of credit quality. This premise applies to nearly every third-party loan arrangement. If a bank is working with indirect dealers or brokers for consumer or commercial loans, the bank needs to be conducting sufficient analysis to make a sound underwriting decision. Keep in mind that this premise applies no matter who you are purchasing a loan from—good reputation, bad reputation, large bank, small bank. The analysis needs to be completed. This basic premise carries right over to third-party loan marketing companies such as credit-card marketers and payday lenders using the bank as a lending conduit. This is because the bank is taking credit risk and putting earnings and capital at risk—significant risk in some cases. Therefore, the bank needs to know whom they're doing business with, from both an operational and financial standpoint.

I've heard some banks asking, "But why do I need to get a financial statement on this third-party company? The company indicates they will buy all the loans and take all the liability?" The key to this is that the bank is highly dependent upon the company's continued ability to buy the loans and absorb the liability.

Let's move on to slide 20. A major downfall in the due diligence process is often not fully understanding what activities the company will be performing. Take the case of banks that outsource merchant processing and credit-card activities, but fail to realize that the service contract did not include fraud monitoring of transactions and, in one case, charge back processing,—costly mistakes for either activity.

Operational, or functional, reviews are critical. If a third party is providing all servicing for loans that the bank is retaining, does the company have the controls in place to perform the duties in a safe and sound manner and conform with laws and regulations? It is the bank's responsibility to ensure compliance with laws and regulations, even when delegating services to a third party.

Another important aspect is, can the company provide management information systems (MIS) to the bank for monitoring purposes of the activities? If they can't, they need to develop the MIS, or the bank may need to rethink its decision.

As listed on slide 21, this is also the time to understand what quality assurance and audit expectations of the third party the bank needs to put in place. Just because the financial review is favorable, if the audit indicates control deficiencies or servicing problems, it may not be the best decision to move forward without conducting more research and ensuring control issues are resolved. In the case of delegating activities, such as initial underwriting and collections, the bank needs to understand if the activities will be performed to the bank's standards. Keep in mind that I said "initial underwriting" because the bank should always have the final say.

On this note, one of the most glaring examples of where everything went wrong is outlined on slides 22 and 23. The lender outsourced marketing, delegated underwriting, and outsourced collections. These third parties performed satisfactorily for about a year. Then the lender approved the marketer to introduce a new, subprime, unsecured product. Growth of the new product was more than 100,000 accounts per month. Delinquencies and losses skyrocketed. In the end it cost the bank's shareholders well over $100 million to maintain the bank adequately capitalized and reserved.

What happened? One of the primary problems was with the bank's due diligence of the third party's processes prior to the introduction of the new product. None of the parties had enough staff to handle the volume of accounts when the growth erupted. Customer service was bombarded with complaints. Underwriting did not use any of the approved criteria, and

Collections was critically understaffed. All of which should have been noticed in the planning and due diligence phases of introducing the new product. And the bank could have curtailed the marketing if they would have used proper monitoring. Mike, I'll turn the subject over to you.

Mr. Koll: Thanks, Greg. While the basic framework for selecting a third party—completing a due diligence review for IT products—is the same as it is for credit and other products, there are some areas that are more likely to pop up in this era of rapid technological change. I've listed some of these on slide 24.

For example, many of the products and companies in the technology arena are relatively new and untried. This presents interesting challenges when the bank is completing a due diligence review. Many times the bank will be forced to rely on inadequate information to assess financial viability and customer satisfaction.

With the recent "dot-com bubble burst," the ability of new technology companies to receive additional funding from investors has been severely curtailed. If the bank is one of the first customers and the company experiences financial troubles, is management and the board willing to step in and support the product themselves if the vendor fails?

Another key area to look at when doing due diligence for IT service providers, is what information is available to you, both before and after you sign a contract?

Does the company routinely contract for a SAS 70 (Statement on Auditing Standards No. 70, American Institute of Certified Public Accountants) review? This review is a negotiated audit of a company's control environment as it relates to a particular system or product. A SAS 70 Type II review includes limited testing of the anticipated controls to ensure they are working as expected. Just remember that third-party vendor management can significantly influence the results of a SAS 70 review, since they negotiate over what the review covers, and they provide the basic description of the control environment. That is why a SAS 70 audit is only one tool for management to use as part of their due diligence review.

Another interesting question to ask during due diligence is whether the company will share the name of firms that decided not to purchase the product. This can be a source of balanced information on the benefits and potential drawbacks of that particular product.

When doing due diligence, management should also inquire about user groups. If a user group or groups exist, they can also be a good source of information. Particularly if they can share a current wish list for product enhancement. Sometimes the user groups will contract for separate SAS 70 reviews to ensure a more independent look at the existing control environment.

A good due diligence review will also cover how the vendor provides the service. Does the vendor rely on additional third parties to provide expertise, or do they do all the work themselves? If the vendor outsources key portions of the process, that introduces another layer of complexity to the relationship.

Some quick examples may help highlight the importance of these topics. The first one I'll call "vendor mergers." In a bank that I am familiar with, they are on their third Internet banking service provider in two years. The company they originally contracted with encountered financial difficulties and merged into a second company, who then began having financial difficulties and merged into a third company. The surviving products in each company have been slightly different, requiring continual retraining of customers and employees on the features of the product offered by the bank. The bank did not do a good initial financial analysis of the vendor they originally contracted with, so the merger activity came as a surprise. While more appropriate due diligence may not have changed their original choice, management certainly would have been better prepared for the resulting mergers when they occurred.

The second example I refer to as, "Who has the data?" Another bank that I know about contracted with a company to digitize their loan files and provide that information electronically to officers. In the course of an examination covering the Gramm–Leach–Bliley Act Section 501(b), management discovered that the vendor contracted with a third company, who actually developed the product they sold to the bank. As a result, the bank's loan file data resides on two servers owned by a company that the bank does not have a contract with. Management had

failed to reserve in its contract the right to review the controls that this third company puts in place to protect the confidentiality of the bank's customers information. Again, a more complete due diligence review should have highlighted this arrangement, allowing the bank to address the issue before customer data was converted to the new system.

My final example I'll refer to as "wireless networks." Another case of insufficient due diligence occurred when a bank decided to invest in wireless technology for the bank's internal network. The chairman's son shared with his father how cool the college's wireless networks were, and his father decided to invest in this technology for the bank. During an IT exam, the examiners heard about these plans and found out that no one at the bank understood wireless technology. They just knew they were going to implement it. Upon finding out that wireless technology poses significant risk that management was unaware of, the bank decided to abandon this project. Appropriate due diligence in this case would have saved management time and effort, as this project would never have been approved if the potential security risks were discovered up front.

I'll turn it back to you, Kirk.

Mr. Spurgin: Now let's move to the issue of contracts. The contract is an important risk control device—the opportunity to define the expectations and obligations of each party, the framework of how the arrangement is to work. A clearly written contract can prevent miscommunication and misunderstanding.

Slide 25 lists topics that banks should consider when preparing written contracts—the scope of the arrangement, identifying the content, format, and frequency of the product or service to be provided. You'll have to be diligent in specifying what you need and what you expect, because vendors won't necessarily know. A good rule of thumb is you get only what you ask for. The contract should specify fees and compensation for the service provided, how much the activity will cost, or the fees it will produce. The contract should address performance measures or benchmarks, commonly called service level agreements in an IT context, that define what level of service is expected of the third party. These measures provide the basis for monitoring ongoing performance and the success of the arrangement. The contract should clearly lay out

responsibilities for providing and receiving information. It should discuss the frequency and type of reports received, including financial and audit information, and should be sufficient to allow the bank to assess the performance of the third party relative to the performance measures.

Banks should generally ensure that periodic internal or external audits are conducted of the vendor. And in some cases banks may reserve the right to itself audit the third party or to engage an outside auditor to conduct an audit. Audit reports should include a review of the third party's internal control environment, as it relates to the service or product being provided to the bank. Reports should also include a review of the third party's security and business continuity programs. Again, you get only what you ask for, in terms of reports and performance information from the vendor.

The contract should prohibit the use of or disclosure of the bank's information except as necessary to provide the contracted services. If the third party receives nonpublic personal information regarding the bank's customers, it must implement appropriate security measures designed to meet the objectives of Gramm–Leach–Bliley Act 501(b) guidelines with which the bank must comply. The contract should identify the vendor's responsibility for protecting program and data files and for maintaining business continuity plans, including the testing of the plans. The contract should stipulate what constitutes default and/or termination and should identify remedies and allow for opportunities to cure defaults. It should state termination and notification requirements with timeframes to allow for the orderly conversion to another vendor and without prohibitive expense. And it should provide for the timely return of the bank's data and other bank resources.

Some other points that may need to be addressed in written contracts are listed on slide 25 and are fully discussed within the bulletin itself.

Greg, what are some contract issues from a credit perspective?

Mr. Isaacs: Kirk, this is the test of how well a bank performed their planning risk assessment and due diligence. As indicated on slide 26, work in these areas is fundamental to contract

provisions. The contract is the place to make sure the bank has stated its rights to conduct operational reviews, audits, and obtain standard management information systems. Financial information is critical if the bank is dependent on a third party to buy loans or share in the liability. Another fundamental issue is supplying timely information on loan purchases and participations in order to conduct ongoing analysis.

Third-party marketers often do not have the financial wherewithal to survive for very long if operational or credit losses increase. Failure of a third party providing credit-related services or loan-buying arrangements can greatly increase the risk to the bank, and has significantly contributed to the failure or voluntary liquidation of several banks. This underscores the importance of obtaining the financial information regularly and, if concerns are noted, appropriately amending the arrangement if possible. To do so however, requires some detail in the contracts regarding obtaining financial information as well as termination and recourse requirements.

Moving on to slide 27. The earlier leasing example provided in the strategic planning section is a classic case of not understanding the responsibilities of each party. In that example, among the other issues, the bank did not have a formal servicing agreement in place for the collection and submission of payments.

Another area in which to be vigilant when reviewing a new contract or existing contract, is the liability or recourse provisions as indicated on slide 28. Depending upon the circumstances, the bank may have more risk than they believed. For example, many merchant processing arrangements with third parties, such as acting as an agent bank, indicate the bank takes all or part of the liability if the merchant cannot cover chargebacks. If your bank has an agent bank arrangement, check your contract. You may be surprised to find out the party you contracted with may expect you to cover the losses. Although this example is a low-risk situation with most community banks, it is something to keep in mind when reviewing any contract.

Marketing companies also pose some interesting contractual issues. Let's take a company I saw marketing an overdraft protection product. The company in the contract and agreements was

clearly trying to state that the overdraft was not a loan and therefore did not create a credit risk. They were right. It did not create a credit risk for the marketing company, but it clearly created a credit risk for the bank. But more importantly, the marketing company in this case was to handle the monitoring and measuring processes but there was no mention of MIS-sharing with the bank or recourse by the bank in the event of credit performance issues or customer service issues. The contracting question only had one form of recourse and that was if profitability hurdles were not met.

Mike, I'll turn the discussion over to you.

Mr. Koll: Thank you, Greg. While basic contract provisions are the same across all products and services, I've listed some key areas from an IT standpoint on slides 29 and 30. 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 the 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, the bank may face unanticipated difficulties in getting control over their own information after service provider bankruptcy.

An area that is often missed, especially by community banks, is the area of service level agreements. These are typically addendums to a contract that specify what level of service is expected. These addendums could specify expectations for response times, system availability, data integrity, and the timing of management report availability. Most of the time these agreements define an acceptable range for each measure.

Another key area for IT contracts is to make sure that each party's responsibilities are set forth in four key functions: customer complaints, intrusion detection and monitoring, security including Gramm–Leach–Bliley Act 501(b) compliance, and business continuity planning. Without defined responsibilities, it is very easy for customer complaints, intrusion attempts, and security controls to be neglected, as each party believes the other one is handling it. For Gramm–Leach–Bliley Act section 501(b), management also needs to remember that all contracts signed prior to

May 2001 must be renegotiated to address this article by July 1, 2003. Also management must understand their responsibilities for business continuity planning in order to provide for a smooth recovery from a disastrous event.

IT contracts should also discuss the bank's rights to review audit reports on the service provider. Bank management needs to have access to this information in order to assess the control environment at the service provider. If this type of access is not granted in the contract, it may be difficult for management to fulfill some of their responsibilities in the area of security over customer data.

Here's an example that illustrates what type of problems poor contracts can cause: a community bank contracted with a third party to do their core processing, by signing a standard vendor contract. When examiners criticized the bank for not monitoring the vendor's financial and operational condition on a periodic basis, the bank went back to the vendor looking for current financial statements and audit reports. The vendor 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.

Finally, I just want to remind everyone that contracts should provide that the performance of services by external parties for the bank is subject to OCC examination oversight. Kirk?

Mr. Spurgin: Thanks, Mike. Now I'm on slide 31. The fourth and ongoing stage of the risk management program is monitoring of the third party with respect to its activities and performance. Again, the formality of the oversight program will vary, depending on the nature and risks of the activity. Generally, banks should review the third party's financial condition at least annually, and more frequently when risk is high or increasing or for complex activities. For significant relationships, as with the due diligence phase, this analysis should be similar to what would be expected if a third party were a borrower, and audited financial statements might be required. If a third party uses subcontractors, as is common in many outsourced technology arrangements, banks should determine that the company is meeting its financial obligations to its subcontractors. Banks should also review the adequacy of the third party's insurance coverage

to see to it that the coverage required by the contract remains in force and effect. Banks should also monitor the vendor's controls by reviewing policies and reports that are provided under the contract, such as audit reports, compliance reports, regulatory reports, security reviews, and reports of business continuity planning and testing. As said earlier, banks may opt to conduct onsite reviews and audits in some cases, including participation in user groups. Also, banks should assess the quality of service provided by the third party by regularly reviewing reports documenting the vendor's performance relative to the agreed-upon benchmarks of service level agreements. Customer complaints should be reviewed. And banks may consider the need to administer mystery shopper or customer call-back programs to determine customer satisfaction with any products and services provided by the vendor. Banks should also assess the quality of training provided to bank employees, if applicable. Finally, banks should periodically compare actual earnings and costs to budgeted amounts to determine whether the arrangement is providing the return that was projected during the initial strategic planning phase.

Greg will now provide some more information about ongoing oversight of vendors who provide credit-related products and services.

Mr. Isaacs: Improper monitoring has been the Achilles heel of many third-party credit arrangements. As listed on slide 32, many credit-related problems have resulted from a poor understanding of activities performed by the third party, improperly established MIS reporting, no functional or operational area reviews, no quality assurance reviews or audits, no ongoing financial monitoring, and no monitoring of loan concentrations. Several of the examples that I have described in previous sections highlight the importance of ongoing monitoring.

Let me provide a couple more to illustrate its importance. These examples are outlined on slides 33 through 35. First, let's take a look at a couple of common arrangements: indirect dealers and brokers. It is important to have MIS to track the performance of the loans booked. Often, a little analysis will show whether or not it is a wise decision both from a credit risk and profitability aspect to continue an arrangement. Poor performance or changing performance can indicate changes in the business practices of a dealer or broker. One area where I've seen numerous issues is in the proper monitoring of delegated underwriting functions. That is where the bank

relies on a third party to conduct the underwriting, with final approval by the bank. Issues involving improper monitoring of delegated underwriting activities are especially common when the bank is acting as a conduit for payday lenders and subprime credit card marketers. I've seen several cases that underscore the total failure of the review process. Loans were booked that did not go through a review to ensure that underwriting standards were followed. Basically, anything that came through the door from a third party was booked. This is the perfect scenario for a third party to provide loans that do not meet the bank's underwriting standards or to make fictitious loans. This is compounded even more when the collection activities are also at the same third party, as manipulations may occur. In some cases, this has led to significant problems and financial losses.

I focus primarily on the credit risk side of third-party credit arrangements; however, keep in mind that reputation and compliance issues can cause significant difficulties. For example, a current instance of this is the Justice Department stating that third-party marketers running a thrift subprime credit card business violated the Equal Credit Opportunity Act. The reimbursement ordered: over $1 million. This recent case serves to underscore the importance of monitoring the actions of third-party marketing, origination, servicing, and collection activities, not just for credit risk but for other risks as well. I'll again turn the discussion over to Mike.

Mr. Koll: Thanks, Greg. Ongoing oversight in an IT environment deals mainly with the ongoing viability of the company providing the service, the present level of service, and the control environment. I've listed key points in each of these areas on slides 36 through 38. For ongoing viability, reviewing the company's financial condition is important. However, for new companies, the financial information may not be that good or that reliable. In the case of privately held companies, it may not be available at all. If financial statements aren't available, you may need to ask for budget projections or recent customer trends. Another possibility is reviewing news publications for any press releases related to that company.

Analyzing the financial condition may be difficult as well, as the result of some of the things we mentioned earlier. IT companies tend to have very different balance sheets. Most of the value in the company may reside in assets that are largely intangible. This would include the value of

software they developed, goodwill attained in a merger or consolidation, or a value for the customer base currently under contract.

In spite of all this, management needs to make the effort to obtain this information and analyze it to the best of their ability. If you have a vendor with statements that are difficult to analyze, you may want to enlist the help of a seasoned credit officer or perhaps a larger correspondent bank to guide you through the analysis process.

To assess the quality of ongoing service, service level agreements should be in place. Without specific measures, it is difficult to define good performance versus fair performance. In a really serious dispute, this could result in a long, drawn-out court battle. Performance data should be reviewed on a regular basis, depending on the volume of customer use of the product. For key products, monthly may not be often enough. If the service provider doesn't prepare the information as often as bank management would like to see it, what does that say about how the service provider is managing the quality of service? Another item to consider is what information is used to determine when a customer is dissatisfied? Are the standards the service provider uses the standards you want to follow? The quality of service provided to the bank is also a function of how quickly the bank can change product, terms, and conditions, and how costly is it to implement new features and functionality. A product that cannot be adapted quickly to serve the needs of your customers is not a good quality product. How well does the service provider respond to your concerns? Do you receive call backs in a reasonable period of time? If the company doesn't act on your request, do you receive a good explanation for why? All of these need to be factored into the quality of the service provided.

The final area I'll discuss in ongoing monitoring is controls. Management has a number of potential sources here. SAS 70 reports can provide a good description of the control environment in place at the service provider. A SAS 70, Type II report requires testing of the controls. For this reason it is generally preferred over a SAS 70 Type I report.

For financial institutions, if the company you are a customer of in a service bureau environment is examined by the regulatory agencies, you have the right to request a copy of that examination

report from your agency. However, simply getting a copy of this report will not satisfy the bank's responsibility to monitor their third-party service provider.

Understanding your responsibilities for business continuity planning will help you maintain service to your customers in times of disaster. Participating when you can in vendor tests of the vendor's business continuity plan is a good way to make sure you understand your responsibilities in this area.

Another key area to monitor for control purposes involves vulnerability assessments and penetration tests. Knowing what is reviewed in these areas and understanding how your third-party service provider responds to the results provides a lot of insight into how they approach internal controls and security concerns.

An example of why this is important follows: a community bank contracted with a third party to provide transactional Internet banking to their customers. They relied on the third party to set up the Web server in a secure manner. The bank also contracted with two separate third-party firms to do vulnerability assessments and penetration tests on their Internet banking products over a period of six to nine months. In spite of this, the bank was "hacked," using a known vulnerability that had existed for many years. How did this happen? Part of the reason was inadequate monitoring of what the third parties were doing. The vulnerability assessments and penetration tests did not cover the Web server where the vulnerability existed. Management did not do enough work to make sure that the vendors were doing the job they were contracted to do. If management had monitored these vendors more closely, the known vulnerability most likely would have been discovered and fixed before the hacker exploited it.

Kirk?

Mr. Spurgin: In wrapping up, we should emphasize the importance of the board of directors' involvement in the risk management process. The board should be a part of the risk assessment and vendor selection processes and should periodically review information reflecting the performance of significant vendors and other results of management's ongoing oversight

activities. The board should be thoroughly aware of the risks presented by material third-party arrangements and of the results of management's oversight program.

And you're probably wondering what the examiners will be looking at, with regard to third-party arrangements. Examiners routinely ask during periodic monitoring activities if management has introduced, or plans to introduce, any new products and services. We strongly encourage you to consult your examiner-in-charge early in the process so he or she can give you a regulatory perspective on the activity. During examinations, examiners will want to understand how you manage these types of relationships. For new activities, they'll want to discuss your strategic planning efforts and how you assess the risk. They'll look at the results of the due diligence review of your new vendor or service provider and at the contract governing the activity.

For new and existing activities, examiners will want to review the reports that you routinely use to monitor the third party's performance and controls. They'll look at your analysis of the company's financial condition. They'll review board and committee minutes and take a look at the information presented to the board to determine the level of board involvement in the activities.

But on the flipside, for activities that are performed well and have been well supervised, examiners may review relatively little, because of the perception of low risk. But examiners will criticize banks whose material third-party arrangements pose undue risk or whose risk management systems over those activities are inadequate or ineffective.

In conclusion, OCC supports banks' use of third parties to meet strategic objectives when management and the board implement appropriate risk management processes over those third-party activities. Control of the activities should never be relinquished to the third party. The risk management system should be commensurate with the complexity of the activity and the risks posed by it. Some processes may need to be highly structured and formal, while others may be far less systematic. Again, it all depends on the risks presented in the context of your individual bank. But a risk management process over third-party activities is simply one part of an overall, robust risk management structure. That's the lecture portion of our presentation.

Now I'll turn it back over to Ted so that he can give us the results of our polling question. And then turn it over to you to ask questions of the panel.

Mr. Tatera: Alright. And our polling question earlier—we had 142 sites respond to the number of participants at each site. And we came up with a minimum of 600 participants for today's program.

Now we're going to the interactive portion of the program. You can interact with our presenters. If you'd like to ask a question or make a comment, right now press the number one on your touchtone telephone keypad. And I'll call on you by the first name of the registrant at your site and the city and state that you're calling from. If you are on a speakerphone, we ask that you please use your telephone handset. This way everyone will be able to hear you more clearly. And as I mentioned earlier, some speakerphones do have a tendency to clip off the incoming audio if noise or conversation is detected in the room. If your question is answered before we call on you, press the pound key and you'll be taken out of the queue.

You can still send your faxes, 715–833–5469. Again, 715–833–5469. Send your faxes.

We have about 26 minutes left in the program, and we will address those faxes. And, also, we would like you each to limit your question to one—we would like to answer as many of your questions as possible.

So, if you do have a question or a comment, right now press the number one on your touchtone telephone keypad. And let's go over to Oakland, California, and Janet's site first. Go ahead, please.

California: Yes, this is Tom Ray. In the contract portion on the IT, you stated that intrusion detection and monitoring should be one of those four areas. And I would assume then that you're reporting from the section up above would also be the reporting on intrusions in the

environment beyond just the service area, though, especially when you consider the reputation risk. Is that correct?

Mr. Koll: This is Mike. I would agree that reporting of any type of intrusion should be part of a standard contract provision that deals with reporting. You can get to response times and service levels—just the basic performance itself. If the bank has a third party providing a contract and a service, you need to know when that service is being attacked from the outside. I would think that would be vital piece of information you'd want to include in your contract.

California: And that would go for whether it's commercial information or customer information—either side?

Mr. Koll: It is mandated by Gramm–Leach–Bliley for nonpublic personal information, but I would also think you'd want to know that if it was attacking on the commercial side as well.

California: Thank you.

Mr. Tatera: You're very welcome. Thank you for your question. Now we have 24 and a half minutes left in the program. We have two callers left in the queue. So if you do have a question or a comment, please push the number one right now on your touchtone telephone keypad.

Let's go to James' site in Sheboygan, Michigan. Go ahead, please.

Michigan: Could you elaborate on the kinds of indemnification clauses you would or would not like to see in contracts?

Mr. Gillespie: This is Jeff Gillespie. Our main point about indemnification clauses is that the bank should review them carefully and shouldn't just passively accept what's offered. Banks should have their legal staff involved in looking at those clauses, because often we have found situations where, through indemnification and hold-harmless clauses, the bank really ends up

absorbing all the risk for the relationship. And frankly, that creates a "moral hazard"[1] situation—where the service provider or the vendor no longer has an incentive in terms of maintaining sound or proper procedures. So the important thing is just to look at these clauses carefully and get your lawyers involved.

Michigan: We have a follow-up to that.

Mr. Gillespie: Certainly.

Michigan: We're a smaller community bank, and, frequently, when you're dealing with vendors of the size that you do with technology services, often times it's the take-it-or-leave-it response you get, when you ask for any variation of contracts.

Mr. Gillespie: And the question is, "How do I deal with that?"

Michigan: Exactly.

Mr. Gillespie: That's a very important question. Certainly there are a number of different approaches. When you enter into a basic negotiations, you should have a list of what you're looking for—what characteristics, what provisions in the contract you want. OCC Bulletin 2001–47, I think, lays out a good list for you to look at. You might also consider asking for copies of the vendor's contract in advance of your serious negotiations, so you can see how well potential vendors, who use what we'll call "boiler plate contracts," how well those contracts line up with 2001–47—so you'll know what issues you have going into the negotiation.

Another way is, as both Mike and Greg suggested, is to talk with other banks before you get into your negotiations, so you know basically what issues and concerns have arisen. User groups can be a wonderful source for this information. The basic point is that, when small banks are dealing with large service providers, they're at a real disadvantage in terms of negotiating. So you have

[1] "Moral hazard" is the likelihood that the behavior of a person (or vendor) will change as a result of the removal of real or perceived potential risks from certain activities.

to select who you're going to approach. You have to select your potential vendors based on proper advance reviews. And if enough small banks do that, then the market will work in your favor.

Michigan: Thank you.

Mr. Tatera: Alright, thank you very much for your call. Next, let's move on to New York City and Amir's site. Go ahead, please.

New York: Hi, you have discussed outsourcing technology and credit-related activities. We are looking at outsourcing our human resources function to a third-party Fortune 500 company. I was just collecting some references on this company, and I noted that no financial institutions were provided as a reference. I was wondering, does anybody have any experience with outsourcing human resources (HR), and if there were any other special considerations in addition to those that you mentioned in connection with this activity?

Mr. Spurgin: This is Kirk. I don't think any of us in the room actually have experience with HR outsourcing. But from my personal perspective, I wouldn't necessarily be troubled by the fact that there were no other financial institution clients. But essentially the same risk management principles that we laid out in this bulletin would certainly apply to that same type of outsourcing activity. Does that answer your question?

New York: Well, sort of, in that I shouldn't be concerned about not finding financial institutions, namely banks, as signing up for HR outsourcing. Of course, there are several brokerage companies that have done this, and they certainly are as heavily regulated as we are. So I think that answers my question.

Mr. Spurgin: Well, in general, too, we are aware of banks and other financial companies that outsource their HR departments. And you know, if you're asking in general if we're concerned with that, I would say that as long as that outsourcing is well managed there wouldn't be a serious concern about that.

New York: Do you have any special problems with the fact that this would involve the leasing of your employees to the outsourcing company?

Mr. Gillespie: This is Jeff Gillespie. There certainly are issues that can arise from the sharing of employees or the leasing of employees. If you look at 7.0001 in part 7 of the OCC regulations, you'll find some discussion about dual or shared employees.

New York: Thank you very much.

Mr. Tatera: Thank you for your call. And we have approximately 18 minutes left in the program, four callers left in the queue. So let's go to Amit's site in East Brunswick, New Jersey. Go ahead, please.

New Jersey: Yeah, could someone give us an idea or some examples of performance measures or benchmarks that you've indicated on slide 25 for contracts, particularly related to IT contracts. What do community banks need to look for in their contracts with respect to performance measures or benchmarks?

Mr. Koll: This is Mike Koll again. One of the reasons why we're talking about service level agreements, especially as related to the community bank market, is that there are not a lot of community banks out there that have put these in place. What you're basically going to be asking for are criteria that will be used to define what is an acceptable level of service. For example, if you're contracting with a third party to provide a telecommunications network, one of the benchmarks you would put out there is the amount of time the network is available to your employees. Is it a 95 percent availability? Is it 99 percent availability? That's typically how those types of things are going to be referenced. If you're talking about a customer-service or a customer-complaint or call-in center type function, then you're talking about the average wait time before someone picks up the phone—the average number of rings before a call is answered. It's basically performance measures for the company providing the service, so that you both have

a very clear understanding of what level of service you are expecting to be provided. Does that help?

New Jersey: A little bit. I guess we're looking for some more examples for the actual systems of small community banks, where the systems are outsourced to an IT service provider, with respect to their database, and what type of items they should think about including in their contracts.

Mr. Koll: Well, again, since you're outsourcing—I'm assuming—the entire system, you're going to want on-time availability. You're going to want to know exactly what the vendor expects to provide, as well as when information is entered into the system and processed at the end of the day and how soon before management reports are there—those types of issues.

New Jersey: OK.

Mr. Tatera: Alright, well thank you for your call. We have three callers left in the queue. So if you'd like to be placed in the queue to ask a question or to make a comment, simply press the number one right now on your touchtone telephone keypad.

Let's go next to Mark's site in Bettendorf, Iowa. Go ahead, please.

Iowa: We currently receive a SAS 70 audit report from our largest third-party vendor who provides electronic data processing services to us. We also use a large bank that provides [bond? inaudible] accounting services to us. And we recently asked them for a SAS 70 audit report. And they said that they do not have that. They use an internal audit department to do that. Does that suffice, or are we supposed to be getting a SAS 70 audit report from these types of companies?

Mr. Koll: Actually, this is Mike again, a SAS 70 is just one tool. From our perspective as regulators, you should be getting reports that tell you about the control environment, if that's the result of an internal audit that's being done at a financial institution or a third-party service

provider, where a SAS 70 is not the most important thing. What is most important is, what does that audit cover? What are the limitations there? What are the findings? And what is management doing about it? Those are the kinds of questions that you're going to need to be able to answer after looking at this information. But the SAS 70 is simply one tool and is more prevalent when you're talking about independent third-party service providers.

Mr. Tatera: Does that answer your question?

Iowa: Thank you very much.

Mr. Tatera: Alright, thank you for your call. And continuing on, we have about 14 minutes left in the program. Let's go to Cherry Hill, New Jersey, and John's site. Go ahead, please.

New Jersey: Hi, we have a question about monitoring controls regarding vulnerability assessments and that type of thing. At our bank we have systems in place to detect intrusions, and we do our own penetration testing. Does that mitigate somewhat our risk with our third-party servicers as far as contractual natures around that type of thing?

Mr. Koll: This is Mike again. Since you aren't technically contracting with a third party to provide these services, doing them yourselves does mitigate the risk of doing it with a third party. The risks are still there, in that you have to make sure you're doing an adequate job of the vulnerability assessments and the network intrusion detection in order to make sure no one comes in unnoticed. But you certainly have mitigated any risk that would've arisen strictly from a third-party provider standpoint.

New Jersey: OK, thank you.

Mr. Tatera: Alright, thank you very much. We have two calls left in the queue. Let's go now to Donald's site in Cambridge, Massachusetts. Go ahead, please.

Massachusetts: Thank you. It strikes me that there are a couple of challenges in applying these processes.The first is to do so on some sort of consistent basis as it pertains to due diligence and contract management. And the second is to support some form of auditability related to the application of those processes. Can the OCC comment as to both, for the benefit of community banks and national banks, on what direction you're providing in so far as automation of these processes? So, is documentary evidence as contained in files and the like sufficient? Or are you encouraging these banks to automate an informative system?

Mr. Koll: This is Mike again. And I'm not aware that the OCC as an agency is mandating how the monitoring is to be either reported or documented. If it's an electronic system that's been automated, as long as it provides the information that you need to monitor the relationship, I think we'll be satisfied with that. Likewise, if you're getting paper reports from the vendor, as long as that's happening on a timely basis, and you're getting the information when you need it, that should also suffice from our perspective. Did that answer your question, or did I miss the point?

Massachusetts: Yeah, I think what you've answered for me is what direction you might provide. It would seem, given some of the inherent complexities of these relationships, that doing it on a paper-based process presents its challenges particularly in making it an auditable process.

Mr. Gillespie: This is Jeff Gillespie. I just want to add that I'm sure your lawyers will tell you that, if you're receiving electronic reports or documents, you want to make sure that they are received and retained in a way that would make them admissible in court, in the event that you did end up with a dispute. The law in this area is still developing, and it varies from state to state. So again, if you're looking at electronic document retention or record retention, you want to have your legal staff involved. Thanks.

Massachusetts: Thank you.

Mr. Tatera: Alright, thank you very much for your call. We have 11 minutes left in the program, plenty of time to take your calls. If you do have a question or a comment, simply press the number one on your touchtone telephone keypad right now. We have three callers left in the queue. So let's go to Edna's site in Randolph, Vermont. Go ahead, please.

Vermont: Yes, we use Microsoft products for a lot of our software applications, not our major processing, but what is your take on whether or not we should try to do financial analysis on a company such as Microsoft?

Mr. Koll: This is Mike again. For a company such as Microsoft, which tends to be in the daily news and the national news on a daily basis, we take a much more flexible view of any financial information review. Also the type of product that you're using is not what I consider to be critical to your operation. You can go out and get another word processing package that can convert Microsoft Word documents, for example, very quickly. So the risk of something not being workable because of a problem with Microsoft is much lower than it is with some of the other third-party providers. The potential of missing a key development in Microsoft's condition or their ability to provide that service, I think, is remote given the amount of national coverage they get. So we would not expect you to get annual financial statements for example, or to do anything outside of basically just keeping aware of them in the news.

Mr. Gillespie: This is Jeff. To build on what Mike is saying—if you're dealing with a publicly traded company, they're going to be filing public security statements with audited financial statements, and you can rely on those, I would think. Thanks.

Vermont: Thank you.

Mr. Tatera: Alright, thank you very much for your call. Let's now go once again to Janet's site in Oakland, California. We have one call left in the queue. So if you do have a question or a comment, simply press the number one on your touchtone telephone keypad. Janet's site in Oakland, California. Go ahead, please.

California: There's an increasing number of outsourcing of collection and telemarketing to international vendors. That being said, does the FFIEC (Federal Financial Institutions Examination Council) plan on doing any exams of those types of vendors, like they do with the domestic vendors?

Mr. Koll: I'm sorry. Could you ask that one more time for us, please?

California: OK. A lot of collections and telemarketing services are being outsourced to international vendors. That being said, does the FFIEC or the OCC or the OTS plan on doing any IT or any type of safety and soundness exam on those types of vendors?

Mr. Gillespie: This is Jeff Gillespie. The OCC recently issued Bulletin 2002–16, which specifically talks about bank use of foreign-based third-party service providers. In that guidance we specifically say that while we reserve the authority to do reviews of foreign-based service providers, generally we will not. Instead, what we will rely upon the bank's due diligence and monitoring, and also upon the local supervisors to the extent that there are local supervisors that review those providers. So take a look at OCC Bulletin 2002–16. I think it will answer your question.

California: OK.

Mr. Gillespie: Thanks.

Mr. Tatera: Thank you very much for your call. Next, Tampa, Florida, at Paul's site. Go ahead, please.

Florida: Yes, can you please clarify the scope of contracts that must be renegotiated by July 1, 2003, if they were negotiated prior to May 2001?

Mr. Gillespie: Yeah, this is Jeff Gillespie. Basically, they are contracts that involve the processing of customer information as defined under the (Gramm–Leach–Bliley) 501(b)

guidelines, which are located in 12 CFR part 30 for national banks, and that ties in with the definition of customer information in the privacy rule, also promulgated under Gramm–Leach–Bliley. So, if you have a service provider that is collecting or processing "customer information," the contract will no longer be grandfathered after July 2003, and you should renegotiate that contract so it will comply with the requirements of 501(b).

Florida: OK, thank you very much.

Mr. Gillespie: You're welcome.

Mr. Tatera: Alright, thank you for your call. Moving on now. Let's go to Charlotte, North Carolina, and Nancy's site. Go ahead, please.

North Carolina: Thank you. This is Nancy [Staff?] with Bank of America in Charlotte. What do you consider adequate evidence that a third-party supplier's obligations to subcontractors are being met?

Mr. Koll: This is Mike. Adequate evidence that a third-party vendor's responsibility with their subcontractors is being met, is that what the question is covering?

North Carolina: Yes, one thing that I heard today that I have read before is that banks, to be diligent, need to make sure that the person they are contracting with has met their obligation, or is meeting their obligations, to subcontractors. And I was just wondering what you consider adequate evidence that the third party is meeting their obligations?

Mr. Koll: I think the difficult part of that question is that it's going to vary depending upon the situation and the criticality of the business being done for each individual institution.

North Carolina: Let's assume it's a critical technology supplier.

Mr. Koll: What we're going to expect the bank to do is to be able to look at the information provided by the vendor and satisfy themselves that the vendor is managing that subcontractor relationship in the manner they should be. We're not going to be satisfied with them just saying, "Well, we haven't heard of any problems" or "It appears that the payments are all on time." We're going to be looking for the bank to be aware of what the vendor's process for working with that subcontractor is.

North Carolina: And do you have something in mind as to what the bank should be requiring as evidence? I mean, do you actually want some sort of written statement that is in a file someplace, that's showing that they're saying, "We're currently meeting it," or do you want the banks to be contacting the subcontractors directly with the supplier's approval to say our obligations are being met?

Mr. Gillespie: This is Jeff Gillespie. We're not looking for legal evidence here. We're looking for something that would be commercially reasonable and basically establish the fact that the bank is looking to make sure that there are not going to be unexpected problems arising with a subcontractor due to a payment dispute. So there's a lot of flexibility here.

North Carolina: And you don't want to give me some good ideas?

Mr. Gillespie: Well, I think the written report is a good idea. We're just not going to say that that's absolutely mandated in every case.

North Carolina: OK, thank you.

Mr. Tatera: Alright, thank you very much for your call. We have five calls in the queue. Let's go to Jane's site in Denver, Colorado. Go ahead, please. Jane's site, Denver, Colorado. Do you have your mute on?

Alright, let's move on to Ann's site in St. Paul, Minnesota. Go ahead, please.

Minnesota: Hello, our question has to do with notification of the large third-party providers. I mean, we've had situations where we've contacted large third-party providers, and they have been unaware of some of these regulations and have been a little bit put out by some of the requirements that we presented to them in terms of their contract, etc. What are you doing to help us with that? Thank you. [audible click]

Mr. Gillespie: This is Jeff Gillespie. There are a number of different things we've done. First is that when we issue the bulletins, of course, they are addressed to service providers. For example, Bulletin 2001–47, was issued to and made available to service providers. And when we issued the bulletin, we included a publication on our Web site, so it is readily available to service providers.
Second is that to the extent that the OCC is the examining authority for particular large service providers, the examiners would discuss 2001–47 with the service providers. The bulletin has only been out since November 2001, and it's going to take a while for it to become general knowledge within the service provider community.

The last thing is, if your bank ends up with a problem with a service provider in terms of how 2001–47 might apply to them, we'll be happy to work with the bank in terms of explaining to the service provider what the implications of the bulletin are. Is that responsive?

Mr. Tatera: I believe they did disconnect.

Mr. Gillespie: OK.

Mr. Tatera: Alright, moving on now. We have four calls left in the queue. If you'd like to be placed in the queue to ask a question, simply press the number one on your touchtone telephone keypad. Springhouse, Pennsylvania, and Rob's site. Go ahead, please.

Pennsylvania: The OCC seems to have done a remarkably thorough job of providing detailed guidance for OCC-regulated banks on the scope of these problems. I'm wondering if, without

duplicating your presentation over again, you could point those of us who perhaps have nonOCC-regulated banks to counsel, as well on what the FDIC is doing in this area.

Mr. Gillespie: This is Jeff Gillespie. The OCC Bulletin 2001–47 is based in part upon an FFIEC bulletin that was put out in November 28, 2000, to which the FDIC was a signator. It's called "Risk Management for Outsourced Technology," and I'm confident that that bulletin is available through the FDIC Web site or the FFIEC Web site. Or, if you can't find it there, you can certainly find it on the OCC Web site, under "electronic banking," and it does reflect the thinking of the FDIC.

Pennsylvania: Thank you.

Mr. Tatera: Thank you very much. Moving on now, let's go to Chicago, Illinois, and Sharon's site. Go ahead, please.

Illinois: Hi, I have a couple of questions, please. First of all, I've been very active in the industry in this topic and one of the things that I've heard several compliance officers state that this is guidance. It's not a bulletin;it's not required. And, therefore, those who are responsible for trying to get the momentum behind supporting putting the activity in place are sometimes facing some resistance. Can you tell me why this is not a bulletin? Why is it guidance? Or am I misunderstanding guidance versus bulletin?

Mr. Koll: This is Mike. Sharon, we as a regulatory agency tend to look at our bulletins and our guidance very similarly. So I'm not sure what the difference is. My thought is it's not a regulation because of the sheer amount of flexibility and the sheer volume of differences in the types of third-party relationships that a bank runs across in the course of their business. Because of that and because of the wide variation in the population that we cover, we offer a fairly detailed guidance and expect the examiners and the bankers to be able to pick and choose from that what actually works and makes sense for them at their own locations.

Illinois: OK, though what I've heard you say is that this is guidance, but it is absolutely required activity?

Mr. Gillespie: This is Jeff Gillespie. I'd like to clarify that in part. OCC Bulletin 2001–47 is guidance. It will be the basis for supervisory comments that our examiners will provide and could be the basis for comments that would be, for example, "matters requiring board attention" in an exam report. Distinguish that, however, from the guidelines that are implementing Gramm–Leach–Bliley 501(b), which are mandatory. The Gramm–Leach–Bliley guidelines are discussed within the context of 2001–47. So there are provisions in 2001–47 which are nonmandatory, because they are intended to provide general guidance and flexibility to the industry. On the other hand, 2001–47 also references mandatory provisions in the 501(b) security program and procedures and in the privacy rules, particularly with respect to provisions that should be in vendor contracts. So, admittedly, most of 2001–47 is nonmandatory guidance; it does, however, reference some mandatory provisions, which arise from other issuances or other statutes.

Illinois: Thank you. The second question I have is that we've had a lot of discussion about community banks, which are less complex, and, therefore, the requirements they have to go through to achieve their level of oversight of third-party providers is, of course, less than a more complex financial institution. However, one of my concerns is that when you pull all of these together and look at some of the service providers that service so many community banks, when you have one of those service providers who is failing to exercise appropriate controls, you now have a larger issue. So you have multiple community banks that are going to suffer the results, and, therefore, those would equate to, potentially, one large financial institution's impact. What are you all doing relative to looking at the combined risk associated with community banks in using common service providers?

Mr. Gillespie: This is Jeff Gillespie, and I'll take a stab at that. I think it's a profound issue you're raising. We issued this guidance in part because we recognized that the market that large service providers faced was fractionalized. As you know, there was a large number of small banks that individually did not have a lot of negotiating power. We felt that by providing some

guidance to the industry, we could help these banks in terms of dealing with these larger providers. What we hope will happen is that the smaller community banks will go through the process that we have outlined in 2001–47 and that that will equip them to deal with the larger service providers. For example, two crucial steps are risk assessment and due diligence. We're hoping that when a small institution is thinking about entering into a vendor relationship, they will look at the guidance, do a risk assessment, and come up with a shopping list, if you will, of what sort of contractual provisions they think are particularly important. Then as part of their due diligence, they can check around, for example, with user groups and with trade associations. They can obtain copies of standardized contracts and determine which service providers are most likely to meet their shopping list. Then they'll know that going into their discussions with the service providers. Hopefully they'll pick one that will be most likely to be amenable to their list. And now I think Mike has some additional thoughts.

Mr. Koll: I just wanted to mention that the effect on the banking system, measured by the number of customers and the nature of the service being provided, are some of the key criteria we use when deciding whether or not we, as regulators, are going to examine a third-party service provider in the IT world. So we do try to make sure that we cover, not just the individual bank aspect but also the systemic impact of a single provider on the banking system.

Illinois: Thank you very much. And I have one comment. The gentleman earlier indicated that his experience with his service provider was that they're not happy with these new requirements. And I just want to say that the BITS (Banking Industry Technology Secretariat) arm of the Bankers Roundtable has been very active in bringing the vendors to the table to lay out what they need to do for the bank, for the banking industry, I should say. And one of the things that we've found is that, or at least what I found, is that the same vendor was telling multiple financial institutions that no one else was asking for this. So you know, it's just something to take note of. And also I think that that individual would benefit from going to the BITS site [www.bitsinfo.org] and looking at some of the opportunities we're providing for the vendors to be involved in this. And they are very well aware of the requirements, and the framework that this group developed certainly does provide some very clear guidance. And those efforts are continuing to take place. Thank you very much.

Mr. Tatera: Thank you very much. And we have six calls left in the queue. We have 12 minutes left in the program. Let's go to Jack's site in Fairfield, Texas. Go ahead, please.

Texas: Yes, our question is, we have an affiliate bank that we're looking to move our core processing to, and we're curious as to the level of due diligence needed and the contents of a contract, when you're doing it with a sister bank owned by the same holding company.

Mr. Gillespie: This is Jeff Gillespie. We would generally say that the standards for affiliated service providers are basically the same as for nonaffiliated. Now, how the standards are applied is a different issue. But let me speak to the standards. Really you have to look at 501(b), Gramm–Leach–Bliley, the requirement that the contract require implementation of a security program. We think that applies to affiliated entities. The OCC's guidance on third-party relationships certainly applies to affiliates. And finally, when you're thinking about affiliates, keep in mind that there's section 23b of the Federal Reserve Act, which says that in transactions with affiliates, including servicing transactions, they must be on terms that are substantially the same or at least as favorable to the bank as those prevailing at the time for comparable transactions with nonaffiliates. So I think when you combine all three of those, certainly the guidance that is out there is very pertinent to affiliate relationships.

Mr. Tatera: Does that answer your question? Alright, we'll move on then to Richard's site in Chelmsford, Massachusetts. Go ahead, please.

Massachusetts: Yes, I enjoyed both the presentations today. I listened to the one yesterday. There was one comment, two questions. First, a comment. There were people yesterday and today who are looking for some teeth in this guidance. And I think the keyword I've heard is "requirement." And to the extent that the OCC can help bring out that message that it is in the best interest of banks to use this as a safe and sound measurement practice, that'd be great.

Number two—to the vendors—that it is in their best interest to help the banking industry. To actually provide this information would be terrific.

The question I have is, to what extent in researching the third party's ownership of their own technology does one have to go, if one finds out that the third party itself substantially licenses key technology from yet other third-party providers who might be foreign-based?

Mr. Gillespie: This is Jeff Gillespie. I think that's a very complicated issue, but it ties in with a recent bulletin we issued on use of foreign-based third-party service providers: that's OCC Bulletin 2002–16. And I would think that, although we're talking about a domestic provider, this issuance also applies to domestic providers that have operations or exposures overseas. I think that if you read 2002–16 and apply it to your situation, you'll find that there is some good thinking there. We are not highly specific on this issue, because there's so much variation among the different countries in terms of what sort of country exposure and legal exposures exist. Mike has some additional thoughts.

Mr. Koll: I would just say from a common-sense standpoint that we would put the onus back onto the bank on this question a little bit. You've become aware that the third-party company that you're going to contract with, or thinking about contracting with, gets a significant amount of help from a foreign company. Are you nervous about that? What do you need to make you comfortable? What information do you want to get from the service provider to help you make that relationship part of what the relationship is you're looking at. Those are the kinds of things we as examiners would go back to the bank with, and we'd ask those questions and look at it from that kind of a common-sense approach.

Mr. Tatera: Does that answer your question?

Massachusetts: Yes, very good.

Mr. Tatera: Alright. Thank you very much for your call. Rand's site, St. Louis, Missouri. Go ahead, please.

Missouri: Yes, I think that the gentleman who spoke just a second ago pretty much answered my question, but first of all I want to say that my overall impression of this seminar is that it was great. It covered a lot of things that should not be taken for granted and should be second nature. My question is, if there is liability in a third-party vendor using software without proper licensing, is that a risk for the community bank employing the third-party vendor?

Mr. Gillespie: This is Jeff Gillespie. This tends to go back to the point that we raise in 2001–47 with respect to reviewing indemnification provisions in contracts. And I strongly encourage you, when you're entering into a contract, have your lawyers involved and have them look at the indemnification provisions. In some cases we've seen instances where service providers try to shift risk over to customer banks for activities that the service provider is primarily liable on. That is problematic for a number of reasons, not the least of which because it creates a "moral hazard," where the service provider has less incentive to check to make sure that they're operating in conformance with legal requirements.

Mr. Tatera: Alright, thank you very much for your call. We have three calls left in the queue. And 5 and a half minutes left in the program. Let's try Jane's site in Denver, Colorado. Go ahead, please.

Colorado: Hi, this is Janet. I have a couple of questions. First of all, in the actual review of the vendors—we're already doing much of this and are certainly going back through our contracts to make sure that we have the necessary items. And we've been including financial review, both current and previous-year comparisons, all of the contractual items that you've mentioned with the exception of the insurance adequacy and we're adding that, quality and frequency of releases, user group participation. The things that we're now asking for, and I'm talking about two primary vendors, one would be our mainframe software vendor—we're an in-house processor—but our software vendor, and then our card processor and/or ATM switch processor. And I guess my feeling is that we need to add some monitoring for their controls over our customer information, over card stock, things like that, as well as obtain a statement from them, stating that they do comply with GLBA. My question is, are those the things that you feel we need to add? Do you have any insight as to how to go about asking for those, or what exactly we're

looking for? And then as far as insurance adequacy, I think we know some of the questions to ask; I don't know that we have all the details of their business to be able to make a true risk assessment as to whether their insurance coverage is adequate. Do you have any insights there?

Mr. Gillespie: This is Jeff Gillespie. Let me address the GLBA issues first. GLBA is quite clear that the bank in its contract with the service provider has to have a provision that the service provider handling the nonpublic customer information will implement appropriate measures designed to meet the objectives of the guidelines. So that should be in your contract. It shouldn't just be a statement. It should actually be in your contract.

The other thing to keep in mind is privacy. The banking agencies have recommended that the contract must have a provision limiting the service provider's disclosure and use of customer information. So those are two things that really should be in your contract. Just mere statements are not enough, I would say. And I'm going to open the floor now to other people who might want to comment on insurance or other issues.

Mr. Spurgin: Janet, this is Kirk. With regard to insurance, we were just trying to make the general point that a bank should review the vendor's coverage, just in general, relating to such things as fidelity, fire, liability, errors and omissions, protection of documents in transit—those types of things. Now in terms of giving you specific ideas as to sufficiency coverage and things like that, I don't know that we have very much guidance there. I would recommend that you talk to the bank's insurance provider and see if they could give you some guidance as to what types of specific coverages you should be looking for and things of that nature.

Colorado: OK, thank you. And I just have one other quick question. We are somewhat at a loss as to how to go about monitoring the security and control processes of our telecommunications vendors, and obviously that's a big piece of that. And are there any insights there?

Mr. Koll: Janet, this is Mike. You're definitely in a large group when you talk about not being comfortable with the monitoring ability of the telecommunication providers. It's an area we

continue to work on, but I'm afraid there aren't really a lot of concrete suggestions we can give you at this time.

Colorado: OK, and in most cases we have no contracts like you would with another kind of vendor.

Mr. Koll: Right.

Colorado: OK, alright. Thank you.

Mr. Tatera: Thank you very much for your call. Ladies and gentlemen, we are out of time. We have 30 seconds left—time enough for a closing comment.

Mr. Spurgin: Thanks, Ted. This is Kirk. I really appreciate everybody's time and attendance today. You've asked some very good questions. We hope that the seminar was informative and beneficial for you. If you have any additional questions that you couldn't get to, we would recommend that you contact your supervisory office or examiner-in-charge. They're going to be the folks who are most familiar with your bank and your circumstances and can probably offer the best advice. And they can consult with us here at Headquarters if they need additional consultation. Again, we thank you for your attendance today. We hope that it was beneficial. And we hope that you will join us on future seminars. Thanks a lot.

Mr. Tatera: Thank you, Comptroller Hawke, Kirk Spurgin, Greg Isaacs, Mike Koll, and Jeff Gillespie for your excellent presentation. I'd again like to remind our participants to please carefully fill out the evaluation form that was included with your written materials and fax it using your machine's fine or superfine setting to the number listed on the page. The information that you provide is very important to this program as well as any future programs. We'd like to thank you very much for joining us. This concludes our program. You may now disconnect.