

FDIC New York Regional Office
Regulatory Conference Call
“Managing Third Party Risk”
Moderator: George Small
March 3, 2011
1:00 pm CT

Coordinator: Welcome and thank you for standing by. At this time all participants are in a listen-only mode. After the presentation we will conduct a question and answer session. To ask a question please press star then 1. You will be prompted to record your first and last name. Today's conference is being recorded. If there are any objections please disconnect at this time.

I would now like to introduce your host for today's conference, Dan Frye.

Daniel Frye: Thank you, (Dorie). Good afternoon everyone. My name is Dan Frye and I'm the Acting Regional Director for the FDIC's New York region. It's my pleasure to welcome you to today's regulatory conference call. We'll cover a topic that has both risk and management and consumer compliance implications. Going forward we plan to conduct calls like this on a quarterly basis if the industry finds them helpful.

In June 2008 the FDIC issued a Financial Institution Letter, or a FIL as we call them, entitled Guidance for Managing Third Party Risk. In November of that year another FIL was issued that provided guidance on Payment Processor Relationships. Today we will cover a variety of issues including the potential risks arising from third-party relationships, the risk management process, and the FDIC's supervision of third-party relationships. We hope this call will provide helpful information to assist your bank in mitigating any risk associated with your relationships with third-parties.

We appreciate very much your participation on today's call. Your telephone confirmation notice included an agenda for today's presentation as well as a slide deck for the various topics being discussed. The slides should assist you in following today's presentation and can be used for future reference. If you have any questions related to the presentation, you may contact the individuals listed at the end of the deck.

There will be a question and answer session following the formal presentation. And please note that you can also email questions at any time during the presentation to nycalls -- one word -- @fdic.gov. At the end of the presentation the operator will provide procedures for calling in a question.

Joining me today to deliver this presentation is Senior Review Examiner for Compliance Sherry Antonellis and Supervisory Examiner for Risk Management Colleen Marano. Also with us today to address any questions related to Information Technology, Examination Specialist Stephanie Williams.

Thanks once again for participating in this call. Without further ado I will now turn the program over to Colleen who will begin the discussion.

Colleen Marano: Thanks again. Good afternoon everyone. First I would like to quickly go over the agenda for today's call and that's on Slide 3. We will start by giving you some background information about third-party relationships and then talk about some of the potential risks that can arise from those relationships. Next we will cover the risk management process as it relates to third-party relationships and review the requirements of the Bank Services Company Act. Then lastly we'll discuss FDIC's supervision of third-party relationships.

Please take note of any questions that may come up during the presentation. Dan provided the email address for submitting questions that may arise during our talk and we'll have a question and answer session at the end of the presentation. The next slide please.

To begin I'd like to talk about what we mean when discussing third-party relationships and the risks associated with those relationships. We will define third-party relationships, discuss what banks commonly use third-parties for, and really focus on appropriate risk management processes for third-party relationships.

Let's move to Slide 5. Third-party relationships as we speak about them today are broadly defined as entities with which financial institutions have entered into a business relationship. These entities can be bank or non-bank, affiliated or non-affiliated, regulated or non-regulated, or domestic or foreign. Financial institutions often use third-parties to help facilitate customer access to bank services or products or to perform functions on their behalf.

Examples of third-party relationships could include for instance a company that markets a (stored) value card on behalf of the bank or a corporation that provides loan review services for the financial institution. Other examples include third-party relationships designed to perform functions more traditionally handled by the financial institution such as loan operations or call centers, infrastructure support, IT, and audit functions. Slide 6 shows common third-party relationships.

The use of third parties can assist a bank's management in attaining strategic objectives by increasing revenues or reducing costs. It can also serve as a vehicle for management to access expertise or efficiencies for a particular activity. Such use of third-parties can also have the benefit of freeing up

resources for other projects, can reduce time to market and allow for 24-hour access to particular bank services.

Any decision to enter into a third-party arrangement should first be considered by the board of directors and senior management. Remember though that the use of third-parties does not negate or lessen the bank and management's - the board and management's responsibility to ensure that activities conducted on a third-party arrangement are being conducted in a safe and sound manner and comply with applicable laws, regulations, and guidance as well as the banks own internal policies.

Today our goal is to provide you with a general framework for implementing an effective third-party risk management process. Transactions and affiliates subject to 23A and B of the Federal Reserve Act will not be addressed in this presentation. In addition, our presentation is not meant to replace or supersede any previously issued FDIC guidance on third-party risk.

We do hope that through today's presentation you will be able to gain more insight into the FDIC's view on managing third-party arrangements and their associated risks and apply that insight to controlling third-party risks in your own institutions.

So let's go to Slide 7. Now that I've covered the background of third-parties and relationships with institutions, I'd like to talk about the potential risks associated with these relationships and provide some practical examples. Numerous risks can arise from financial institutions relationships or arrangements with third-parties. Failure to manage these risks could potentially harm the institution through financial loss, reputation risk, supervisory actions, and loss of customer relationships.

Keep in mind when you - we discuss third party risk that not all risks will necessarily apply to each third-party relationship. The financial institutions' board of directors and senior management are responsible for understanding the nature of these risks and their potential impact before entering into the third-party arrangement.

Let me summarize some major third-party risks and these are not considered all inclusive. First let's discuss strategic risk. Strategic risk can occur when a financial institution fails to implement appropriate business decisions that are consistent with the institution's strategic goals. Such exposure can occur when the financial institution uses a third party to perform functions or services that do not assist with achieving corporate strategic goals or don't provide adequate return on investment.

For example, say that a financial institution uses a third party for marketing consumer loans. If that agreement is not developed appropriately and the contract structured properly, or if the relationship is not correctly managed once established, consumer loan growth could well exceed the institution's strategic plans for growth intended in that portfolio.

In addition, the board may have expressly prohibited certain types of lending such as subprime borrowers, but the third party might have a different understanding of what constitutes subprime. These strategic risks could manifest in additional risks such as capital problems or problems in achieving other board approved strategic goals.

Reputation risk is another potential third-party risk. This is a risk of negative public opinion about your institution. This could occur when a third-party relationship results in dissatisfied customers, interactions that are inconsistent with institution policies, inappropriate recommendations, security breaches,

and violations of law. Also keep in mind that negative publicity of any third party with which the institution has dealings could also harm the reputation of the bank if that relationship is publicly known and it could possibly lead to litigation.

An example of reputation risk would be if a third party handles private customer information for the bank and such information was compromised due to the third party's failure to provide adequate internal controls. Reputation risk is closely tied to **compliance, legal, and liquidity risks**.

The next risk to consider is operational risk. Operational risk is very closely tied to transaction risk, which will be covered next. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

An example would be if a bank has a contract with a third party to service all inbound customer service calls and this might include requests for a loan application and reports of lost or stolen debit cards. If some unforeseen act of God event impacted that services ability to respond to callers for an extended period of time, what would this impact be to the institution if the service provider did not have appropriate contingency plans in place?

This scenario also ties into transaction risk which could occur when problems are encountered with service or product delivery by the third party. The institution can become exposed to this risk when a third party fails to perform as expected for such reasons as inadequate capacity, technological failure, human error, or even fraud.

Good contingency and business resumption planning can help minimize transaction and operational risks. It is vitally important that proper controls are

- over technology used in third-party arrangements are in place. A lack of such controls could result in threats to the security and integrity of systems and resources which could lead to unauthorized transactions or the inability to transact business as expected.

For example, where a bank has a contract with a third-party payment processor, situations can arise where the bank ultimately processes transactions for hundreds of merchants because its third-party partner is using the established deposit account at the bank to initiate ACH transactions and to deposit remotely created checks for its own merchant clients. This situation can significantly increase transaction risk, among other risks, because the volume of transactions processed both in number and dollar volumes becomes significantly larger than ever intended.

Additional risk exists where the bank is unaware of the products, services in which the underlying merchants are involved. If such activities are somehow fraudulent or illegal, then the legal, compliance, and reputation risks are magnified.

Credit risk may also arise from third-party arrangements. Credit risk is the risk that a third party or any other creditor necessary to the third-party relationship is unable to meet the terms of the contractual arrangement with the financial institution or to perform financially as agreed. In its most basic form credit risk is the financial condition of the third party itself.

In some third-party arrangements the contract provides that the third party insures some measure of performance related to the obligations arising from the relationship such as loan origination programs. In this case, credit risk would be a factor in assessing overall third-party risk. The use of third parties that market or originate certain types of loans, solicit and refer customers,

conduct underrating analysis, or set up product programs for the bank could also result in credit risk.

Liquidity risks or funding risks can be elevated as a result of third-party relationships. By its very basic definition, liquidity is the risk that assets cannot convert to cash or that access to borrowing is interrupted.

With third-party activities such as merchant processing, the acquiring bank has settlement exposure if they pay the merchant or fund transactions before receiving credit from the issuing bank. Merchants are often required to maintain deposits at the bank for this settlement. If the acquiring bank relies on such deposits as funding for other activities, another exposure arises because these deposits are not stable sources of funding. Also if there are substantial chargebacks by one or more merchants and the bank's financial condition or reputation becomes strained, access to borrowing lines could tighten or may even become unavailable.

Sherry Antonellis will now finish discussing potential risks and then move on to the risk management process.

Sherry Antonellis: Thank you, Colleen. Compliance risk exists when the products or activities of a third party are not consistent with governing laws, rules, regulations, polices, or ethical standards. This risk usually increases when an institution has not taken third-party oversight into consideration in developing its compliance management system or CMS. The general tenets of a successful CMS at the bank level such as board and senior management oversight, monitoring, audit and training must also be applied to any third-party relationships that have consumer protection implications.

For example, if a bank contracts with a third party to market its credit cards; management must take steps with the third party to ensure compliance with consumer protection law and regulations just as they would for the bank. This would include regular monitoring of promotional and marketing materials and Web sites, review of the marketer's compliance audits, and monitoring complaint trends for potential issues.

With marketers there should be particular concern with compliance with Section 5 of the Federal Trade Commission or FTC Act as it relates to unfair or deceptive practices. The FDIC has seen numerous cases where such violations have occurred under these circumstances.

Another example with high levels of compliance risk would be a scenario in which a bank has contracted with a third party to take loan applications on its behalf. This is particularly true where Internet applications are involved. We have seen many situations where third parties are taking Internet applications for consumer loans where consumers are asked for prohibited information, such as gender, in violation of the Equal Credit Opportunity Act and Federal Reserve Board Regulation B.

Any bank involved in relationships where compliance risk is present must ensure that such activities are being overseen as part of the banks CMS. The level of such oversight is dependent upon the level of compliance risk involved in the relationship.

Legal risk can occur in a third-party relationship if the third party does not adhere to applicable law and regulation or to the terms of the contract with the financial institution thereby exposing the institution to potential legal and/or regulatory action.

The previously mentioned scenario involving payment processors is also a good example of potential legal risk in a third-party relationship. If merchants utilizing the payment processor to move consumer funds through the deposit account at the institution are involved in illegal activities that harm consumers, this would expose the bank to potential legal action. Examples of this would be foreclosure scams or certain payday type lenders that utilize these types of payment processors to receive payments from consumers who are ultimately harmed by these activities.

When an insured depository institution is used to facilitate these payments, it becomes exposed to potential legal action for involvement in the fraudulent or defective activities. Awareness of the activities of the clients of such payment processors is key to mitigating such risk.

Another consumer protection as well as IT concern is the ability of third parties to maintain the privacy or customer records and to implement an appropriate information security and disclosure program. The financial institution could face liability issues when such third parties have security breaches involving customer information resulting in violation of the safeguarding of customer information standards under FDIC and FTC regulations. This is much like the example provided during the discussion of reputation risk.

Other risks also exist when entering into third-party arrangements and can only be fully determined through a complete understanding and assessment of the resulting arrangement. In addition to the risks we've already discussed here today, possible additional risks could include counterparty, interest rate, price, foreign currency translation, and country risks.

Another factor in third-party oversight that we wanted to mention today that we believe bankers should be aware of is that of institution affiliated parties or IAPs. Under Section 3(u) of the Federal Deposit Insurance Act, or FDI Act, certain third parties with which a bank has established a relationship may be considered an IAP by the FDIC. FDIC is permitted to examine affiliates of insured banks as needed to disclose the relationship between the bank and the given affiliate as well as the effect of that relationship on the bank.

The term IAP encompasses any company that controls, is controlled by, or is under common control with another company. Therefore whether wholly owned or not, a third party could be considered an IAP of the bank for the purposes of the FDI Act. If a third party is determined to be an IAP, this primarily means that the FDIC may pursue enforcement action directly against the third party under Section 8 of the FDI Act and any violation with law or regulation committed by the IAP will be included in the banks report of examination.

We're now moving on to Slide 8. Now that you have an understanding of the potential risks of using third parties, we are going to discuss the risk management processes that you need to have in place to control that risk. Third-party entities may assist management and the board in achieving strategic goals, but such arrangements also reduce management's direct control over the situation. Therefore the use of the third party increases the need for an effective risk management process.

The four main elements of an effective third-party risk management process are risk assessment, due diligence, appropriate contract structuring and review, and oversight. These four elements apply to any third-party activity, but the precise use of this process is dependent upon the nature of the third-

party relationship, the scope and magnitude of the activity, and the risks identified within the relationship.

This process will provide a framework for assessing, measuring, monitoring, and controlling risks associated with third parties. A comprehensive risk management process will enable management of the institution to ensure that capital is sufficient to support the institution's risk exposures and that the third party is operating in a manner consistent with applicable laws, rules, regulations, and guidance, including those intended to protect consumers.

Colleen and I will now provide an overview of each of these four elements in the process, the first of which is the risk assessment. And we are now moving to Slide 9.

A risk assessment is fundamental to the initial decision of whether or not to enter into a third-party relationship. The first step in the risk assessment process should be to ensure that the proposed relationship is consistent with the institution's strategic planning and overall business strategy.

Next management should analyze the benefits, costs, legal aspects, and the potential risks associated with the third party under consideration. It is key for management to develop a thorough understanding of what the proposed relationship will accomplish for the institution and why the use of a third party is in the institution's best interest.

A risk/reward analysis should be performed for significant matters comparing the proposed third-party relationship to other methods of performing the activity or product offering, including the use of other vendors or performing the function in-house. Such analysis should be reviewed by the board or an appropriate committee.

Certain aspects of the risk management risk assessment phase may include the use of internal auditors, compliance officers, technology officers, and legal counsel. This phase should also identify performance criteria, internal controls, reporting needs, and contractual requirements that would be critical to the ongoing assessment and control of specific identified risks.

For example, if the activity involves consumer products and services, the board and management should establish a clear strategy that allows for assessment of compliance with applicable laws, regulations, and guidance as well as a mechanism for midcourse corrections if necessary. In addition, assessing the best method of providing information security and meeting customer privacy requirements should not be overlooked during this phase of the process.

After completing the general assessment of risks, management should review its ability to provide adequate oversight and management of the proposed third-party relationship on an ongoing basis. For significant third-party relationships, the board may consider appointing a senior manager to be responsible for the relationship, including due diligence, implementation, ongoing oversight, and periodic reporting to the board.

A final part of the risk assessment phase involves carefully estimating the long-term financial effect of the proposed third-party relationship. The board should take into account all aspects of the long-term potential with the relationship as well as the managerial expertise and other associated costs that would result from the decision to use a third party and not be unduly influenced only by short-term cost savings.

We're now moving on to Slide 10. If the results of the risk assessment result in a decision to proceed with a plan to establish a third-party relationship, management must move on to the next step in the process, selecting a qualified entity or entities to implement the activity or program through the due diligence process.

Due diligence provides management with the information needed to address the qualitative and quantitative aspects of potential third parties to determine if a relationship would help achieve the institution's strategic and financial goals as well as mitigate identified risks. Not only should due diligence be performed prior to selecting a third party, but it should also be performed on an ongoing basis during the course of the relationship, particularly when events occur that change the risk profile of the relationship.

The scope and depth of due diligence is directly related to the importance and magnitude of the institution's relationship with the third party. For example, large-scale highly visible programs or programs dealing with sensitive data vital to the institution's success warrant an in-depth review of the potential third party while the due diligence process for isolated low-risk third-party activities would be much less comprehensive. The results of your risk assessment would help to determine how due diligence efforts should proceed.

Comprehensive due diligence involves the review of all available information about a potential third party, focusing on the entity's financial condition, specific relevant experience, knowledge of and compliance with applicable laws, regulations and guidance, its reputation, and the scope and effectiveness of its operations and controls. A checklist approach is not sufficient. An institution should have qualitative due diligence standards to which it routinely adheres and that clearly indicate when a third party under consideration should be rejected.

The evaluation of a third party may include the following elements: Financial indicators such as audited financial statements, annual reports, and FTC filings; the significance of the contract on the third party's financial condition; the experience and ability of the company and its principals; the third party's business reputation; the third party's strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies, the existence of any complaints, regulatory actions, or litigation against the company and/or its principals or affiliates. During this process it is worth researching affiliates and different naming conventions as some third parties could attempt to circumvent applicable law and regulations in this way.

The ability to perform using current systems and with potential additional investment required; the use of subcontractors and any other third parties the bank may not directly contract with, including who those entities are and what they will do; the scope of controls, privacy protections, and audit coverage; the company's business continuity strategy and plans.

Knowledge of relevant consumer protection laws, regulations, and guidance; the adequacy of management information systems; the existence and adequacy of programs to ensure compliance with applicable laws, regulations, and guidance; references from existing and former business partners and clients; appropriate and required licensing and registration at both the state and federal levels as well as all forms of appropriate insurance coverage.

I will now turn the call - the program back to Colleen to discuss the third step in the process which is contract structuring and review.

Colleen Marano: Thanks Sherry. The third element of the risk management process is contracting and I'm on Slide 11. Management should ensure that the specific

expectations and obligations of both the institution and the third party are outlined in a written contract.

For material third-party arrangements appropriate legal counsel should review the contracts and the board should approve the third-party arrangement prior to finalization. Also any material or significant contracts should prohibit assignment, transfer, or subcontracting by the third party of its obligation to another entity unless and until management can determine that such action would not negatively affect the institution. The same due diligence standard previously discussed by Sherry should apply to any other third-party entity.

The level of detail in contract provisions will vary with the scope and risks associated with the third-party relationships. The following items should be considered as a contract is structured, but each item is dependent upon the nature and significance of the third-party relationship.

The contract should clearly set forth the rights and responsibilities of each party to the contract and include the following: Timeframe covered by the contract; the frequency, format and specification of the service or product to be provided; other services to be provided by the third party such as support maintenance, training, and customer service; requirements that the third party comply with all applicable laws, regulations, and guidance; authorization for the institution and the appropriate audit, legal, and regulatory agencies to access records of the third party, especially those necessary to evaluate compliance with laws, rules, and regulations.

Identification of which party is responsible for delivering any required customer disclosures; insurance coverage to be maintained by the third party; terms relating to and use of any bank premises, equipment, or employees; permissibility or prohibition of the third party to subcontract or use another

party to meet its contractual obligations and any notice or approval requirements; authorizations for the institution to monitor and periodically review the third party for compliance with this agreement, including audit reports; and indemnification of liability of each party for the actions of the other.

The contract should outline the fees to be paid, including fixed compensation, variable charges, and fees for non-recurring items or special requests. Other items that should be addressed, if applicable, are the responsibility for purchasing and maintaining equipment, including hardware, software and other items. Also the party responsible for payment of any legal or audit expenses should be identified.

Financial institutions should employ compensations that are consistent with sound banking practice and consumer protection laws. Compensation should be structured to promote long-term performance in a safe and sound manner. Any volume and short-term incentives should be strictly controlled, and in the area of loan originations, this will be of particular regulatory concern. The FDIC expressly discourages the use of arrangements which may encourage third-party originators to inappropriately steer borrowers into higher cost products.

Clearly defined performance standards should be included in certain contracts to serve as a basis for measuring the third party's performance and may be used as a factor in some compensation arrangements. Industry standard may be used or standards may be set to reflect a particular relationship. For example, contracts with appraisers should contain language outlining the appraisal industry standards the work must meet. Management should periodically review the performance measures to ensure its objectives are being met.

The contract should specify the type and frequency of management information reports to be received and these reports should include routine reports such as performance reports and audits, financial reports, security reports, and business resumption testing results. Management may also want to consider mandating exception-based reports. These would serve as notification of changes or problems that might affect the nature of the relationship or impose risk to the financial institution. In addition to the types and frequency of audit reports that the institution is entitled to receive, the contract should also specify the institution's right to audit the third party as needed to monitor performance under the contract.

The contract should prohibit third parties from using or disclosing the institution's information except as necessary to perform the functions designated by the contract. The institution's non-public personal information must be handled consistent with the institution's privacy policy and applicable privacy laws and regulations. The contract should require prompt and full disclosure of any breaches of security and - or confidentiality of the information.

Moving on to Slide 12, the contract should specify who will respond to complaints from the institution's customers that the third party receives. If the third party is responsible, a copy of the complaint and the response should be forward to the institution. Also periodic summary reports detailing the status and resolution of complaints should be provided.

The contract should address the third party's responsibility for continuance of services in the event of an operational failure. Third parties should have appropriate protection for backing up information and should maintain disaster recovery and contingency plans with sufficiently detailed operating

procedures. The institution should receive the results of business continuity plan tests.

To mitigate risks associated with contract default and/or terminations, the contract should address these issues as well. There needs to be an understanding of what circumstances constitute default. It needs to identify remedies and provide a reasonable opportunity to cure the default. Similarly, termination rights should be identified in the contract.

Related to the risks associated with default and termination is a question about ownership of the institution's property, including data, equipment, software, and intellectual property such as the institution's name and logo, trademark, and other copyrighted material. The contract should also address ownership and control of any records generated by the third party.

Indemnification provisions require a third party to hold the institution harmless from liability as a result of negligence by the third party and vice-versa. Such a provision may reduce the potential for the institution to be held liable for claims arising from third-party negligence, however, such provisions cannot shift the ultimate responsibility to conduct banking and related activities in a safe and sound manner and in compliance with laws and regulations and sound banking principals to the third party. It is the responsibility of the institutions.

Also the existence of such provisions will not be a mitigating factor where deficiencies indicate the need to seek corrective action, such as for violations of consumer protection or other laws and regulations. The FDIC's consideration of remedial measures, including restitution orders, is made irrespective of the existence of indemnification clauses in third-party contracts as was discussed in the compliance risk example earlier by Sherry.

Many third parties attempt to contractually limit the amount of liability that it incurs as a result of a relationship with an institution. For example, it was not uncommon in the late 90s for Internet banking third-party service contracts to absolve the servicer of all liability for the services that they provided for the institutions. So before entering into such a contract, institution management should consider whether the proposed damage limitation is reasonable compared to the amount of loss the institution could experience if the third party fails to adequately perform.

Sherry will now discuss the key supervisory issues related to the use of third-party relationships at your institution.

Sherry Antonellis: Thank you Colleen. We're now moving on to Slide 13. The fourth element of an effective third-party risk management process is adequate oversight of third-party activities and adequate quality control over those products and services provided through third-party arrangements. This will serve to minimize exposure to potential financial loss, reputational damage, and supervisory action.

Management should provide for ongoing review of the third party's operations in order to verify that they are consistent with the terms of the written agreement and that identified risks are being controlled. The institution's CMS should also ensure that the third party's continued compliance with applicable law, regulation, and guidance continues as well as internal policies and procedures of the institution. Unfortunately the FDIC has seen numerous cases where institutions have failed to include consumer protection considerations within their third party oversight efforts.

The board should also be involved in the oversight of significant third parties and should ensure that management is providing appropriate ongoing monitoring. The institution may consider designating a specific officer to coordinate the oversight activities and involve compliance and other operational areas such as audit and information technology as necessary within the monitoring process. The extent of oversight of a particular third party will depend upon the potential risks, the scope and magnitude of the arrangement, and these are all dependent upon the results of your risk assessment.

An effective oversight program will generally include monitoring of the third party's quality of service, risk management practices, financial condition, and applicable controls and reports. Results of oversight activities should be periodically reported to the institution's board or designated committee. If weaknesses are identified, they should be documented and promptly addressed.

An institution's ongoing monitoring efforts should really be directed by the risk assessment just as initial due diligence efforts are. Once completed, the initial risk assessment should not become obsolete. This assessment should be a living document that is constantly adapted to reflect the changing risk profile of the third-party relationship.

Such risks would include new products or services, new laws, regulations or guidance, new geographic or demographic markets, new software or hardware, the use of new subcontractors, and new marketing or promotional methods. These are all considerations that can impact the risk profile of the relationship and should therefore trigger a revision of the existing risk assessment. This revised risk assessment should then be the basis for your ongoing due diligence and monitoring efforts.

Performance monitoring should include, as appropriate, the following elements: An evaluation of the overall effectiveness of the third-party relationship and consistency with the institution's strategic goals; a review of licensing and/or registrations on an ongoing basis to assure that the third party can legally perform the services or offer the products that it's doing.

An annual evaluation of the third party's financial condition; a review of the adequacy of the third party's insurance coverage; a review of audit reports or monitoring reports of the third party with follow-up on needed corrective actions. There should also be a review of the scope of the audit and monitoring as well as the work paper to ensure that it was sufficient to detect possible issues.

Monitor for compliance with applicable laws, regulation, and guidance. A review of the third party's business resumption contingency planning and testing; an assessment of the effect of any changes in key third party personnel; a review of the third party's performance in the context of contractual requirements and performance standards with appropriate follow-up as needed; a determination of the adequacy of any training provided to employees of the institution.

The results of the testing program or programs for third parties who have direct interaction with customers; periodic reviews of customer complaints related to the products and services provided by the third party, including resolution of those complaints; performance of onsite visits, the results of which should be documented; and finally, meeting as needed with representatives of the third party to discuss performance and operational issues.

The bank should retain proper documentation as evidence of this monitoring and of management of the risks associated with the third-party relationship. These should include items such as valid contracts, business plans, risk analyses, due diligence reports, and oversight activities, including reports to the board or delegated committees. Additionally, any dispute resolution documents should also be retained.

We're now moving to Slide 14 and the Bank Service Company Act. Another factor relevant to third-party oversight is the requirements of the Bank Service Company Act. Section 7 of the Act requires institutions to notify their primary federal regulator in writing within 30 days of contract of relationships with third parties which provide certain services to the institution. These services include check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices and similar items, or any other clerical, bookkeeping, accounting, statistical or similar functions performed for the depository institution.

FDIC Form 6120/06 may be used to satisfy this notice requirement. The form contains identification, location, and contact information for the bank, the servicer, and a description of the services provided. In lieu of the form, notification may be provided by letter. Either the form or the letter containing the notice information must be submitted to the Regional Director, Division of Risk Management of the region in which the bank's main office is located. You may refer to Financial Institution Letter or FIL-49-99 dated June 3, 1999, for further information on this topic.

Colleen will now conclude with the final section of our prepared presentation which addresses how FDIC approaches its supervision of third-party relationships.

Colleen Marano: Let's move to Slide 15. A financial institution's board of directors and senior management are responsible for identifying and controlling risks arising from third-party relationships to the same extent as if the third-party activities were handled within the institution. While your institution may seek to mitigate third-party relationship risks through the use of indemnity agreements or other contract provisions, this does not relieve the institution, management, and the board of directors from the ultimate responsibility for operating the institution in a safe and sound manner and in compliance with laws and regulations.

The FDIC reviews a financial institution's management of significant third-party relationships in the context of the normal supervisory process. Third-party arrangements are reviewed during FDIC safety and soundness, (plus) BSA and information technology examinations. Such arrangements are also evaluated during compliance examinations to ensure the products, services, and activities of the third party comply with consumer protection laws, regulations, and guidance.

FDIC examiners will focus on your institution's documentation of management processes for identifying, measuring, monitoring, and controlling risks associated with the use of significant third-party relationships. The depth of the examination review will depend on the scope of activities conducted by the third party and the degree of risk associated with the activity in the relationship.

Examiners may request and review contracts, policies, procedures, activity reports, and other relevant records which management has used to select, monitor, and manage significant third-party relationships. This means that the examiners will closely review the risk assessment as well as the initial and ongoing due diligence performed by management. Depending on the products

or services offered or marketed by the third party, examiners may also perform account level testing to review for performance and assess mitigation of the risks previously discussed.

Examiners may use various tools to facilitate the examination of different activities. For example, the FFIEC Outsourcing Technology Services and the Supervision of Technology Service Providers IT handbooks are used.

FDIC also revised its IT Officer's Questionnaire to incorporate an entire section on vendor management and service provider oversight. The revised questionnaire asks banks if they have an adequate vendor management program, if they have reported their service provider relationships, if providers were located outside the US, if agreements require vendors to satisfy all applicable laws and regulations, if providers are required to implement measures to satisfy the interagency guidelines establishing information security standards, and if the institution has appropriate measures to monitor compliance.

Examiner findings and recommendations will be addressed as needed in the report of exams. Examination findings from third party reviews will typically be factored into the management component rating due to the propensity of findings related to the compliance area, but they may also be factored into other component ratings such as capital, earnings, asset quality, liquidity, interest rate sensitivity, and the composite rating, as well as the institution's compliance with laws and regulations.

Appropriate corrective actions, including enforcement actions and restitution orders, may be pursued for deficiencies related to third-party relationships which pose a safety and soundness or compliance management concern or for deficiencies which result in violations of applicable laws and regulations.

Remember, third party contract provisions or indemnity clauses will not insulate your institution from such corrective actions.

That concludes our prepared remarks from the slide deck. I'll turn the program back over to Dan.

Daniel Frye: Thank you Colleen and thank you Sherry for your remarks. We're now going to go to the question and answer session, but first I'd like to acknowledge that there may be questions from some of you that will require a little more research on our part but there also may be insufficient time to get the whole of your questions today. You can be assured, however, that any question that isn't fully addressed today will be answered by our staff. All registrants for today's presentation will be provided with responses via email where appropriate.

So without any further delay, I'm going to turn the session back over to (Dorie) who will reiterate the procedure for participants to call in your questions. (Dorie).

Coordinator: Thank you. At this time if you would like to ask a question, please press star then 1. You will be prompted to record your first and last name. To withdraw your request, press star 2. Once again, to ask a question press star then 1 now.

We do have a question from the Mizuho Corporate Bank. Your line is open.

Woman: Hi, yes, thank you. I would like you to clarify when you say third party here, I know you have indicated all entities, but I think I would like a clarification on entities. If you actually have different branches in the United States and you are, for example, located in California and you are using a system that is also -

or used by another branch in another state, so would that be considered a third party? Is it nec- you're the same entity, you're just a different branch.

Entity may be defined probably that you are - have the same taxpayer ID, but do you have a different license perhaps, you - or you, of course, you acquire your license if - we are a state chartered bank, so we had to acquire license from our corresponding states. So define entities there from the regulatory perspective. From the examination perspective if you don't have jurisdiction over that state how would you know - how would you examine this bank that is using a product or also a service that is being used by another branch in another state? I hope I'm making sense of this question.

Colleen Marano: I'm not quite sure I do understand exactly the situation, but it sounds like you've asked (us if)...

Woman: May I just - may I interject real quick -- entities, I - instead of saying affiliate it may be a third party, it may say it's a different affiliate? What about just a different branch, but in a different - located in a different state?

Colleen Marano: So it's a branch of your bank crossing state boundaries.

Woman: Yes, exactly.

Colleen Marano: All right. And they are using it sounds like an IT third party?

Woman: Exactly. No, let's say you are using that particular branch's - another branch's product, but is it...

Colleen Marano: Okay. Okay. So it's just...

Woman: Right.

Colleen Marano: ...that that branch is servicing you.

Woman: Yes. And it looks like we're outsourcing from that, yes, exactly.

Colleen Marano: Okay.

Woman: They're servicing ours, yes.

Colleen Marano: Okay. We didn't cover when it's an affiliated type relationship because that's an internal service. That's - so that's an internal process that you're describing here and that technically wasn't covered in what we discussed today.

Woman: Yes.

Colleen Marano: I think an internal audit would handle that because it's an internal process. So you would have a risk assessment from that perspective.

Woman: Okay.

Colleen Marano: So is that process being handled appropriately through what you have set up being an internal entity handling your process. And I don't know what they're processing for you. Does that make sense? I know we're being kind of cryptic here, but does that make sense?

Woman: Yes, I think I can understand what you said, the internal audits responsibility. But that would also depend on how and if you have a different regulators. You know, for example, in different states.

This particular state does not have jurisdiction to that - to another branches and then they cannot - I think they would expect - or (report) in California, they would expect the California branch to make sure that they have conducted some kind of a third party also - almost review, right, of that particular product or service because you - so I see there is an expectation from the examiners in our state to make sure that that service has already been assessed. But is that service considered a third party? That's my question. And do we need to follow the same guidelines?

Colleen Marano: I think the applicability of the guidelines would be less intense, if I can use that terminology, but absolutely from a - from an examination perspective you would need to know that that service is being provided appropriately, it was meeting your needs, and that risks were addressed. So if your own internal audit had met those needs - the question would definitely be asked has that service been looked at by the institution, by the branch, and you would need to reach a comfort level.

Sometimes depending on what the service is, and I still don't know exactly what the service is, maybe there is a SAS 70 that was performed on the entity providing it to your branch - you're using it as the service. I probably would need to know more. But the examiners who examine your institution who need to know, and maybe it does cross regulators, are asking appropriate questions to make sure that the risks are mitigated.

Woman: Yes, that would...

Woman: Okay, that might require something more that may be a more specific question.

Colleen Marano: If you...

Woman: And I think we can...

Colleen Marano: If you want to email the question in to the nycalls box with more specific information, we can address it with more details.

Woman: Sure, we'll - I'll do that.

Colleen Marano: Okay.

Woman: Because like you said, internal audit. Internal audit only depends on your guidelines as well...

Colleen Marano: Okay.

Woman: ...so it would be - you would have to provide, I think, the direction as to how to treat that particular service in a different state. But I will do that. Let me just send you a, I think, an email and I - and the service provided is not just IT, it is actually a service like performed by an operations area for example.

Colleen Marano: Okay. Okay, we'll...

Woman: Okay.

Colleen Marano: ...look at it then. Thank you.

Woman: That's just hypothetical question. Okay.

Colleen Marano: Okay.

Woman: Thank you.

Coordinator: At this time we have no additional questions.

Daniel Frye: While we're waiting for calls, maybe we'll take some of the Internet questions.

Sherry Antonellis: We have an email question, could you tell of any new risks we should be aware of regarding flood map changes for properties which become located in special hazard flood areas?

This is not really a new risk. Basically what happens is that it - over time FEMA, or the Federal Emergency Management Agency, will update the flood maps. What happens then is that a property that was in a flood zone may no longer be in a flood zone or vice-versa. Generally institutions use a third party for this service, a flood determination company, so you would need to have an ongoing - an initial process to determine that they do that, that they monitor the flood maps to provide any changes and that they would update you with those changes.

That's sort of been a risk that's been out there and is an ongoing one, so I don't believe it's new and I'm not aware of any new risks aside from FEMA has been updating maps quite frequently lately. And hopefully that will answer your question.

Man: Okay, we have a question from Banco Santander. It's a two-part question.

The first part, the notification requirement under Section 7 of the Bank Services Company Act, does it include IT contracts when development of software, software licenses, hardware support, et cetera. We don't have the

specifics with us regarding Section 7 of the Bank Services Company Act.
We'll get back to the gentleman that asked that specific question.

The second part of the questions said could you give examples of core processing. Well basically core processing in a bank would consist of loan processing, deposit activity, general ledger activities, and anything to do with the platform services. So those are like four examples of what we consider core processing.

Daniel Frye: (Dorie), do we have any other calls on the line?

Coordinator: Yes, our next question comes from Eastern Bank. Your line is open.

Woman: Thank you. I actually have a question about best practices. In your various examinations have you run across any best practices in how these assessments are done, i.e. are they embedded in other risk management reviews that are being conducted by the compliance groups instead of having distinct vendor management reviews?

For instance, under GLBA, under privacy, if there were a vendor management vendor section embedded in the GLBA review and the assessment was done as it related to privacy controls at the various vendors, if there's a complaint - a consumer complaint review and there's a specific vendor section within that to detect any trends that had occurred or registered complaints. Is the embedding of a vendor management program within existing compliance management systems something you'd recommend?

Sherry Antonellis: Well I think -- that's an excellent question, thank you -- I think that it would depend on how you - your compliance management system functions overall. You know, if your vendor management policies functions, you know, very

outside of your general compliance function, then that might not be a good idea. You know, but whatever works for your institution.

I think that if your compliance system is embedded within your operational procedures, it generally works better if you don't make it a separate, you know, separate risk assessment, a separate entity. If it's included in whatever you do on an everyday basis, it generally makes it easier for people to understand and easier to identify potential risks and also what those mitigators are, if they exist, and where the holes might be.

But I really think it depends a lot on how your compliance management system functions, you know, whether it's centralized, whether it's decentralized. If you have, you know, a number of loan processing offices or a number of different product lines, you might have credit cards, you might have mortgages, commercial lending, it really depends on how your bank functions and what the operations are.

If it's a small bank then I think the embedding is probably a good thing and it probably would be more efficient. But if you have divisions that operate completely separate from each other and differently, then the embedding might not work as well. I know that's not - there's no hard and fast answer and I'm sorry for that, but...

Woman: No that's fine. Thank you.

Sherry Antonellis: Okay. Thank you.

Daniel Frye: (Dorie).

Coordinator: Thank you. Our next question comes from (Danvers Bank). Your line is open.

Man: Yes, can you go over the process for us obtaining FFIEC IT examination reports on our third party processing vendors?

Man: You would need to submit a request to the regional office specifically detailing what it is that you're looking for and we would get back to you. And that is Daniel Frye, Acting Regional Director.

Man: Okay.

Man: And do you have the address...

Man: Yes, I do.

Daniel Frye: Okay, good. And as I understand it, they're not typically forwarded to the banks that are serviced but we will provide them upon request to the institution.

Man: Upon request, that's why I mentioned...

Daniel Frye: Yes, very good.

Man: Yes, I think that's an element of vendor risk management.

Daniel Frye: Sure is. Thank you for the question.

Coordinator: Our next question comes from Franklin Savings Bank. Your line is open.

Man: Thank you. I just have a question with regard to the agreements or the contracts you have with third parties. You listed off a number of matters that

we should take into consideration such as employment agreements or policies that the vendor may have with their own employees and obviously most of our critical vendors are companies like Fiserv or IBM or Dell or what have you and I'm just wondering a bank our size - we don't have a lot of leverage to maybe get that information from companies like that.

So are those matters that are - that you listed at that laundry list, if you will, things that we should just consider as part of the review process or are those matters that we should document where we tried to get the information and we couldn't or - I'm just - it seems like a pretty long list that you went through that should be included in the contract and that the bank should have information on and I'm not sure how we would even have the ability to get some of that.

Colleen Marano: Right. When you review the FIL you'll see that it's listed as those are recommended sections of a contract, provisions to be included in a contract, and it will depend on the vendor you're contracting with or the third party who you're contracting with, so those com- those you've mentioned, Fiserv and IBM, those contracts we do see as being rather standard, so I understand the question, I understand your concerns.

If it needed to be more germane to the institution, those would be provisions you would then rewrite more specifically I think, but as you read the FIL it says consider those provisions per third party, per contract, per services and activities. So it would - you would consider each one independently per contract.

Man: Would it be expected that we would have to document that we considered those in some way or if you come in and you look at the vendor due diligence file and you see the work that has been done, is that going to be satisfactory to the examiners onsite?

Colleen Marano: Yes, I don't think you - there's no checklist approach. I don't think you need to be - have - show that you've lined up the FIL and said we don't have this provision because, we do have this provision because...

Man: Okay.

Colleen Marano: The work you've put in to developing a contract would hopefully be evident in your vendor files.

Man: Okay. Thank you.

Sherry Antonellis: And I think it would depend on your risk assessment as well. We would look to that initially. And if you identify certain risks, we would look to see that you took appropriate action to address them through due diligence and the contract.

Man: Okay, I just wanted - that's very helpful. Thank you. I just wanted to make sure that that would be sufficient and there wouldn't be criticism of the bank for not in some way documenting, even though they couldn't get it, documenting that they couldn't get it and I wouldn't want to have - I wouldn't want to be, if you will, on the hook to try to complete that laundry list as you say or that checklist because it's a lot of work if - for something that you probably can't get in a lot of cases. So thank you.

Sherry Antonellis: You're welcome.

Coordinator: At this time we have no additional questions.

Daniel Frye: Okay, do we have any more email...

Man: No.

Daniel Frye: No email. Well okay, well listen, that concludes our presentation for today and we want to thank you all for participating. We will be posting a written transcript of this call as well as an audio file in the near future. We also welcome any feedback you have on the session or suggestions that you might have for future calls. If you have any please send them to the nycalls' mailbox at fdic.gov. Thanks again for your participating - participation and have a great day.

And thank you, (Dorie), for getting us through this.

Coordinator: Thank you. And thank you for joining today's conference. That does conclude the call. All participants may disconnect.

Daniel Frye: Good work.

END