Title Insurance Participant and Abstract Company Best Practices

Why, Who and How Much?

Questions and Answers About Best Practices

IOWA LAND TITLE ASSOCIATION

Overview

- Does ALTA "Best Practices Program" apply to Abstract Companies?
- Why are lenders feeling intense pressure to scrutinize title professionals?
- What should be your response?
- If you adopt a Best Practices Program, who will assess compliance?
- How much will compliance cost?

Poll

- How many of the attendees today are ALTA Members?
- How many of you are familiar with ALTA's "Best Practices Program"?
- How many of you have started work on developing a Best Practices Program for your company?
- How many of you think Financial Institutions should be exercising Best Practices in their offices?

How, or why, does the Best Practices Program apply to Abstractors?

"Best Practices" are designed to…..

- #1 – Insure you have proper licenses to operate
- #2 – If you handle escrows, insure you properly manage your fiduciary responsibilities
- #3 – Insure you carefully handle all confidential information in your possession
- #4 – If you conduct closings, insure you comply with RESPA and other federal laws
- #5 – If you issue title Certificates, you timely produce them and report them to your Underwriter
- #6 – Insure you have proof of adequate professional liability coverage
- #7 – Insure you properly and promptly respond to consumer complaints

At least some parts of the Best Practices Program can apply to even a "Pure" Abstract Company

- For example, look at your obligations to comply with confidential information that is contained in your files……..

At least some parts of the Best Practices Program can apply to even a "Pure" Abstract Company

- For example, look at your obligations to comply with confidential information that is contained in your files……..
- **But did you know that you must comply with the Financial Privacy Rule established in 1999 and enforced by the Federal Trade Commission under the "Bank Holding Company Act"?**

Does the FTC Privacy Rule apply to Abstract Companies?

- You provide title search and abstract services

Does the FTC Privacy Rule apply to Abstract Companies?

- You provide title search and abstract services
- Title search and abstract services are defined as "Settlement Services" under RESPA – 12 U.S. CODE § 2602

Does the FTC Privacy Rule apply to Abstract Companies?

- You provide title search and abstract services
- Title search and abstract services are defined as "Settlement Services" under RESPA –12 U.S. CODE § 2602
- According to the Bank Holding Company Act, providing "Settlement Services" is a "Financial Activity"

Does the FTC Privacy Rule apply to Abstract Companies?

- You provide title search and abstract services
- Title search and abstract services are defined as "Settlement Services" under RESPA – 12 U.S. CODE § 2602
- According to the Bank Holding Company Act, providing "Settlement Services" is a "Financial Activity"
- Under section 4(k) of the Bank Holding Company Act, the Privacy Rule applies to businesses that are "significantly engaged" in "financial activities"

Does the FTC Privacy Rule apply to Abstract Companies?

- You provide title search and abstract services
- Title search and abstract services are defined as "Settlement Services" under RESPA – 12 U.S. CODE § 2602
- According to the Bank Holding Company Act, providing "Settlement Services" is a "Financial Activity"
- Under section 4(k) of the Bank Holding Company Act, the Privacy Rule applies to businesses that are "significantly engaged" in "financial activities"
- Under the Privacy Rule, an institution that is "significantly engaged" in financial activities is considered a financial institution.

Does the FTC Privacy Rule apply to Abstract Companies?

- You provide title search and abstract services
- Title search and abstract services are defined as "Settlement Services" under RESPA – 12 U.S. CODE § 2602
- According to the Bank Holding Company Act, providing "Settlement Services" is a "Financial Activity"
- Under section 4(k) of the Bank Holding Company Act, the Privacy Rule applies to businesses that are "significantly engaged" in "financial activities"
- Under the Privacy Rule, an institution that is "significantly engaged" in financial activities is considered a financial institution.

You are a "financial institution"

But you being deemed a "Financial Institution" is Not what is driving the need for a Best Practices Program

Recent Regulatory pressures on the Lenders are driving the need for a Best Practices Program

What specifically is causing the increased pressure to scrutinize title professionals?

A combination of Legislation….. and Regulators….

- Gramm Leach Bliley
- Office of the Comptroller of the Currency
- Federal Deposit Insurance Corporation
- Federal Reserve Board
- Dodd Frank
- Consumer Financial Protection Bureau

A combination of Legislation….. and Regulators….

- Gramm Leach Bliley
- Office of the Comptroller of the Currency
- Federal Deposit Insurance Corporation
- Federal Reserve Board
- Dodd Frank
- Consumer Financial Protection Bureau
- **…….and recent history of unprecedented fines!**

- **Gramm Leach Bliley** – 1999

It repealed part of the Glass-Steagall Act of 1933, removing barriers in the market among banking companies, securities companies and insurance companies that prohibited any one institution from acting as any combination of an investment bank, a commercial bank, and an insurance company.

Primary issue relevant to title related entities –

Title Search,
Abstract,
Certificate Issuing Participants
and Settlement Entities are
"Financial Institutions"

…….and it requires each to protect NPPI

- Difference between
"NPPI"
and
"Private" information

- Some NPPI is obvious
- Information in transition, even though it eventually becomes public, is NPPI

NPPI = Personally Identifiable Financial Information"

16 CFR 313.3 (o)

NPPI = Personally Identifiable Financial Information"

16 CFR 313.3 (o)

"*The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;"*

16 CFR 313.3 (o)(2)c)

NPPI = Personally Identifiable Financial Information"

16 CFR 313.3 (o)

"*The fact that an individual is or has been one of your customers or has obtained a financial product or service from you; "*

16 CFR 313.3 (o)(2)c)

" Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;"

16 CFR 313.3 (o)(2)(d)

- Gramm Leach Bliley – 1999
  - Protection of NPPI
  - GLB compliance is mandatory; whether a financial institution discloses nonpublic personal information or not, there must be a policy in place to protect the information from foreseeable threats in security and data integrity.
  - Express provisions govern the collection, disclosure, and protection of consumers' nonpublic personal information; or personally identifiable information

- Gramm Leach Bliley – 1999
  - The Financial Privacy Rule requires "financial institutions" to provide each consumer with a privacy notice at the time the consumer relationship is established ……..
  - The privacy notice must explain what information is collected about the consumer, where that information is shared, how that information is used, and how that information is protected.

- Privacy Notices
  - If you are not currently providing a Privacy Notice to your customers, you should consider developing that practice
  - Your Underwriter may have you distribute a copy of their Privacy Notice, but that is not compliance with your obligation to provide a Notice that defines how you will protect customer's private information

Key Legislation….. and Regulators…. driving Best Practices Initiatives

- ✓Gramm Leach Bliley
- Office of the Comptroller of the Currency
- Federal Deposit Insurance Corporation
- Dodd Frank
- Consumer Financial Protection Bureau

- OCC – Office of the Comptroller of the Currency
  - The OCC regulates and supervises about 2,000 national banks and federal savings associations and 50 federal branches of foreign banks in the U.S., accounting for over three-quarters of the total assets of all U.S. commercial banks (as of 2012)

- OCC – Office of the Comptroller of the Currency
  - OCC Advisory Letter 2000-9, "Third-Party Risk."
  - OCC Bulletin 2001- 47, "Third-Party Relationships: Risk Management Principles," and

.....Rescinded

- OCC – Office of the Comptroller of the Currency
  - Current Guidance to Lenders
  - OCC Bulletin **2013**-29, "Third-Party Relationships: Risk Management Principles," released October 30, 2013

Real Estate Settlements are "Critical Activities"

The OCC expects a bank to have risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the bank's organizational structures. Therefore, the OCC expects more comprehensive and rigorous oversight and management of third-party relationships that involve ***critical activities***—significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that

- For third-party relationships that are likely to involve critical activities, the OCC expects banks to conduct "extensive due diligence" before entering into the relationship. The 2013 Bulletin also states that the bank's board of directors should approve any contract that will involve critical activities prior to execution.
- And, for existing or future third-party relationships that may not presently involve critical activities, the OCC makes clear that the bank's senior management is responsible for "periodically" assessing the relationships to determine whether the third party's activities have become a critical activity.
- Under the guidance, senior management also is responsible for ensuring that *periodic "independent reviews" are conducted on the third-party risk management process* when a bank involves third parties in critical activities.

Key Legislation….. and Regulators…. driving Best Practices Initiatives

- ✓Gramm Leach Bliley
- ✓Office of the Comptroller of the Currency
- Federal Deposit Insurance Corporation
- Federal Reserve Board
- Dodd Frank
- Consumer Financial Protection Bureau

- FDIC – Federal Deposit Insurance Corporation
  - Supervisory Insights – "Third Party Arrangements : Elevating Risk Awareness", Issued June 2007
  - Financial Institution Letters: "Third-Party Risk Guidance for Managing Third-Party Risk". Issued June 2008

Key Legislation….. and Regulators…. driving Best Practices Initiatives

- ✓ Gramm Leach Bliley
- ✓ Office of the Comptroller of the Currency
- ✓ Federal Deposit Insurance Corporation
- Federal Reserve Board
- Dodd Frank
- Consumer Financial Protection Bureau

- Federal Reserve Board
  - On December 5, 2013, the Federal Reserve Board (FRB or the Fed) issued Supervision and Regulation Letter 13-19, which details and attaches the Fed's Guidance on Managing Outsourcing Risk (FRB Guidance).
  - The FRB Guidance sets forth risks arising out of the use of service providers and the regulatory expectations relating to risk management programs. It is substantially similar to OCC Bulletin 2013-29.

Key Legislation….. and Regulators…. driving Best Practices Initiatives

- ✓ Gramm Leach Bliley
- ✓ Office of the Comptroller of the Currency
- ✓ Federal Deposit Insurance Corporation
- ✓ Federal Reserve Board
- Dodd Frank
- Consumer Financial Protection Bureau

- Dodd Frank – Passed 2011

The Dodd-Frank Act implements changes that, among other things, affect the oversight and supervision of financial institutions, and create a new agency responsible for implementing and enforcing compliance with consumer financial laws…..

Key Legislation….. and Regulators…. driving Best Practices Initiatives

- ✓ Gramm Leach Bliley
- ✓ Office of the Comptroller of the Currency
- ✓ Federal Deposit Insurance Corporation
- ✓ Federal Reserve Board
- ✓ Dodd Frank
- **Consumer Financial Protection Bureau**

- CFPB – Consumer Financial Protection Bureau
  - CFPB was created by Congress as part of the Dodd-Frank Act to "Protect consumers by carrying out Federal consumer financial laws."

- The Consumer Financial Protection Bureau ("CFPB") expects supervised banks and nonbanks to oversee their business relationships with **service providers** in a manner that ensures compliance with Federal consumer financial law, which is designed to protect the interests of consumers and avoid consumer harm…

- *Service provider* is generally defined in section 1002(26) of the Dodd-Frank Act as "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service." (12 U.S.C. § 5481 (26)...

- "The mere fact that a [bank] enters into a business relationship with a service provider does not absolve the [bank] of responsibility for complying with Federal consumer financial law to avoid consumer harm".

- "A service provider … can harm consumers and create potential liabilities for both the service provider and the entity with which it has a business relationship. ***Depending on the circumstances, legal responsibility may lie with the [bank] as well as with the [service provider]"***.
- *Source:* **CFPB Bulletin 2012-03, Dated April 13, 2012** (Emphasis Added)

A new age……
Unprecedented fines as an enforcement tool

49 State Attorney General Litigation

- In February 2012, 49 state attorneys general and the federal government announced a historic joint state-federal settlement with the country's five largest mortgage servicers:
  - Ally/GMAC
  - Bank of America
  - Citi
  - JPMorgan Chase
  - Wells Fargo

49 State Attorney General Litigation

- $25 **Billion** Settlement
- The agreement settles state and federal investigations finding that the country's five largest mortgage servicers routinely signed foreclosure related documents outside the presence of a notary public and without really knowing whether the facts they contained were correct.

- CFPB Enforcement Action……. shortly after April CFPB Bulletin (2012-03)
  - American Express –
  - Discover –
  - Capital One –

- CFPB Enforcement Action shortly after April CFPB Bulletin (2012-03)
  - American Express – $85 million
  - Discover – $200 million
  - Capital One – $210 million
- The Message: Lenders are responsible and liable for acts of third party providers that harm consumers …….
- ……and lack of oversight can be extremely Costly!

CFPB Director Richard Cordray warned that "*we are signaling as clearly as we can that other financial institutions should review their marketing practices to ensure that they are not deceiving or misleading consumers into purchasing financial products or services*."

In less than three months, the CFPB has led the resolution of investigations coordinated with multiple federal and state agencies to extract $435 million in reimbursements to customers, more than $46 million in civil monetary penalties payable to the Civil Penalty Fund, and fines in excess of $55 million payable to other federal agencies.

Pressures on Lenders

- Regulatory Guidance to Lenders
  - Gramm Leach Bliley – 1999
  - Office of Comptroller of Currency – 2000, 2001 and 2013
  - Federal Deposit Insurance Corp. – 2006
  - Dodd Frank – 2011
  - Consumer Financial Protection Bureau Created – June 2011
    - CFPB was created by Congress as part of the Dodd-Frank Act to "Protect consumers by carrying out Federal consumer financial laws."
  - Federal Government and state attorneys general – 2011-2012
    - Consent Orders – 5 major Lending Service Organization – $25 Billion
  - CFPB Bulletin – April 2012 …… More than just Guidance
  - OCC 2013-29 – October 30, 2013 …….. Expressed directives
  - Federal Reserve Board – Dec 5, 2013– reiterates OCC directives

Conclusion

- I would not be as worried about CFPB knocking at your door,……. but you can reasonably anticipate Lenders threatening to take you off the approved list if you can't demonstrate your office is exercising "Best Practices" in their relationship with you.

- What should you be doing?

More Information

www.alta.org/bestpractices

- Best Practices
- Best Practice Assessment
- Best Practice Certification Package
- Best Practices Tool Kit
- Articles about Best Practices
- FAQs

Assessment Phase

How to get ready for the Certification Process?

ALTA Best Practices Framework:

Assessment Procedures

Version 2.0
Published July 19, 2013

AMERICAN LAND TITLE ASSOCIATION

Assessment Procedures Workbook

- 20 page Step by Step guidance on what the Third Party assessor will be looking at to determine whether your office is in compliance
- Each of the 7 Pillars is covered and provides details about what is required to earn a "Pass" certification
- Defines how many files are to be pulled for evaluation and what specific documentation will be requested for review

Assessment Procedures Workbook

- Each sub procedure under any of the Pillars is critical
- Instructions: "*Assessment Procedure Numbers are followed by an Asterisk (*). This indicates that a particular Assessment Procedure is a requirement and that a FAIL on that particular Assessment Procedure results in a FAIL for that Best Practice.*"
- Every sub procedure number in the workbook is marked with an Asterisk (*) !!!!!!!!

Assessment Procedures Workbook

- Therefore you must earn a "Pass" certification on 100% of each of the sub procedures in order to earn a "Pass" certification on each Pillar
- Essentially, the Assessment Procedures Workbook is an advanced copy of what will be on the "Test"
- If you know what is going to be on the test, you have a blueprint for what you need to do in developing your Best Practices program

Assessment Procedures Workbook

- Therefore you must earn a "Pass" certification on 100% of each of the sub procedures in order to earn a "Pass" certification on each Pillar
- Essentially, the Assessment Procedures Workbook is an advanced copy of what will be on the "Test"
- If you know what is going to be on the test, you have a blueprint for what you need to do in developing your Best Practices program

Who will conduct the assessment?

and

How much will it cost?

Rep. Barney Frank (right) and Sen. Chris Dodd after President Obama signed the Dodd-Frank bill into law in 2010

What's Next?

Get Started Now

- Obtain & file up-to-date license information
- Compile your current processes
- Create a list of all IT products
- Set Deadlines for Completion
- Communicate with your lenders

Use ALTA's Best Practice Tools

- Weekly Title News Online dedicated to Best Practices
- Checklist to help organize your efforts to meet the Best Practices
- Monthly Title Topics Webinars
- Advertisements in Trade Publications
- Visit www.alta.org/bestpractices for more tips and tools

Questions?

Thanks for allowing me to speak to the Iowa Land Title Association

If you need to ask me questions after the presentation you can reach me at

Gene McCullough
Title Experts and Management Services
gene@titleexperts.biz

865-310-7842

Knoxville, Tennessee

cfpb Consumer Financial Protection Bureau

1801 L Street NW, Washington, DC 20036

CFPB Bulletin 2012-03

Date: April 13, 2012

Subject: Service Providers

The Consumer Financial Protection Bureau ("CFPB") expects supervised banks and nonbanks to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law, which is designed to protect the interests of consumers and avoid consumer harm. The CFPB's exercise of its supervisory and enforcement authority will closely reflect this orientation and emphasis.

This Bulletin uses the following terms:

Supervised banks and nonbanks refers to the following entities supervised by the CFPB:

- Large insured depository institutions, large insured credit unions, and their affiliates (12 U.S.C. § 5515); and
- Certain non-depository consumer financial services companies (12 U.S.C. § 5514).

Supervised service providers refers to the following entities supervised by the CFPB:

- Service providers to supervised banks and nonbanks (12 U.S.C. §§ 5515, 5514); and
- Service providers to a substantial number of small insured depository institutions or small insured credit unions (12 U.S.C. § 5516).

Service provider is generally defined in section 1002(26) of the Dodd-Frank Act as "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service." (12 U.S.C. § 5481(26)). A service provider may or may not be affiliated with the person to which it provides services.

Federal consumer financial law is defined in section 1002(14) of the Dodd-Frank Act (12 U.S.C. § 5481(14)).

A. Service Provider Relationships

The CFPB recognizes that the use of service providers is often an appropriate business decision for supervised banks and nonbanks. Supervised banks and nonbanks may outsource certain functions to service providers due to resource constraints, use service providers to develop and market additional products or services, or rely on expertise from service providers that would not otherwise be available without significant investment.

However, the mere fact that a supervised bank or nonbank enters into a business relationship with a service provider does not absolve the supervised bank or nonbank of responsibility for complying with Federal consumer financial law to avoid consumer harm. A service provider that is unfamiliar with the legal requirements applicable to the products or services being offered, or that does not make efforts to implement those requirements carefully and effectively, or that exhibits weak internal controls, can harm consumers and create potential liabilities for both the service provider and the entity with which it has a business relationship. Depending on the circumstances, legal responsibility may lie with the supervised bank or nonbank as well as with the supervised service provider.

B. The CFPB's Supervisory Authority Over Service Providers

Title X authorizes the CFPB to examine and obtain reports from supervised banks and nonbanks for compliance with Federal consumer financial law and for other related purposes and also to exercise its enforcement authority when violations of the law are identified. Title X also grants the CFPB supervisory and enforcement authority over supervised service providers, which includes the authority to examine the operations of service providers on site.[1] The CFPB will exercise the full extent of its supervision authority over supervised service providers, including its authority to examine for compliance with Title X's prohibition on unfair, deceptive, or abusive acts or practices. The CFPB will also exercise its enforcement authority against supervised service providers as appropriate.[2]

C. The CFPB's Expectations

The CFPB expects supervised banks and nonbanks to have an effective process for managing the risks of service provider relationships. The CFPB will apply these expectations consistently, regardless of whether it is a supervised bank or nonbank that has the relationship with a service provider.

To limit the potential for statutory or regulatory violations and related consumer harm, supervised banks and nonbanks should take steps to ensure that their business arrangements with service providers do not present unwarranted risks to consumers. These steps should include, but are not limited to:

- Conducting thorough due diligence to verify that the service provider understands and is capable of complying with Federal consumer financial law;

---

[1] *See*, *e.g.*, subsections 1024(e), 1025(d), and 1026(e), and sections 1053 and 1054 of the Dodd-Frank Act, 12 U.S.C. §§ 5514(e), 5515(d), 5516(e), 5563, and 5564.
[2] *See* 12 U.S.C. §§ 5531(a), 5536.

- Requesting and reviewing the service provider's policies, procedures, internal controls, and training materials to ensure that the service provider conducts appropriate training and oversight of employees or agents that have consumer contact or compliance responsibilities;
- Including in the contract with the service provider clear expectations about compliance, as well as appropriate and enforceable consequences for violating any compliance-related responsibilities, including engaging in unfair, deceptive, or abusive acts or practices;
- Establishing internal controls and on-going monitoring to determine whether the service provider is complying with Federal consumer financial law; and
- Taking prompt action to address fully any problems identified through the monitoring process, including terminating the relationship where appropriate.

For more information pertaining to the responsibilities of a supervised bank or nonbank that has business arrangements with service providers, please review the CFPB's *Supervision and Examination Manual: Compliance Management Review* and *Unfair, Deceptive, and Abusive Acts or Practices*.[3]

[3] http://www.consumerfinance.gov/wp-content/themes/cfpb_theme/images/supervision_examination_manual_11211.pdf at 32 (CMR 1), 37 (CMR 6), 44 (UDAAP 1), and 59 (UDAAP 6).

BRYAN CAVE
A Broader Perspective

Alert

Financial Services Group

To: Our Clients and Friends

March 25, 2014

A Significant Change Is Occurring Regarding Regulatory Oversight of Banks and Their Third Party Relationships. Both Banks and their Vendors Must Pay Attention.

Introduction

First there was the Bulletin about third party vendors issued by the Consumer Financial Protection Bureau (CFPB) in April 2012.[1] Then it was the FFIEC's guidance on IT service providers in October 2012.[2] Next came the FDIC's September 2013 Financial Institution Letter about payment processing relationships with high risk merchants.[3] Then there was the news on October 30th 2013 about the OCC's Guidance on Third Party Relationships[4], followed shortly by the Federal Reserve Board's Guidance on Managing Outsourcing Risks in December 2013. [5]

Let's face it. There has always been guidance and concerns about banks and their relationships with third party service providers. But in recent years it has become quite obvious that the bar has been raised on how banks relate to their third party processors, program managers and other service providers. These changes have occurred over time, by a matter of degrees. But it is increasingly plain that we are seeing a significant sea change in how regulators approach the relationships between banks and their third party vendors. Examiners are digging deeper - - *especially into the content of bank contracts* - and the scope of review is extending to more and more vendors.

1 http://www.consumerfinance.gov/newsroom/consumer-financial-protection-bureau-to-hold-financial-institutions-and-their-service-providers-accountable/
2 https://www.ffiec.gov/press/pr103112.htm
3 http://www.fdic.gov/news/news/financial/2013/fil13043.html
4 http://www.occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
5 http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf

In recent months, public commentary from some of the regulators have revealed even more clearly how this recent guidance will impact banks and their vendors. In this article we will describe the regulatory developments and provide some practical guidance as to what this will mean -- not only for banks, but for their processors and other service providers.

Recent Regulatory Developments.

Banks and other financial institutions have always been expected to choose their vendors carefully and monitor the performance of those vendors. Most institutions have done a reasonably good job in this regard. However, recent regulatory publications and the focus of recent regulatory examinations and enforcement actions indicate that the standards and expectations are now much higher.

The CFPB issued a bulletin on April 13, 2012 regarding the use of service providers, accompanied by a press release stating, "CFPB to Hold Financial Institutions and their Service Providers Accountable." This bulletin, CFPB Bulletin 2012-03 (the CFPB Bulletin), states that the CFPB "expects supervised banks and nonbanks to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law."(emphasis added).

A Financial institution letter issued by the FDIC on September 27, 2013 focused on banks that facilitate payment processing services, either director OR through a third party, for merchant customers engaged in "higher-risk activities." Again the regulators indicated that banks are expected not only to perform proper risk assessments and conduct due diligence, but they are expected to determine whether the "merchant customers are operating in accordance with applicable law." That's a significant responsibility, difficult to achieve, especially when the there is a third party involved.

On October 30, 2013, the Office of the Comptroller of the Currency (OCC) published risk Management Guidance regarding third-party relationships, OCC Bulletin 2013-29 (the OCC Bulletin). The OCC Bulletin is broader in scope than the CFPB Bulletin in that it does not focus only on consumer protection but instead refers to all "third-party relationships involving critical activities," a concept we address further below. Following suit, the Federal Reserve (FRB) issued its guidance in December 2013 that almost echoed the OCC Bulletin point-for-point.

The CFPB Bulletin applies to "supervised banks and nonbanks." CFPB-supervised banks are all banking institutions and their affiliates with total assets exceeding $10 billion. CFPB-supervised nonbanks are certain nonbank businesses, regardless of size, that do business in the following markets: mortgage companies (originators, brokers, and servicers, and loan modification or foreclosure relief services); payday lenders; and private education lenders. The CFPB also supervises all non-banks that are "larger participants" with respect to other consumer financial products or services as determined by the CFPB. The "service providers" of concern are those persons that provide a material service to a covered institution in connection with the offering or providing of a consumer financial product or service.

According to the CFPB Bulletin, the CFPB expects all of its supervised banks and nonbanks to have an effective process for managing the risks of service provider relationships. It is very important to note that the CFPB intends to apply these standards even if the supervised bank or nonbank does not have a direct relationship with the service provider. This would seem to mean that a bank or nonbank is responsible for its vendor's service providers if those service providers perform a material service relating to the bank's or non-bank's consumer products or services. Similarly, the OCC and FRB expect a bank's contract with its third-party vendors to address the third-party's use of subcontractors and the responsibilities for and monitoring of those subcontractors.

Other than the fact that the CFPB focuses on consumer products and services and the OCC and FRB approach vendor risk management more broadly, the Bulletins issued by the three regulators show some similar regulatory expectations, including:

- Thorough due diligence of the service provider, which the OCC notes could call for on-site visits depending on the risks of the relationship;
- Clear contractual expectations for the service provider, including enforceable consequences for violating contractual requirements (see more below); and
- Establishment and maintenance of internal controls and on-going monitoring of the service provider.

Bank Board and Management Requirements

The OCC and FRB Bulletins are quite detailed and include significantly more strongly stated expectations of the bank's board and management. In fact, the OCC stated that "a bank's failure to have an effective third-party risk management process…may be an unsafe and unsound banking practice."[6] For example, under the OCC's guidance, a supervised bank's board of directors has the following specific responsibilities:

- Ensure an effective process is in place to manage risks related to third-party relationships in a manner consistent with the bank's strategic goals, organizational objectives, and risk appetite.
- Approve the bank's risk-based policies that govern the third-party risk management process and identify critical activities.
- Review and approve management's plans for using third parties that involve critical activities.
- Review summary of due diligence results and management's recommendations to use third parties that involve critical activities.
- Approve contracts with third parties that involve critical activities.

[6] http://www.occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

- Review the results of management's ongoing monitoring of third-party relationships involving critical activities.

- Ensure management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring.

- Review results of periodic independent reviews of the bank's third-party risk management process.

Contractual Requirements

The OCC Bulletin also includes a comprehensive list of issues that the OCC will expect to be addressed in each institution's contracts with this third-party vendors. If your company provides services to a bank, you should not be surprised when the bank demands these contractual provisions, even if it was never required before. Matters that the OCC will expect banks to include in their contracts include:

Nature and Scope of Arrangement

Contracts for complicated or highly technical services have not always included the detail that is now expected. Future contracts would need to be more clear on such issues as the specific nature and scope of the arrangement; the frequency, content, and format of the service, product, or function to be provided; where the services are to be performed; and the use of the bank's information, facilities, personnel, systems, and equipment, as well as access to and use of the bank's or customers' information.

Performance Measures or Benchmarks

Contracts should specify clear and verifiable performance measures. The Bulletin notes that such measures can be used to motivate the third party's performance, penalize poor performance, or reward outstanding performance.

Responsibilities for Providing, Receiving, and Retaining Information

Ensure that the contract requires the third party to provide and retain timely, accurate, and comprehensive information such as records and reports that allow bank management to monitor performance, service levels, and risks. The contract also should stipulate the frequency and type of reports required, including for example, performance reports, control audits, financial statements, security reports, BSA/AML and Office of Foreign Asset Control (OFAC) compliance responsibilities and reports for monitoring potential suspicious activity, reports for monitoring customer complaint activity, and business resumption testing reports.

In addition, the contract should address the responsibilities and reports regarding such matters as catastrophic events, data loss, service or systems interruptions, significant changes to the vendor's systems or key personnel, and significant business changes such as result from changes in ownership, among other things.

The Right to Audit and Require Remediation

The contract should ensure that the bank has a right to audit, monitor performance, and require remediation when issues are identified. For certain types of services, such as technology services, the audits should specifically address applicable technology and security standards. Audit reports also should include a review of the third party's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.

Responsibility for Compliance With Applicable Laws and Regulations

Ensure the contract addresses compliance with the specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, and clearly specifies the parties' respective obligations for such compliance.

Costs and Compensation

Be very clear on all aspects of costs and compensation, including which party is responsible for costs of systems changes necessitated by changes in laws or other circumstances and costs for audits and similar requirements.

Ownership and License

Be sure to clearly address each parties' rights to use the information, technology and intellectual property of the other, and include appropriate warranties on the part of the third party related to its acquisition of licenses for use of any intellectual property developed by other third parties. If the bank purchases software, establish escrow agreements to provide for the bank's access to source code and programs under certain conditions (e.g., insolvency of the third party).

Confidentiality and Integrity

Prohibit the third party and its subcontractors from using or disclosing the bank's information, except as necessary to provide the contracted activities or comply with legal requirements. If the third party receives bank customers' personally identifiable information, the contract should ensure that the third party implements and maintains appropriate security measures to comply with privacy regulations and regulatory guidelines.

Business Resumption and Contingency Plans

Ensure the contract provides for continuation of the business function in the event of problems affecting the third party's operations, including degradations or interruptions resulting from natural disasters, human error, or intentional attacks. The contract also should require the third party to provide the bank with operating procedures to be carried out in the event business resumption and disaster recovery plans are implemented. Include specific time frames for business resumption and recovery that meet the bank's requirements, and when appropriate, regulatory requirements.

Indemnification

Carefully assess indemnification clauses that require the bank to hold the third party harmless from liability.

Insurance

Require the third party is required to maintain adequate insurance, notify the bank of material changes to coverage, and provide evidence of coverage where appropriate.

Dispute Resolution

Consider whether the contract should establish a dispute resolution process (arbitration, mediation, or other means) to resolve problems between the bank and the third party in an expeditious manner, and whether the third party should continue to provide activities to the bank during the dispute resolution period.

Limits on Liability

Determine whether the contract limits the third party's liability and whether the proposed limit is in proportion to the amount of loss the bank might experience because of the third party's failure to perform or to comply with applicable laws. While not specifically stated in the OCC Bulletin, we suggest caution in agreeing to terms that cap liability based on the amount of fees paid.

Default and Termination

Of course every contract should be clear on what constitutes an event of default, the remedies for such default, and the consequences of termination of the contract. The OCC Bulletin also states that the bank should determine whether the contract includes a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally directs the bank to terminate the relationship.

Customer Complaints

Specify whether the bank or third party is responsible for responding to customer complaints, how complaints are handled and how complaint information is provided to the bank.

Subcontracting

If the vendor will be allowed to use subcontractors, specify the activities that can or cannot be subcontracted and address the third party's liability for activities or actions by its subcontractors and which party is responsible for the costs and resources required for any additional monitoring and management of the subcontractors. Reserve the right to terminate the contract without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract.

Foreign-Based Third Parties

If your vendor is based in a foreign country, be sure to address choice-of-law and jurisdictional matters.

If your bank is not very familiar with the laws of the foreign country, seek appropriate legal guidance before entering into the contract.

OCC Supervision

All contracts with service providers should provide for federal bank regulator access to the service provider, including access to all work papers, drafts, and other materials. The OCC generally has the authority to examine and to regulate the functions or operations performed or provided by third parties to the same extent as if they were performed by the bank itself on its own premises.

Practical Advice and Next Steps.

We have had the opportunity to share concerns with and ask questions of OCC staff in Washington, DC, on a number of occasions. In those conversations, the OCC staff repeatedly suggested that regulatory expectations of banks have not actually changed from the past. However, at the same time the staff acknowledged that their focus will be on contractual relationships between banks and their third party vendors, including contracts entered into prior to the OCC Bulletin. If the concerns stated are not dealt with in such contracts to the standards expressed in the recent OCC and FRB Bulletins, some institutions might be facing harsh examinations when these existing arrangements are reviewed.

In that regard, the OCC noted that each bank should do the following:

- First, prioritize their review of existing third-party relationships, focusing on those involving critical activities.

- Second, review each contract to ensure that the critical terms described above are addressed, including:

    - clear expectations about compliance, as well as appropriate and enforceable consequences for violating any compliance-related responsibilities;

    - rights to audit the vendor, at reasonable times and with reasonable frequency, for compliance with the contract and compliance related responsibilities; and

    - rights to terminate such contract for material violations

- Amend or update any contracts that fall short of these standards.

- For those contracts that cannot be re-negotiated or amended, a bank will need to "step up its risk management game internally" - - that is, until such time that necessary contractual protections can be added, the bank will need to increase monitoring and other oversight activities to address the higher risk.

As noted above, the OCC Bulletin purports to focus on third-party relationships involving "critical activities." What this might mean in practice is anybody's guess and the OCC's judgment will ultimately control, but the OCC Bulletin itself states that critical activities include:

"significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that

- could cause a bank to face significant risk if the third party fails to meet expectations.

- could have significant customer impacts.

- require significant investment in resources to implement the third-party relationship and manage the risk.

- could have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house."

With this broad definition, if a bank is ultimately embarrassed or criticized by customers or the media for activities performed by a third party, virtually any activity that previously seemed non-critical could with hindsight later be deemed to have been "critical". In the meantime, banks have few options but to comply with these extraordinarily high standards with respect to third party processors, service providers, and vendors.

Should you have any questions or concerns, please feel free to contact us. The following Bryan Cave Payments Group members can provide contractual and bank regulatory assistance:

John ReVeal Washington DC 202-508-6395 John.reveal@bryancave.com	Judith Rinearson New York, NY 212-541-1135 Judith.rinearson@bryancave.com	Linda Odom Washington DC 202-508-6331 Linda.Odom@bryancave.com
Karen Louis Atlanta GA 404-572-6766 Karen.louis@bryancave.com	Jennifer Crowder Kansas City, MO 816-374-3365 Jennifer.crowder@bryancave.com	Courtney Stolz Washington DC 202-508-6076 Courtney.stolz@bryancave.com
Dan Wheeler San Francisco CA 415- 675-3472 Dan.wheeler@bryancave.com	Margo Strahlberg Chicago, IL 312-602-5094 Margo.strahlberg@bryancave.com	Rob Lystad Atlanta, GA 404-572-6831 Rob.lystad@bryancave.com

Guidance on Managing Outsourcing Risk

Division of Banking Supervision and Regulation
Division of Consumer and Community Affairs
Board of Governors of the Federal Reserve System

December 5, 2013

Table of Contents

I. Purpose

In addition to traditional core bank processing and information technology services, financial institutions[1] outsource operational activities such as accounting, appraisal management, internal audit, human resources, sales and marketing, loan review, asset and wealth management, procurement, and loan servicing. The Federal Reserve is issuing this guidance to financial institutions to highlight the potential risks arising from the use of service providers and to describe the elements of an appropriate service provider risk management program. This guidance supplements existing guidance on technology service provider (TSP) risk,[2] and applies to service provider relationships where business functions or activities are outsourced. For purposes of this guidance, "service providers" is broadly defined to include all entities[3] that have entered into a contractual relationship with a financial institution to provide business functions or activities.

II. Risks from the Use of Service Providers

The use of service providers to perform operational functions presents various risks to financial institutions. Some risks are inherent to the outsourced activity itself, whereas others are introduced with the involvement of a service provider. If not managed effectively, the use of service providers may expose financial institutions to risks that can result in regulatory action, financial loss, litigation, and loss of reputation. Financial institutions should consider the following risks before entering into and while managing outsourcing arrangements.

- *Compliance risks* arise when the services, products, or activities of a service provider fail to comply with applicable U.S. laws and regulations.
- *Concentration risks* arise when outsourced services or products are provided by a limited number of service providers or are concentrated in limited geographic locations.
- *Reputational risks* arise when actions or poor performance of a service provider causes the public to form a negative opinion about a financial institution.

---

[1] For purposes of this guidance, a "financial institution" refers to state member banks, bank and savings and loan holding companies (including their nonbank subsidiaries), and U.S. operations of foreign banking organizations.

[2] Refer to the *FFIEC Outsourcing Technology Services Booklet* (June 2004) at http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx.

[3] Entities may be a bank or nonbank, affiliated or non-affiliated, regulated or non-regulated, or domestic or foreign.

- *Country risks* arise when a financial institution engages a foreign-based service provider, exposing the institution to possible economic, social, and political conditions and events from the country where the provider is located.
- *Operational risks* arise when a service provider exposes a financial institution to losses due to inadequate or failed internal processes or systems or from external events and human error.
- *Legal risks* arise when a service provider exposes a financial institution to legal expenses and possible lawsuits.

III. Board of Directors and Senior Management Responsibilities

The use of service providers does not relieve a financial institution's board of directors and senior management of their responsibility to ensure that outsourced activities are conducted in a safe-and-sound manner and in compliance with applicable laws and regulations. Policies governing the use of service providers should be established and approved by the board of directors, or an executive committee of the board. These policies should establish a service provider risk management program that addresses risk assessments and due diligence, standards for contract provisions and considerations, ongoing monitoring of service providers, and business continuity and contingency planning.

Senior management is responsible for ensuring that board-approved policies for the use of service providers are appropriately executed. This includes overseeing the development and implementation of an appropriate risk management and reporting framework that includes elements described in this guidance. Senior management is also responsible for regularly reporting to the board of directors on adherence to policies governing outsourcing arrangements.

IV. Service Provider Risk Management Programs

A financial institution's service provider risk management program should be risk-focused and provide oversight and controls commensurate with the level of risk presented by the outsourcing arrangements in which the financial institution is engaged. It should focus on outsourced activities that have a substantial impact on a financial institution's financial condition; are critical to the institution's ongoing operations; involve sensitive customer information or new bank products or services; or pose material compliance risk.

The depth and formality of the service provider risk management program will depend on the criticality, complexity, and number of material business activities being outsourced. A

community banking organization may have critical business activities being outsourced, but the number may be few and to highly reputable service providers. Therefore, the risk management program may be simpler and use less elements and considerations. For those financial institutions that may use hundreds or thousands of service providers for numerous business activities that have material risk, the financial institution may find that they need to use many more elements and considerations of a service provider risk management program to manage the higher level of risk and reliance on service providers.

While the activities necessary to implement an effective service provider risk management program can vary based on the scope and nature of a financial institution's outsourced activities, effective programs usually include the following core elements:

A. Risk assessments;

B. Due diligence and selection of service providers;

C. Contract provisions and considerations;

D. Incentive compensation review;

E. Oversight and monitoring of service providers; and

F. Business continuity and contingency plans.

A. Risk Assessments

Risk assessment of a business activity and the implications of performing the activity in-house or having the activity performed by a service provider are fundamental to the decision of whether or not to outsource. A financial institution should determine whether outsourcing an activity is consistent with the strategic direction and overall business strategy of the organization. After that determination is made, a financial institution should analyze the benefits and risks of outsourcing the proposed activity as well as the service provider risk, and determine cost implications for establishing the outsourcing arrangement. Consideration should also be given to the availability of qualified and experienced service providers to perform the service on an ongoing basis. Additionally, management should consider the financial institution's ability and expertise to provide appropriate oversight and management of the relationship with the service provider.

This risk assessment should be updated at appropriate intervals consistent with the financial institution's service provider risk management program. A financial institution should revise its risk mitigation plans, if appropriate, based on the results of the updated risk assessment.

B. Due Diligence and Selection of Service Providers

A financial institution should conduct an evaluation of and perform the necessary due diligence for a prospective service provider prior to engaging the service provider. The depth and formality of the due diligence performed will vary depending on the scope, complexity, and

importance of the planned outsourcing arrangement, the financial institution's familiarity with prospective service providers, and the reputation and industry standing of the service provider. Throughout the due diligence process, financial institution technical experts and key stakeholders should be engaged in the review and approval process as needed. The overall due diligence process includes a review of the service provider with regard to:

1. Business background, reputation, and strategy;
2. Financial performance and condition; and
3. Operations and internal controls.

1. Business Background, Reputation, and Strategy

Financial institutions should review a prospective service provider's status in the industry and corporate history and qualifications; review the background and reputation of the service provider and its principals; and ensure that the service provider has an appropriate background check program for its employees.

The service provider's experience in providing the proposed service should be evaluated in order to assess its qualifications and competencies to perform the service. The service provider's business model, including its business strategy and mission, service philosophy, quality initiatives, and organizational policies should be evaluated. Financial institutions should also consider the resiliency and adaptability of the service provider's business model as factors in assessing the future viability of the provider to perform services.

Financial institutions should check the service provider's references to ascertain its performance record, and verify any required licenses and certifications. Financial institutions should also verify whether there are any pending legal or regulatory compliance issues (for example, litigation, regulatory actions, or complaints) that are associated with the prospective service provider and its principals.

2. Financial Performance and Condition

Financial institutions should review the financial condition of the service provider and its closely-related affiliates. The financial review may include:

- The service provider's most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results.
- The service provider's sustainability, including factors such as the length of time that the service provider has been in business and the service provider's growth of market share for a given service.
- The potential impact of the financial institution's business relationship on the service provider's financial condition.

- The service provider's commitment (both in terms of financial and staff resources) to provide the contracted services to the financial institution for the duration of the contract.
- The adequacy of the service provider's insurance coverage.
- The adequacy of the service provider's review of the financial condition of any subcontractors.
- Other current issues the service provider may be facing that could affect future financial performance.

3. Operations and Internal Controls

Financial institutions are responsible for ensuring that services provided by service providers comply with applicable laws and regulations and are consistent with safe-and-sound banking practices. Financial institutions should evaluate the adequacy of standards, policies, and procedures. Depending on the characteristics of the outsourced activity, some or all of the following may need to be reviewed:

- Internal controls;
- Facilities management (such as access requirements or sharing of facilities);
- Training, including compliance training for staff;
- Security of systems (for example, data and equipment);
- Privacy protection of the financial institution's confidential information;
- Maintenance and retention of records;
- Business resumption and contingency planning;
- Systems development and maintenance;
- Service support and delivery;
- Employee background checks; and
- Adherence to applicable laws, regulations, and supervisory guidance.

C. Contract Provisions and Considerations

Financial institutions should understand the service contract and legal issues associated with proposed outsourcing arrangements. The terms of service agreements should be defined in written contracts that have been reviewed by the financial institution's legal counsel prior to execution. The characteristics of the business activity being outsourced and the service

provider's strategy for providing those services will determine the terms of the contract. Elements of well-defined contracts and service agreements usually include:

- ***Scope:*** Contracts should clearly define the rights and responsibilities of each party, including:
  - Support, maintenance, and customer service;
  - Contract timeframes;
  - Compliance with applicable laws, regulations, and regulatory guidance;
  - Training of financial institution employees;
  - The ability to subcontract services;
  - The distribution of any required statements or disclosures to the financial institution's customers;
  - Insurance coverage requirements; and
  - Terms governing the use of the financial institution's property, equipment, and staff.
- ***Cost and compensation:*** Contracts should describe the compensation, variable charges, and any fees to be paid for non-recurring items and special requests. Agreements should also address which party is responsible for the payment of any legal, audit, and examination fees related to the activity being performed by the service provider. Where applicable, agreements should address the party responsible for the expense, purchasing, and maintenance of any equipment, hardware, software or any other item related to the activity being performed by the service provider. In addition, financial institutions should ensure that any incentives (for example, in the form of variable charges, such as fees and/or commissions) provided in contracts do not provide potential incentives to take imprudent risks on behalf of the institution.
- ***Right to audit:*** Agreements may provide for the right of the institution or its representatives to audit the service provider and/or to have access to audit reports. Agreements should define the types of audit reports the financial institution will receive and the frequency of the audits and reports.
- ***Establishment and monitoring of performance standards:*** Agreements should define measurable performance standards for the services or products being provided.
- ***Confidentiality and security of information:*** Consistent with applicable laws, regulations, and supervisory guidance, service providers should ensure the security and confidentiality of both the financial institution's confidential information and the financial institution's customer information. Information security measures for outsourced functions should be viewed as if the activity were being performed by the financial institution and afforded the same protections. Financial institutions have a responsibility to ensure service providers take appropriate measures designed to meet

the objectives of the information security guidelines within Federal Financial Institutions Examination Council (FFIEC) guidance[4], as well as comply with section 501(b) of the Gramm-Leach-Bliley Act. These measures should be mapped directly to the security processes at financial institutions, as well as be included or referenced in agreements between financial institutions and service providers.

Service agreements should also address service provider use of financial institution information and its customer information. Information made available to the service provider should be limited to what is needed to provide the contracted services. Service providers may reveal confidential supervisory information only to the extent authorized under applicable laws and regulations.[5]

If service providers handle any of the financial institution customer's Nonpublic Personal Information (NPPI), the service providers must comply with applicable privacy laws and regulations.[6] Financial institutions should require notification from service providers of any breaches involving the disclosure of NPPI data. Generally, NPPI data is any nonpublic personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available.[7] Financial institutions and their service providers who maintain, store, or process NPPI data are responsible for that information and any disclosure of it. The security of, retention of, and access to NPPI data should be addressed in any contracts with service providers.

When a breach or compromise of NPPI data occurs, financial institutions have legal requirements that vary by state and these requirements should be made part of the contracts between the financial institution and any service provider that provides storage, processing, or transmission of NPPI data. Misuse or unauthorized disclosure of confidential customer data by service providers may expose financial institutions to liability or action by a federal or state regulatory agency. Contracts should clearly authorize and disclose the roles and responsibilities of financial institutions and service providers regarding NPPI data.

- ***Ownership and license:*** Agreements should define the ability and circumstances under which service providers may use financial institution property inclusive of data, hardware, software, and intellectual property. Agreements should address the ownership and control of any information generated by service providers. If financial institutions purchase software from service providers, escrow agreements may be

---

[4] For further guidance regarding vendor security practices, refer to the *FFIEC Information Security Booklet* (July 2006) at http://ithandbook.ffiec.gov/it-booklets/information-security.aspx.

[5] *See* 12 CFR Part 261.

[6] *See* 12 CFR Part 1016.

[7] *See* 12 U.S.C. 6801(b).

needed to ensure that financial institutions have the ability to access the source code and programs under certain conditions.[8]

- ***Indemnification:*** Agreements should provide for service provider indemnification of financial institutions for any claims against financial institutions resulting from the service provider's negligence.

- ***Default and termination:*** Agreements should define events of a contractual default, list of acceptable remedies, and provide opportunities for curing default. Agreements should also define termination rights, including change in control, merger or acquisition, increase in fees, failure to meet performance standards, failure to fulfill the contractual obligations, failure to provide required notices, and failure to prevent violations of law, bankruptcy, closure, or insolvency. Contracts should include termination and notification requirements that provide financial institutions with sufficient time to transfer services to another service provider. Agreements should also address a service provider's preservation and timely return of financial institution data, records, and other resources.

- ***Dispute resolution:*** Agreements should include a dispute resolution process in order to expedite problem resolution and address the continuation of the arrangement between the parties during the dispute resolution period.

- ***Limits on liability:*** Service providers may want to contractually limit their liability. The board of directors and senior management of a financial institution should determine whether the proposed limitations are reasonable when compared to the risks to the institution if a service provider fails to perform.[9]

- ***Insurance:*** Service providers should have adequate insurance and provide financial institutions with proof of insurance. Further, service providers should notify financial institutions when there is a material change in their insurance coverage.

- ***Customer complaints:*** Agreements should specify the responsibilities of financial institutions and service providers related to responding to customer complaints. If service providers are responsible for customer complaint resolution, agreements should provide for summary reports to the financial institutions that track the status and resolution of complaints.

- ***Business resumption and contingency plan of the service provider:*** Agreements should address the continuation of services provided by service providers in the event of operational failures. Agreements should address service provider responsibility for

---

[8] Escrow agreements are established with vendors when buying or leasing products that have underlying proprietary software. In such agreements, an organization can only access the source program code under specific conditions, such as discontinued product support or financial insolvency of the vendor.

[9] Refer to SR letter 06-4, "Interagency Advisory on the Unsafe and Unsound Use of Limitations on Liability Provisions in External Audit Engagement Letters," regarding restrictions on the liability limitations for external audit engagements at http://www.federalreserve.gov/boarddocs/srletters/2006/SR0604.htm.

backing up information and maintaining disaster recovery and contingency plans. Agreements may include a service provider's responsibility for testing of plans and providing testing results to financial institutions.

- ***Foreign-based service providers:*** For agreements with foreign-based service providers, financial institutions should consider including express choice of law and jurisdictional provisions that would provide for the adjudication of all disputes between the two parties under the laws of a single, specific jurisdiction. Such agreements may be subject to the interpretation of foreign courts relying on local laws. Foreign law may differ from U.S. law in the enforcement of contracts. As a result, financial institutions should seek legal advice regarding the enforceability of all aspects of proposed contracts with foreign-based service providers and the other legal ramifications of such arrangements.

- ***Subcontracting:*** If agreements allow for subcontracting, the same contractual provisions should apply to the subcontractor. Contract provisions should clearly state that the primary service provider has overall accountability for all services that the service provider and its subcontractors provide. Agreements should define the services that may be subcontracted, the service provider's due diligence process for engaging and monitoring subcontractors, and the notification and approval requirements regarding changes to the service provider's subcontractors. Financial institutions should pay special attention to any foreign subcontractors, as information security and data privacy standards may be different in other jurisdictions. Additionally, agreements should include the service provider's process for assessing the subcontractor's financial condition to fulfill contractual obligations.

D. Incentive Compensation Review

Financial institutions should also ensure that an effective process is in place to review and approve any incentive compensation that may be embedded in service provider contracts, including a review of whether existing governance and controls are adequate in light of risks arising from incentive compensation arrangements. As the service provider represents the institution by selling products or services on its behalf, the institution should consider whether the incentives provided might encourage the service provider to take imprudent risks. Inappropriately structured incentives may result in reputational damage, increased litigation, or other risks to the financial institution. An example of an inappropriate incentive would be one where variable fees or commissions encourage the service provider to direct customers to products with higher profit margins without due consideration of whether such products are suitable for the customer.

E. Oversight and Monitoring of Service Providers

To effectively monitor contractual requirements, financial institutions should establish acceptable performance metrics that the business line or relationship management determines to be indicative of acceptable performance levels. Financial institutions should ensure that

personnel with oversight and management responsibilities for service providers have the appropriate level of expertise and stature to manage the outsourcing arrangement. The oversight process, including the level and frequency of management reporting, should be risk-focused. Higher risk service providers may require more frequent assessment and monitoring and may require financial institutions to designate individuals or a group as a point of contact for those service providers. Financial institutions should tailor and implement risk mitigation plans for higher risk service providers that may include processes such as additional reporting by the service provider or heightened monitoring by the financial institution. Further, more frequent and stringent monitoring is necessary for service providers that exhibit performance, financial, compliance, or control concerns. For lower risk service providers, the level of monitoring can be lessened.

Financial condition: Financial institutions should have established procedures to monitor the financial condition of service providers to evaluate their ongoing viability. In performing these assessments, financial institutions should review the most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity and operating results. If a service provider relies significantly on subcontractors to provide services to financial institutions, then the service provider's controls and due diligence regarding the subcontractors should also be reviewed.

***Internal controls*:** For significant service provider relationships, financial institutions should assess the adequacy of the provider's control environment. Assessments should include reviewing available audits or reports such as the American Institute of Certified Public Accountants' Service Organization Control 2 report.[10] If the service provider delivers information technology services, the financial institution can request the FFIEC Technology Service Provider examination report from its primary federal regulator. Security incidents at the service provider may also necessitate the institution to elevate its monitoring of the service provider.

Escalation of oversight activities: Financial institutions should ensure that risk management processes include triggers to escalate oversight and monitoring when service providers are failing to meet performance, compliance, control, or viability expectations. These procedures should include more frequent and stringent monitoring and follow-up on identified issues, on-site control reviews, and when an institution should exercise its right to audit a service provider's adherence to the terms of the agreement. Financial institutions should develop criteria for engaging alternative outsourcing arrangements and terminating the service provider contract in the event that identified issues are not adequately addressed in a timely manner.

F. Business Continuity and Contingency Considerations

Various events may affect a service provider's ability to provide contracted services. For example, services could be disrupted by a provider's performance failure, operational disruption, financial difficulty, or failure of business continuity and contingency plans during operational

[10] Refer to www.AICPA.org.

disruptions or natural disasters. Financial institution contingency plans should focus on critical services provided by service providers and consider alternative arrangements in the event that a service provider is unable to perform.[11] When preparing contingency plans, financial institutions should:

- Ensure that a disaster recovery and business continuity plan exists with regard to the contracted services and products;
- Assess the adequacy and effectiveness of a service provider's disaster recovery and business continuity plan and its alignment to their own plan;
- Document the roles and responsibilities for maintaining and testing the service provider's business continuity and contingency plans;
- Test the service provider's business continuity and contingency plans on a periodic basis to ensure adequacy and effectiveness; and
- Maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to perform.

G. Additional Risk Considerations

Suspicious Activity Report (SAR) reporting functions: The confidentiality of suspicious activity reporting makes the outsourcing of any SAR-related function more complex. Financial institutions need to identify and monitor the risks associated with using service providers to perform certain suspicious activity reporting functions in compliance with the Bank Secrecy Act (BSA). Financial institution management should ensure they understand the risks associated with such an arrangement and any BSA-specific guidance in this area.

***Foreign-based service providers*:** Financial institutions should ensure that foreign-based service providers are in compliance with applicable U.S. laws, regulations, and regulatory guidance. Financial institutions may also want to consider laws and regulations of the foreign-based provider's country or regulatory authority regarding the financial institution's ability to perform on-site review of the service provider's operations. In addition, financial institutions should consider the authority or ability of home country supervisors to gain access to the financial institution's customer information while examining the foreign-based service provider.

Internal audit: Financial institutions should refer to existing guidance on the engagement of independent public accounting firms and other outside professionals to perform work that has been traditionally carried out by internal auditors.[12] The Sarbanes-Oxley Act of

---

[11] For further guidance regarding business continuity planning with service providers, refer to the *FFIEC Business Continuity Booklet* (March 2008) at http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx.

[12] Refer to SR 13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing," specifically the section titled, "Depository Institutions Subject to the Annual Audit and Reporting Requirements of Section 36 of the FDI Act" at http://www.federalreserve.gov/bankinforeg/srletters/sr1301.htm.
Refer also to SR 03-5, "Amended Interagency Guidance on the Internal Audit Function and its Outsourcing,"

2002 specifically prohibits a registered public accounting firm from performing certain non-audit services for a public company client for whom it performs financial statement audits.

Risk management activities: Financial institutions may outsource various risk management activities, such as aspects of interest rate risk and model risk management. Financial institutions should require service providers to provide information that demonstrates developmental evidence explaining the product components, design, and intended use, to determine whether the products and/or services are appropriate for the institution's exposures and risks.[13] Financial institutions should also have standards and processes in place for ensuring that service providers offering model risk management services, such as validation, do so in a way that is consistent with existing model risk management guidance.

---

particularly the section titled, "Institutions Not Subject to Section 36 of the FDI Act that are Neither Public Companies nor Subsidiaries of Public Companies" at http://www.federalreserve.gov/boarddocs/srletters/2003/sr0305.htm.

[13] Refer to SR 11-7, "Guidance on Model Risk Management" which informs financial institutions of the importance and risk to the use of models and the supervisory expectations that financial institutions should adhere to. http://www.federalreserve.gov/bankinforeg/srletters/sr1107.htm

Office of the Comptroller of the Currency
U.S. Department of the Treasury

OCC 2013-29

Subject: Third-Party Relationships
Date: October 30, 2013

To: Chief Executive Officers and Chief Risk Officers of All National Banks and Federal Savings Associations, Technology Service Providers, Department and Division Heads, All Examining Personnel, and Other Interested Parties

Description: Risk Management Guidance

Summary

This bulletin provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships. A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise.[1]

The Office of the Comptroller of the Currency (OCC) expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.[2]

This bulletin rescinds OCC Bulletin 2001-47, "Third-Party Relationships: Risk Management Principles," and OCC Advisory Letter 2000-9, "Third-Party Risk." This bulletin supplements and should be used in conjunction with other OCC and interagency issuances on third-party relationships and risk management listed in appendix B. In connection with the issuance of this bulletin, the OCC is applying to federal savings associations (FSA) certain guidance applicable to national banks, as indicated in appendix B.

Highlights

- A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.
- A bank should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
- An effective risk management process throughout the life cycle of the relationship includes
  - plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.
  - proper due diligence in selecting a third party.
  - written contracts that outline the rights and responsibilities of all parties.
  - ongoing monitoring of the third party's activities and performance.
  - contingency plans for terminating the relationship in an effective manner.
  - clear roles and responsibilities for overseeing and managing the relationship and risk management process.
  - Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management.
  - Independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.

Note for Community Banks

This guidance applies to all banks with third-party relationships. A community bank should adopt risk management practices commensurate with the level of risk and complexity of its third-party relationships. A community bank's board and management should identify those third-party relationships that involve critical activities and ensure the bank has risk management practices in place to assess, monitor, and manage the risks.

Background

Banks continue to increase the number and complexity of relationships with both foreign and domestic third parties, such as

- outsourcing entire bank functions to third parties, such as tax, legal, audit, or information technology operations.
- outsourcing lines of business or products.
- relying on a single third party to perform multiple activities, often to such an extent that the third party becomes an integral component of the bank's operations.
- working with third parties that engage directly with customers.[3]
- contracting with third parties that subcontract activities to other foreign and domestic providers.
- contracting with third parties whose employees, facilities, and subcontractors may be geographically concentrated.
- working with a third party to address deficiencies in bank operations or compliance with laws or regulations.

The OCC is concerned that the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships. The OCC has identified instances in which bank management has

- failed to properly assess and understand the risks and direct and indirect costs involved in third-party relationships.
- failed to perform adequate due diligence and ongoing monitoring of third-party relationships.
- entered into contracts without assessing the adequacy of a third party's risk management practices.
- entered into contracts that incentivize a third party to take risks that are detrimental to the bank or its customers, in order to maximize the third party's revenues.
- engaged in informal third-party relationships without contracts in place.

These examples represent trends whose associated risks reinforce the need for banks to maintain effective risk management practices over third-party relationships.

Risk Management Life Cycle

The OCC expects a bank to have risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the bank's organizational structures. Therefore, the OCC expects more comprehensive and rigorous oversight and management of third-party relationships that involve ***critical activities***—significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that

- could cause a bank to face significant risk[4] if the third party fails to meet expectations.
- could have significant customer impacts.
- require significant investment in resources to implement the third-party relationship and manage the risk.
- could have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.

An effective third-party risk management process follows a continuous life cycle for all relationships and incorporates the following phases:

Planning: Developing a plan to manage the relationship is often the first step in the third-party risk management process. This step is helpful for many situations but is necessary when a bank is considering contracts with third parties that involve critical activities.

Due diligence and third-party selection: Conducting a review of a potential third party before signing a contract[5] helps ensure that the bank selects an appropriate third party and understands and controls the risks posed by the relationship, consistent with the bank's risk appetite.

Contract negotiation: Developing a contract that clearly defines expectations and responsibilities of the third party helps to ensure the contract's enforceability, limit the bank's liability, and mitigate disputes about performance.

Ongoing monitoring: Performing ongoing monitoring of the third-party relationship once the contract is in place is essential to the bank's ability to manage risk of the third-party relationship.

Termination: Developing a contingency plan to ensure that the bank can transition the activities to another third party, bring the activities in-house, or discontinue the activities when a contract expires, the terms of the contract have been satisfied, in response to contract default, or in response to changes to the bank's or third party's business strategy.

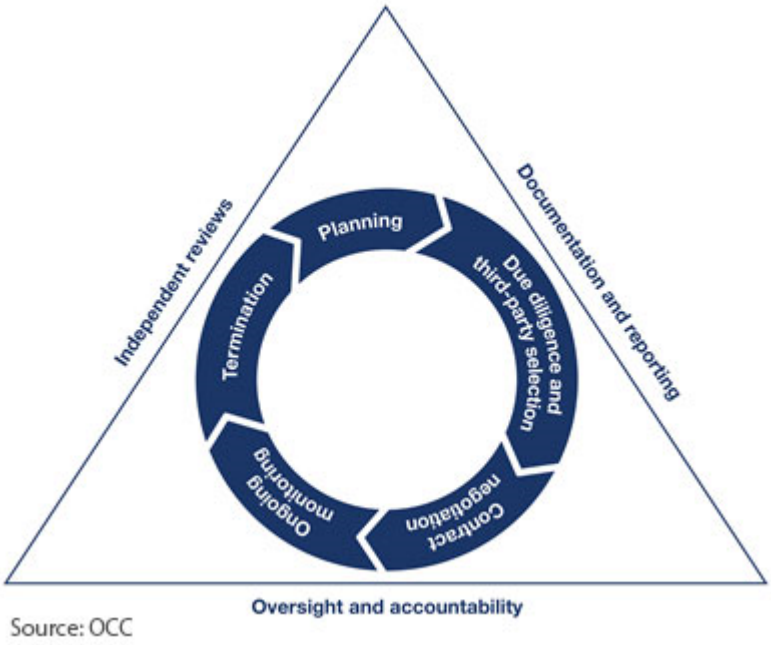
In addition, a bank should perform the following throughout the life cycle of the relationship as part of its risk management process:

Oversight and accountability: Assigning clear roles and responsibilities for managing third-party relationships and integrating the bank's third-party risk management process with its enterprise risk management framework enables continuous oversight and accountability.

Documentation and reporting: Proper documentation and reporting facilitates oversight, accountability, monitoring, and risk management associated with third-party relationships.

Independent reviews: Conducting periodic independent reviews of the risk management process enables management to assess whether the process aligns with the bank's strategy and effectively manages risk posed by third-party relationships**.**

Figure 1: Risk Management Life Cycle



Source: OCC

Planning

Before entering into a third-party relationship, senior management should develop a plan to manage the relationship. The management plan should be commensurate with the level of risk and complexity of the third-party relationship and should

- discuss the risks inherent in the activity.
- outline the strategic purposes (e.g., reduce costs, leverage specialized expertise or technology, augment resources, expand or enhance operations), legal and compliance aspects, and inherent risks associated with using third parties, and discuss how the arrangement aligns with the bank's overall strategic goals, objectives, and risk appetite.
- assess the complexity of the arrangement, such as the volume of activity, potential for subcontractors, the technology needed, and the likely degree of foreign-based third-party support.
- determine whether the potential financial benefits outweigh the estimated costs to control the risks (including estimated direct contractual costs and indirect costs to augment or alter bank processes, systems, or staffing to properly manage the third-party relationship or adjust or terminate existing contracts).
- consider how the third-party relationship could affect other strategic bank initiatives, such as large technology projects, organizational changes, mergers, acquisitions, or divestitures.
- consider how the third-party relationship could affect bank and dual employees[6] and what transition steps are needed to manage the impacts when the activities currently conducted internally are outsourced.
- assess the nature of customer interaction with the third party and potential impact the relationship will have on the bank's customers—including access to or use of those customers' confidential information, joint marketing or franchising arrangements, and handling of customer complaints—and outline plans to manage these impacts.
- assess potential information security implications including access to the bank's systems and to its confidential information.
- consider the bank's contingency plans in the event the bank needs to transition the activity to another third party or bring it in-house.
- assess the extent to which the activities are subject to specific laws and regulations (e.g., privacy, information security, Bank Secrecy Act/Anti-Money Laundering (BSA/AML), fiduciary requirements).
- consider whether the selection of the third party is consistent with the bank's broader corporate policies and practices including its diversity policies and practices.
- detail how the bank will select, assess, and oversee the third party, including monitoring the third party's compliance with the contract.
- be presented to and approved by the bank's board of directors when critical activities are involved.

Due Diligence and Third-Party Selection

A bank should conduct due diligence on all potential third parties before selecting and entering into contracts or relationships. A bank should not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the activity in compliance with all applicable laws and regulations and in a safe and sound manner.

The degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. More extensive due diligence is necessary when a third-party relationship involves critical activities. On-site visits may be useful to understand fully the third party's operations and capacity. If the bank uncovers information that warrants additional scrutiny, it should broaden the scope or assessment methods of the due diligence as needed.

The bank should consider the following during due diligence:

Strategies and Goals

Review the third party's overall business strategy and goals to ensure they do not conflict with those of the bank. Consider how the third party's current and proposed strategic business arrangements (such as mergers, acquisitions, divestitures, joint ventures, or joint marketing initiatives) may affect the activity. Also consider reviewing the third party's service philosophies, quality initiatives, efficiency improvements, and employment policies and practices.

Legal and Regulatory Compliance

Evaluate the third party's legal and regulatory compliance program to determine whether the third party has the necessary licenses to operate and the expertise, processes, and controls to enable the bank to remain compliant with domestic and international laws and regulations. Check compliance status with regulators and self-regulatory organizations as appropriate.

Financial Condition

Assess the third party's financial condition, including reviews of the third party's audited financial statements. Evaluate growth, earnings, pending litigation, unfunded liabilities, and other factors that may affect the third party's overall financial stability. Depending on the significance of the third-party relationship, the bank's analysis may be as comprehensive as if extending credit to the third party.

Business Experience and Reputation

Evaluate the third party's depth of resources and previous experience providing the specific activity. Assess the third party's reputation, including history of customer complaints or litigation. Determine how long the third party has been in business, its market share for the activities, and whether there have been significant changes in the activities offered or in its business model. Conduct reference checks with external organizations and agencies such as the industry associations, Better Business Bureau, Federal Trade Commission, state attorneys general offices, state consumer affairs offices, and similar foreign authorities. Check U.S. Securities and Exchange Commission or other regulatory filings. Review the third party's Web sites and other marketing materials to ensure that statements and assertions are in-line with the bank's expectations and do not overstate or misrepresent activities and capabilities. Determine whether and how the third party plans to use the bank's name and reputation in marketing efforts.

Fee Structure and Incentives

Evaluate the third party's normal fee structure and incentives for similar business arrangements to determine if the fee structure and incentives would create burdensome upfront fees or result in inappropriate risk taking by the third party or the bank.

Qualifications, Backgrounds, and Reputations of Company Principals

Ensure the third party periodically conducts thorough background checks on its senior management and employees as well as on subcontractors who may have access to critical systems or confidential information. Ensure that third parties have policies and procedures in place for removing employees who do not meet minimum background check requirements.

Risk Management

Evaluate the effectiveness of the third party's risk management program, including policies, processes, and internal controls. Where applicable, determine whether the third party's internal audit function independently and effectively tests and reports on the third party's internal controls. Evaluate processes for escalating, remediating, and holding management accountable for concerns identified during audits or other independent tests. If available, review Service Organization Control (SOC) reports, prepared in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 16 (SSAE 16). Consider whether these reports

contain sufficient information to assess the third party's risk or whether additional scrutiny is required through an audit by the bank or other third party at the bank's request. Consider any certification by independent third parties for compliance with domestic or international internal control standards (e.g., the National Institute of Standards and Technology and the International Standards Organization).

Information Security

Assess the third party's information security program. Determine whether the third party has sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities. When technology is necessary to support service delivery, assess the third party's infrastructure and application security programs, including the software development life cycle and results of vulnerability and penetration tests. Evaluate the third party's ability to implement effective and sustainable corrective actions to address deficiencies discovered during testing.

Management of Information Systems

Gain a clear understanding of the third party's business processes and technology that will be used to support the activity. When technology is a major component of the third-party relationship, review both the bank's and the third party's information systems to identify gaps in service-level expectations, technology, business process and management, or interoperability issues. Review the third party's processes for maintaining accurate inventories of its technology and its subcontractors. Assess the third party's change management processes to ensure that clear roles, responsibilities, and segregation of duties are in place. Understand the third party's performance metrics for its information systems and ensure they meet the bank's expectations.

Resilience

Assess the third party's ability to respond to service disruptions or degradations resulting from natural disasters, human error, or intentional physical or cyber attacks. Determine whether the third party maintains disaster recovery and business continuity plans that specify the time frame to resume activities and recover data. Review the third party's telecommunications redundancy and resilience plans and preparations for known and emerging threats and vulnerabilities, such as wide-scale natural disasters, distributed denial of service attacks, or other intentional or unintentional events. Review the results of business continuity testing and performance during actual disruptions.

Incident-Reporting and Management Programs

Review the third party's incident reporting and management programs to ensure there are clearly documented processes and accountability for identifying, reporting, investigating, and escalating incidents. Ensure that the third party's escalation and notification processes meet the bank's expectations and regulatory requirements.

Physical Security

Evaluate whether the third party has sufficient physical and environmental controls to ensure the safety and security of its facilities, technology systems, and employees.

Human Resource Management

Review the third party's program to train and hold employees accountable for compliance with policies and procedures. Review the third party's succession and redundancy planning for key management and support personnel. Review training programs to ensure that the third party's staff is knowledgeable about changes in laws, regulations, technology, risk, and other factors that may affect the quality of the activities provided.

Reliance on Subcontractors

Evaluate the volume and types of subcontracted activities and the subcontractors' geographic locations. Evaluate the third party's ability to assess, monitor, and mitigate risks from its use of subcontractors and to ensure that the same level of quality and controls exists no matter where the subcontractors' operations reside. Evaluate whether additional concentration-related risks may arise from the third party's reliance on subcontractors and, if necessary, conduct similar due diligence on the third party's critical subcontractors.

Insurance Coverage

Verify that the third party has fidelity bond coverage to insure against losses attributable to dishonest acts, liability coverage for losses attributable to negligent acts, and hazard insurance covering fire, loss of data, and protection of documents. Determine whether the third party has insurance coverage for its intellectual property rights, as such coverage may not be available under a general commercial policy. The amounts of such coverage should be commensurate with the level of risk involved with the third party's operations and the type of activities to be provided.

Conflicting Contractual Arrangements With Other Parties

Obtain information regarding legally binding arrangements with subcontractors or other parties in cases where the third party has indemnified itself, as such arrangements may transfer risks to the bank. Evaluate the potential legal and financial implications to the bank of these contracts between the third party and its subcontractors or other parties.

Senior management should review the results of the due diligence to determine whether the third party is able to meet the bank's expectations and whether the bank should proceed with the third-party relationship. If the results do not meet expectations, management should recommend that the third party make appropriate changes, find an alternate third party, conduct the activity in-house, or discontinue the activity. As part of any recommended changes, the bank may need to supplement the third party's resources or increase or implement new controls to manage the risks. Management should present results of due diligence to the board when making recommendations for third-party relationships that involve critical activities.

Contract Negotiation

Once the bank selects a third party, management should negotiate a contract that clearly specifies the rights and responsibilities of each party to the contract. Additionally, senior management should obtain board approval of the contract before its execution when a third-party relationship will involve critical activities. A bank should review existing contracts periodically, particularly those involving critical activities, to ensure they continue to address pertinent risk controls and legal protections. Where problems are identified, the bank should seek to renegotiate at the earliest opportunity.

Contracts should generally address the following:

Nature and Scope of Arrangement

Ensure that the contract specifies the nature and scope of the arrangement. For example, a third-party contract should specifically identify the frequency, content, and format of the service, product, or function provided. Include in the contract, as applicable, such ancillary services as software or other technology support and maintenance, employee training, and customer service. Specify which activities the third party is to conduct, whether on or off the bank's premises, and describe the terms governing the use of the bank's information, facilities, personnel, systems, and equipment, as well as access to and use of the bank's or customers' information. When dual employees will be used, clearly articulate their responsibilities and reporting lines.[7]

Performance Measures or Benchmarks

Specify performance measures that define the expectations and responsibilities for both parties including conformance with regulatory standards or rules. Such measures can be used to motivate the third party's performance, penalize poor performance, or reward outstanding performance. Performance measures should not incentivize undesirable performance, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on customers. Industry standards for service-level agreements may provide a reference point for standardized services, such as payroll processing. For more customized activities, there may be no standard measures. Instead, the bank and third party should agree on appropriate measures.

Responsibilities for Providing, Receiving, and Retaining Information

Ensure that the contract requires the third party to provide and retain timely, accurate, and comprehensive information such as records and reports that allow bank management to monitor performance, service levels, and risks. Stipulate the frequency and type of reports required, for example: performance reports, control audits, financial statements, security reports, BSA/AML and Office of Foreign Asset Control (OFAC) compliance responsibilities and reports for monitoring potential suspicious activity, reports for monitoring customer complaint activity, and business resumption testing reports.

Ensure that the contract sufficiently addresses

- the responsibilities and methods to address failures to adhere to the agreement including the ability of both parties to the agreement to exit the relationship.
- the prompt notification of financial difficulty, catastrophic events, and significant incidents such as information breaches, data loss, service or system interruptions, compliance lapses, enforcement actions, or other regulatory actions.
- the bank's materiality thresholds and procedures for notifying the bank in writing whenever service disruptions, security breaches, or other events pose a significant risk to the bank.
- notification to the bank before making significant changes to the contracted activities, including acquisition, subcontracting, off-shoring, management or key personnel changes, or implementing new or revised policies, processes, and information technology.
- notification to the bank of significant strategic business changes, such as mergers, acquisitions, joint ventures, divestitures, or other business activities that could affect the activities involved.
- the ability of the third party to resell, assign, or permit access to the bank's data and systems to other entities.

- the bank's obligations to notify the third party if the bank implements strategic or operational changes or experiences significant incidents that may affect the third party.

The Right to Audit and Require Remediation

Ensure that the contract establishes the bank's right to audit, monitor performance, and require remediation when issues are identified. Generally, a third-party contract should include provisions for periodic independent internal or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the bank's in-house functions to monitor performance with the contract. A bank should include in the contract the types and frequency of audit reports the bank is entitled to receive from the third party (e.g., financial, SSAE 16, SOC 1, SOC 2, and SOC 3 reports, and security reviews). Consider whether to accept audits conducted by the third party's internal or external auditors. Reserve the bank's right to conduct its own audits of the third party's activities or to engage an independent party to perform such audits. Audit reports should include a review of the third party's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.

Responsibility for Compliance With Applicable Laws and Regulations

Ensure the contract addresses compliance with the specific laws, regulations, guidance, and self-regulatory standards applicable to the activities involved, including provisions that outline compliance with certain provisions of the Gramm-Leach-Bliley Act (GLBA) (including privacy and safeguarding of customer information); BSA/AML; OFAC; and Fair Lending and other consumer protection laws and regulations. Ensure that the contract requires the third party to maintain policies and procedures which address the bank's right to conduct periodic reviews so as to verify the third party's compliance with the bank's policies and expectations. Ensure that the contract states the bank has the right to monitor on an ongoing basis the third party's compliance with applicable laws, regulations, and policies and requires remediation if issues arise.

Cost and Compensation

Fully describe compensation, fees, and calculations for base services, as well as any fees based on volume of activity and for special requests. Ensure the contracts do not include burdensome upfront fees or incentives that could result in inappropriate risk taking by the bank or third party. Indicate which party is responsible for payment of legal, audit, and examination fees associated with the activities involved. Consider outlining cost and responsibility for purchasing and maintaining hardware and software. Specify the conditions under which the cost structure may be changed, including limits on any cost increases.

Ownership and License

State whether and how the third party has the right to use the bank's information, technology, and intellectual property, such as the bank's name, logo, trademark, and copyrighted material. Indicate whether any records generated by the third party become the bank's property. Include appropriate warranties on the part of the third party related to its acquisition of licenses for use of any intellectual property developed by other third parties. If the bank purchases software, establish escrow agreements to provide for the bank's access to source code and programs under certain conditions (e.g., insolvency of the third party).

Confidentiality and Integrity

Prohibit the third party and its subcontractors from using or disclosing the bank's information, except as necessary to provide the contracted activities or comply with legal requirements. If the third party receives bank customers' personally identifiable information, the contract should ensure that the third party implements and maintains appropriate security measures to comply with privacy regulations and regulatory guidelines. Specify when and how the third party will disclose, in a timely manner, information security breaches that have resulted in unauthorized intrusions or access that may materially affect the bank or its customers. Stipulate that intrusion notifications include estimates of the effects on the bank and specify corrective action to be taken by the third party. Address the powers of each party to change security and risk management procedures and requirements, and resolve any confidentiality and integrity issues arising out of shared use of facilities owned by the third party. Stipulate whether and how often the bank and the third party will jointly practice incident management plans involving unauthorized intrusions or other breaches in confidentiality and integrity.

Business Resumption and Contingency Plans

Ensure the contract provides for continuation of the business function in the event of problems affecting the third party's operations, including degradations or interruptions resulting from natural disasters, human error, or intentional attacks. Stipulate the third party's responsibility for backing up and otherwise protecting programs, data, and equipment, and for maintaining current and sound business resumption and contingency plans. Include provisions—in the event of the third party's bankruptcy, business failure, or business interruption—for transferring the bank's accounts or activities to another third party without penalty.

Ensure that the contract requires the third party to provide the bank with operating procedures to be carried out in the event business resumption and disaster recovery plans are implemented. Include specific time frames for business resumption and recovery that meet the bank's requirements, and when appropriate, regulatory requirements. Stipulate whether and how often the bank and the third party will jointly practice business resumption and disaster recovery plans.

Indemnification

Consider including indemnification clauses that specify the extent to which the bank will be held liable for claims that cite failure of the third party to perform, including failure of the third party to obtain any necessary intellectual property licenses. Carefully assess indemnification clauses that require the bank to hold the third party harmless from liability.

Insurance

Stipulate that the third party is required to maintain adequate insurance, notify the bank of material changes to coverage, and provide evidence of coverage where appropriate. Types of insurance coverage may include fidelity bond coverage, liability coverage, hazard insurance, and intellectual property insurance.

Dispute Resolution

Consider whether the contract should establish a dispute resolution process (arbitration, mediation, or other means) to resolve problems between the bank and the third party in an expeditious manner, and whether the third party should continue to provide activities to the bank during the dispute resolution period.

Limits on Liability

Determine whether the contract limits the third party's liability and whether the proposed limit is in proportion to the amount of loss the bank might experience because of the third party's failure to perform or to comply with applicable laws. Consider whether a contract would subject the bank to undue risk of litigation, particularly if the third party violates or is accused of violating intellectual property rights.

Default and Termination

Ensure that the contract stipulates what constitutes default, identifies remedies and allows opportunities to cure defaults, and stipulates the circumstances and responsibilities for termination. Determine whether it includes a provision that enables the bank to terminate the contract, upon reasonable notice and without penalty, in the event that the OCC formally directs the bank to terminate the relationship. Ensure the contract permits the bank to terminate the relationship in a timely manner without prohibitive expense. Include termination and notification requirements with time frames to allow for the orderly conversion to another third party. Provide for the timely return or destruction of the bank's data and other resources and ensure the contract provides for ongoing monitoring of the third party after the contract terms are satisfied as necessary. Clearly assign all costs and obligations associated with transition and termination.

Customer Complaints

Specify whether the bank or third party is responsible for responding to customer complaints. If it is the third party's responsibility, specify provisions that ensure that the third party receives and responds timely to customer complaints and forwards a copy of each complaint and response to the bank. The third party should submit sufficient, timely, and usable information to enable the bank to analyze customer complaint activity and trends for risk management purposes.

Subcontracting

Stipulate when and how the third party should notify the bank of its intent to use a subcontractor. Specify the activities that cannot be subcontracted or whether the bank prohibits the third party from subcontracting activities to certain locations or specific subcontractors. Detail the contractual obligations—such as reporting on the subcontractor's conformance with performance measures, periodic audit results, compliance with laws and regulations, and other contractual obligations. State the third party's liability for activities or actions by its subcontractors and which party is responsible for the costs and resources required for any additional monitoring and management of the subcontractors. Reserve the right to terminate the contract without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract.

Foreign-Based Third Parties

Include in contracts with foreign-based third parties choice-of-law covenants and jurisdictional covenants that provide for adjudication of all disputes between the parties under the laws of a single, specific jurisdiction. Understand that such contracts and covenants may be subject, however, to the interpretation of foreign courts relying on local laws. Foreign courts and laws may differ substantially from U.S. courts and laws in the application and enforcement of

choice-of-law covenants, requirements on banks, protection of privacy of customer information, and the types of information that the third party or foreign governmental entities will provide upon request. Therefore, seek legal advice to ensure the enforceability of all aspects of a proposed contract with a foreign-based third party and other legal ramifications of each such arrangement.

OCC Supervision

In contracts with service providers, stipulate that the performance of activities by external parties for the bank is subject to OCC examination oversight, including access to all work papers, drafts, and other materials. The OCC treats as subject to 12 USC 1867(c) and 12 USC 1464(d)(7), situations in which a bank arranges, by contract or otherwise, for the performance of any applicable functions of its operations. Therefore, the OCC generally has the authority to examine and to regulate the functions or operations performed or provided by third parties to the same extent as if they were performed by the bank itself on its own premises.[8]

Ongoing Monitoring

Ongoing monitoring for the duration of the third-party relationship is an essential component of the bank's risk management process. More comprehensive monitoring is necessary when the third-party relationship involves critical activities. Senior management should periodically assess existing third-party relationships to determine whether the nature of the activity performed now constitutes a critical activity.

After entering into a contract with a third party, bank management should dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third party commensurate with the level of risk and complexity of the relationship. Regular on site visits may be useful to understand fully the third party's operations and ongoing ability to meet contract requirements. Management should ensure that bank employees that directly manage third-party relationships monitor the third party's activities and performance. A bank should pay particular attention to the quality and sustainability of the third party's controls, and its ability to meet service-level agreements, performance metrics and other contractual terms, and to comply with legal and regulatory requirements.

The OCC expects the bank's ongoing monitoring of third-party relationships to cover the due diligence activities discussed earlier. Because both the level and types of risks may change over the lifetime of third-party relationships, a bank should ensure that its ongoing monitoring adapts accordingly. This monitoring may result in changes to the frequency and types of required reports from the third party, including service-level agreement performance reports, audit reports, and control testing results. In addition to ongoing review of third-party reports, some key areas of consideration for ongoing monitoring may include assessing changes to the third party's

- business strategy (including acquisitions, divestitures, joint ventures) and reputation (including litigation) that may pose conflicting interests and impact its ability to meet contractual obligations and service-level agreements.
- compliance with legal and regulatory requirements.
- financial condition.
- insurance coverage.
- key personnel and ability to retain essential knowledge in support of the activities.
- ability to effectively manage risk by identifying and addressing issues before they are cited in audit reports.
- process for adjusting policies, procedures, and controls in response to changing threats and new vulnerabilities and material breaches or other serious incidents.
- information technology used or the management of information systems.
- ability to respond to and recover from service disruptions or degradations and meet business resilience expectations.
- reliance on, exposure to, or performance of subcontractors; location of subcontractors; and the ongoing monitoring and control testing of subcontractors.
- agreements with other entities that may pose a conflict of interest or introduce reputation, operational, or other risks to the bank.
- ability to maintain the confidentiality and integrity of the bank's information and systems.
- volume, nature, and trends of consumer complaints, in particular those that indicate compliance or risk management problems.
- ability to appropriately remediate customer complaints.

Bank employees who directly manage third-party relationships should escalate to senior management significant issues or concerns arising from ongoing monitoring, such as an increase in risk, material weaknesses and repeat audit findings, deterioration in financial condition, security breaches, data loss, service or system interruptions, or compliance lapses. Additionally, management should ensure that the bank's controls to manage risks from third-party relationships are tested regularly, particularly where critical activities are involved. Based on the results of the ongoing monitoring and internal control testing, management should respond to issues when identified including escalating significant issues to the board.

Termination

A bank may terminate third-party relationships for various reasons, including

- expiration or satisfaction of the contract.
- desire to seek an alternate third party.
- desire to bring the activity in-house or discontinue the activity.
- breach of contract.

Management should ensure that relationships terminate in an efficient manner, whether the activities are transitioned to another third party or in-house, or discontinued. In the event of contract default or termination, the bank should have a plan to bring the service in-house if there are no alternate third parties. This plan should cover

- capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise.
- risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship.
- handling of joint intellectual property developed during the course of the arrangement.
- reputation risks to the bank if the termination happens as a result of the third party's inability to meet expectations.

The extent and flexibility of termination rights may vary with the type of activity.

Oversight and Accountability

The bank's board of directors (or a board committee) and senior management are responsible for overseeing the bank's overall risk management processes. The board, senior management, and employees within the lines of businesses who manage the third-party relationships have distinct but interrelated responsibilities to ensure that the relationships and activities are managed effectively and commensurate with their level of risk and complexity, particularly for relationships that involve critical activities:[9]

Board of Directors

- Ensure an effective process is in place to manage risks related to third-party relationships in a manner consistent with the bank's strategic goals, organizational objectives, and risk appetite.
- Approve the bank's risk-based policies that govern the third-party risk management process and identify critical activities.
- Review and approve management plans for using third parties that involve critical activities.
- Review summary of due diligence results and management's recommendations to use third parties that involve critical activities.
- Approve contracts with third parties that involve critical activities.
- Review the results of management's ongoing monitoring of third-party relationships involving critical activities.
- Ensure management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring.
- Review results of periodic independent reviews of the bank's third-party risk management process.

Senior Bank Management

- Develop and implement the bank's third-party risk management process.
- Establish the bank's risk-based policies to govern the third-party risk management process.
- Develop plans for engaging third parties, identify those that involve critical activities, and present plans to the board when critical activities are involved.
- Ensure appropriate due diligence is conducted on potential third parties and present results to the board when making recommendations to use third parties that involve critical activities.
- Review and approve contracts with third parties. Board approval should be obtained for contracts that involve critical activities.
- Ensure ongoing monitoring of third parties, respond to issues when identified, and escalate significant issues to the board.
- Ensure appropriate documentation and reporting throughout the life cycle for all third-party relationships.
- Ensure periodic independent reviews of third-party relationships that involve critical activities and of the bank's third-party risk management process. Analyze the results, take appropriate actions, and report results to the board.
- Hold accountable the bank employees within business lines or functions who manage direct relationships with third parties.
- Terminate arrangements with third parties that do not meet expectations or no longer align with the bank's strategic goals, objectives, or risk appetite.
- Oversee enterprise-wide risk management and reporting of third-party relationships.

Bank Employees Who Directly Manage Third-Party Relationships

- Conduct due diligence of third parties and report results to senior management.

- Ensure that third parties comply with the bank's policies and reporting requirements.
- Perform ongoing monitoring of third parties and ensure compliance with contract terms and service-level agreements.
- Ensure the bank or the third party addresses any issues identified.
- Escalate significant issues to senior management.
- Notify the third party of significant operational issues at the bank that may affect the third party.
- Ensure that the bank has regularly tested controls in place to manage risks associated with third-party relationships.
- Ensure that third parties regularly test and implement agreed-upon remediation when issues arise.
- Maintain appropriate documentation throughout the life cycle.
- Respond to material weaknesses identified by independent reviews.
- Recommend termination of arrangements with third parties that do not meet expectations or no longer align with the bank's strategic goals, objectives, or risk appetite.

Documentation and Reporting

A bank should properly document and report on its third-party risk management process and specific arrangements throughout their life cycle. Proper documentation and reporting facilitates the accountability, monitoring, and risk management associated with third parties and typically includes

- a current inventory of all third-party relationships, which should clearly identify those relationships that involve critical activities and delineate the risks posed by those relationships across the bank.[10]
- approved plans for the use of third-party relationships.
- due diligence results, findings, and recommendations.
- analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the bank.
- executed contracts.
- regular risk management and performance reports required and received from the third party (e.g., audit reports, security reviews, and reports indicating compliance with service-level agreements).
- regular reports to the board and senior management on the results of internal control testing and ongoing monitoring of third parties involved in critical activities.
- regular reports to the board and senior management on the results of independent reviews of the bank's overall risk management process.

Independent Reviews

Senior management should ensure that periodic independent reviews are conducted on the third-party risk management process, particularly when a bank involves third parties in critical activities. The bank's internal auditor or an independent third party may perform the reviews, and senior management should ensure the results are reported to the board. Reviews may include assessing the adequacy of the bank's process for

- ensuring third-party relationships align with the bank's business strategy.
- identifying, assessing, managing, and reporting on risks of third-party relationships.
- responding to material breaches, service disruptions, or other material issues.
- identifying and managing risks associated with complex third-party relationships, including foreign-based third parties and subcontractors.
- involving multiple disciplines across the bank as appropriate during each phase of the third-party risk management life cycle.[11]
- ensuring appropriate staffing and expertise to perform due diligence and ongoing monitoring and management of third parties.
- ensuring oversight and accountability for managing third-party relationships (e.g., whether roles and responsibilities are clearly defined and assigned and whether the individuals possess the requisite expertise, resources, and authority).
- ensuring that conflicts of interest or appearances of conflicts of interest do not exist when selecting or overseeing third parties.
- identifying and managing concentration risks that may arise from relying on a single third party for multiple activities, or from geographic concentration of business due to either direct contracting or subcontracting agreements to the same locations.

Senior management should analyze the results of independent reviews to determine whether and how to adjust the bank's third-party risk management process, including policy, reporting, resources, expertise, and controls. Additionally, the results may assist senior management's understanding of the effectiveness of the bank's third-party risk management process so that they can make informed decisions about commencing new or continuing existing third-party relationships, bringing activities in-house, or discontinuing activities. Management should respond promptly and thoroughly to significant issues or concerns identified and escalate to the board if the risk posed is approaching the bank's risk appetite limits.

Supervisory Reviews of Third-Party Relationships

The OCC expects bank management to engage in a robust analytical process to identify, measure, monitor, and control the risks associated with third-party relationships and to avoid excessive risk taking that may threaten a bank's safety and soundness. A bank's failure to have an effective third-party risk management process that is commensurate with the level of risk, complexity of third-party relationships, and organizational structure of the bank may be *an unsafe and unsound banking practice.*

When reviewing third-party relationships, examiners should

- assess the bank's ability to oversee and manage its relationships.
- highlight and discuss material risks and any deficiencies in the bank's risk management process with the board of directors and senior management.
- carefully review the bank's plans for appropriate and sustainable remediation of such deficiencies, particularly those associated with the oversight of third parties that involve critical activities.
- follow existing guidance for citing deficiencies in supervisory findings and reports of examination, and recommend appropriate supervisory actions. These actions may range from citing the deficiencies in Matters Requiring Attention to recommending formal enforcement action.
- consider the findings when assigning the management component of the Federal Financial Institutions Examination Council's (FFIEC) Uniform Financial Institutions Rating System (CAMELS ratings).[12] Serious deficiencies may result in management being deemed less than satisfactory.
- reflect the associated risks in their overall assessment of the bank's risk profile.

When circumstances warrant, the OCC may use its authority to examine the functions or operations performed by a third party on the bank's behalf. Such examinations may evaluate safety and soundness risks, the financial and operational viability of the third party to fulfill its contractual obligations, compliance with applicable laws and regulations, including consumer protection, fair lending, BSA/AML and OFAC laws, and whether the third party engages in unfair or deceptive acts or practices in violation of federal or applicable state law. The OCC will pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by the bank or its third party. The OCC has the authority to assess a bank a special examination or investigation fee when the OCC examines or investigates the activities of a third party for the bank.

Further Information

Please contact John Eckert, Director, Operational Risk and Core Policy, at (202) 649-7163.

John C. Lyons Jr.
Senior Deputy Comptroller and Chief National Bank Examiner

Appendix A: Risks Associated With Third-Party Relationships
Appendix B: References

APPENDIX A: Risks Associated With Third-Party Relationships

Use of third parties reduces management's direct control of activities and may introduce new or increase existing risks, specifically, operational, compliance, reputation, strategic, and credit risks and the interrelationship of these risks. Increased risk most often arises from greater complexity, ineffective risk management by the bank, and inferior performance by the third party. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for an expanded discussion of banking risks and their definitions.

Operational Risk

Operational risk is present in all products, services, functions, delivery channels, and processes. Third-party relationships may increase a bank's exposure to operational risk because the bank may not have direct control of the activity performed by the third party.

Operational risk can increase significantly when third-party relationships result in concentrations. Concentrations may arise when a bank relies on a single third party for multiple activities, particularly when several of the activities are critical to bank operations. Additionally, geographic concentrations can arise when a bank's own operations and that of its third parties and subcontractors are located in the same region or are dependent on the same critical power and telecommunications infrastructures.

Compliance Risk

Compliance risk exists when products, services, or systems associated with third-party relationships are not properly reviewed for compliance or when the third party's operations are not consistent with laws, regulations, ethical standards, or the bank's policies and procedures. Such risks also arise when a third party implements or manages a product or service in a manner that is unfair, deceptive, or abusive to the recipient of the product or service. Compliance risk may arise when a bank licenses or uses technology from a third party that violates a third party's intellectual property rights. Compliance risk may also arise when the third party does not adequately monitor and report transactions for suspicious activities to the bank under the BSA or OFAC. The potential for serious or frequent violations or noncompliance exists when a bank's oversight program does not include appropriate audit and control features, particularly when the third party is implementing new bank activities or expanding existing ones, when activities are further subcontracted, when activities are conducted in foreign countries, or when customer and employee data is transmitted to foreign countries.

Compliance risk increases when conflicts of interest between a bank and a third party are not appropriately managed, when transactions are not adequately monitored for compliance with all necessary laws and regulations, and when a bank or its third parties have not implemented appropriate controls to protect consumer privacy and customer and bank records. Compliance failures by the third party could result in litigation or loss of business to the bank and damage to the bank's reputation.

Reputation Risk

Third-party relationships that do not meet the expectations of the bank's customers expose the bank to reputation risk. Poor service, frequent or prolonged service disruptions, significant or repetitive security lapses, inappropriate sales recommendations, and violations of consumer law and other law can result in litigation, loss of business to the bank, or negative perceptions in the marketplace. Publicity about adverse events surrounding the third parties also may increase the bank's reputation risk. In addition, many of the products and services involved in franchising arrangements expose banks to higher reputation risks. Franchising the bank's attributes often includes direct or subtle reference to the bank's name. Thus, the bank is permitting its attributes to be used in connection with the products and services of a third party. In some cases, however, it is not until something goes wrong with the third party's products, services, or client relationships, that it becomes apparent to the third party's clients that the bank is involved or plays a role in the transactions. When a bank is offering products and services actually originated by third parties as its own, the bank can be exposed to substantial financial loss and damage to its reputation if it fails to maintain adequate quality control over those products and services and adequate oversight over the third party's activities.

Strategic Risk

A bank is exposed to strategic risk if it uses third parties to conduct banking functions or offer products and services that are not compatible with the bank's strategic goals, cannot be effectively monitored and managed by the bank, or do not provide an adequate return on investment. Strategic risk exists in a bank that uses third parties in an effort to remain competitive, increase earnings, or control expense without fully performing due diligence reviews or implementing the appropriate risk management infrastructure to oversee the activity. Strategic risk also arises if management does not possess adequate expertise and experience to oversee properly the third-party relationship.

Conversely, strategic risk can arise if a bank does not use third parties when it is prudent to do so. For example, a bank may introduce strategic risk when it does not leverage third parties that possess greater expertise than the bank does internally, when the third party can more cost effectively supplement internal expertise, or when the third party is more efficient at providing a service with better risk management than the bank can provide internally.

Credit Risk

Credit risk may arise when management has exercised ineffective due diligence and oversight of third parties that market or originate certain types of loans on the bank's behalf, resulting in low-quality receivables and loans. Ineffective oversight of third parties can also result in poor account management, customer service, or collection activities. Likewise, where third parties solicit and refer customers, conduct underwriting analysis, or set up product programs on behalf of the bank, substantial credit risk may be transferred to the bank if the third party is unwilling or unable to fulfill its obligations.

Credit risk also may arise from country or sovereign exposure. To the extent that a bank engages a foreign-based third party, either directly or through subcontractors, the bank may expose itself to country risk.

APPENDIX B: References

Additional guidance about third-party relationships and risk management practices can be found in the following documents.[13]

OCC Guidance

Issuance	Date	Subject	Description/Applicability to FSAs
Comptroller's Handbook	Various	Asset Management series	Each of the booklets in the Comptroller's Handbook Asset Management series provides guidance on oversight of third-party providers. **Applies to FSAs.**
Comptroller's Handbook	September 2013	Other Real Estate Owned	Provides guidance on managing foreclosed properties, including risk management of third-party relationships. **Applies to FSAs.**
Comptroller's Handbook	April 2012	SAFE Act	Provides procedures for examining mortgage loan originator (MLO) activities for compliance with the Secure & Fair Enforcement & Licensing Act of 2008, which mandates a nationwide licensing and registration system for residential MLOs. MLOs may be employees of a bank or third-party vendors. **Applies to FSAs.**
Comptroller's Handbook	May 2011	Servicemembers Civil Relief Act of 2003 (SCRA)	Provides guidance on SCRA requirements applicable to banks and servicers, as a large number of banks outsource loan-servicing functions such as credit administration to third-party servicers.
Comptroller's Handbook	December 2010	Truth in Lending Act	Provides guidance to banks and servicers on the content and timing of disclosures; interest rate calculations; and prohibited activities.
Comptroller's Handbook	September 2010	Real Estate Settlement Procedures	Provides guidance to banks and servicers on the content and timing of pre-settlement and settlement disclosures to borrowers and on prohibited practices.
Comptroller's Handbook	January 2010	Fair Lending	Provides guidance on indicators of potential disparate treatment in loan servicing and loss mitigation; use of vendor-designed credit scorecards; and guidance on evaluating third parties.
Comptroller's Handbook	April 2003	Internal and External Audits	Provides guidelines for banks that outsource internal audit.
Comptroller's Handbook	December 2001	Merchant Processing	Provides guidance on risk management of third-party processors.
Comptroller's Handbook	February 1994	Retail Nondeposit Investment Sales	Provides guidance on risk management and board oversight of third-party vendors selling nondeposit investment products. (See OCC Bulletin 1994-13)
Alert 2012-16	December 21, 2012	Information Security: Distributed Denial of Service Attacks and Customer Account Fraud	Highlights the risks related to these attacks; raises awareness for banks to be prepared to mitigate associated risks. Preparation may include ensuring sufficient resources in conjunction with pre-contracted third-party servicers that can assist in managing the internet-based traffic flow. **Applies to FSAs.**
Alert 2001-4	April 24, 2001	Network Securities Vulnerabilities	Alerts banks to review contracts with service providers to ensure that security maintenance and reporting responsibilities are clearly described.
News Release 2013-116	July 17, 2013	OCC Statement Regarding Oversight of Debt Collection and Debt Sales	Appendix provides guidance on the due diligence and ongoing monitoring of third parties to which banks sell consumer debt. **Applies to FSAs.**
News Release 2012-93	June 21, 2012	Regulators Issue Joint Guidance to Address Mortgage Servicer Practices that Affect Servicemembers	Provides guidance to banks and mortgage servicers, including ensuring that their employees are adequately trained about the options available for homeowners with permanent change of station orders. **Applies to FSAs.**

Bulletin 2013-10	March 29, 2013	Flood Disaster Protection Act: Interagency Statement on Effective Dates of Certain Provisions of the Biggert–Waters Act and Impact on Proposed Interagency Questions and Answers	Provides guidance to lenders or their servicers regarding the contents of notifications to borrowers about flood insurance renewals, force placement to ensure continuity of coverage, use of private flood insurance policies, related insurance fees, and escrow accounts. Provides summaries of new requirements for disclosure contents and timing. **Applies to FSAs.**
Bulletin 2011-39	September 22, 2011	Fair Credit Reporting and Equal Credit Opportunity Acts—Risk-Based Pricing Notices: Final Rules	Provides guidance on notification requirements (timing, content) when adverse credit decision relies on a credit score, including those generated by third-party vendors (i.e., consumer reporting agencies). **Applies to FSAs.**
Bulletin 2011-30	July 6, 2011	Counterparty Credit Risk Management: Interagency Supervisory Guidance	Addresses some of the weaknesses highlighted by the recent financial crisis and reinforces sound governance of counterparty credit risk (CCR) management practices through prudent board and senior management oversight and an effective CCR management framework. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2011-29	June 30, 2011	Foreclosure Management: Supervisory Guidance	Discusses third-party vendor management and reaffirms expectations that management should properly structure, carefully conduct, and prudently manage relationships with third-party vendors, including outside law firms assisting in the foreclosure process. **Applies to FSAs.**
Bulletin 2011-27	June 28, 2011	Prepaid Access Programs: Risk Management Guidance and Sound Practices	Highlights the risks and provides risk management guidance concerning prepaid access programs. **Applies to FSAs.**
Bulletin 2011-26	June 28, 2011	Authentication in an Internet Banking Environment: Supplement	Reinforces the guidance's risk management framework and updates expectations regarding banks' authentications systems and practices whether they are provided internally or by a technology service provider. **Applies to FSAs.**
Bulletin 2011-12	April 4, 2011	Sound Practices for Model Risk Management: Supervisory Guidance	Includes guidance on the use of third-party models. **Applies to FSAs.**
Bulletin 2011-11	March 29, 2011	Risk Management Elements: Collective Investment Funds and Outsourcing Arrangements	Expands upon long-standing guidance on sound risk management and beneficiary/participant protections for bank-offered collective investment funds (CIF). The focus is on supervisory concerns that arise if a bank delegates responsibility for a bank CIF to a third-party service provider, such as a registered investment adviser. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2010-42	December 10, 2010	Sound Practices for Appraisals and Evaluations: Interagency Appraisal and Evaluation Guidelines	Provides guidance regarding a bank's responsibility for selecting appraisers and people performing evaluations based on their competence, experience, and knowledge of the market and type of property being valued. **Applies to FSAs.**
Bulletin 2010-30	August 16, 2010	Reverse Mortgages: Interagency Guidance	Provides guidance on managing the compliance and reputation risks when making, purchasing, or servicing reverse mortgages through a third party, such as a mortgage broker or correspondent. **Applies to FSAs.**
Bulletin 2010-7	February 18, 2010	Tax Refund Anticipation Loans: Guidance on	Provides guidance to enhance, clarify, and increase awareness regarding the measures the OCC expects to see in place for tax refund-related products offered

		Consumer Protection and Safety and Soundness	by banks, including issues related to reliance on third-party tax return preparers who interact with consumers.
Bulletin 2010-1	January 8, 2010	Interest Rate Risk: Interagency Advisory on Interest Rate Risk Management	Includes guidance on selection, control frameworks, and validation of third-party asset liability management models. **Applies to FSAs.**
Bulletin 2009-15	May 22, 2009	Investment Securities: Risk Management and Lessons Learned	Provides guidance for banks that use the services of third parties who compile and provide investment analytics for bank management.
Bulletin 2008-12	April 24, 2008	Payment Processors: Risk Management Guidance	Provides guidance to banks regarding relationships with third-party processors and requirements for effective due diligence, underwriting, and monitoring. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2008-5	March 6, 2008	Conflicts of Interest: Risk Management Guidance—Divestiture of Certain Asset Management Businesses	Provides guidance for banks that contemplate divestiture of affiliated funds and associated advisers, whether directly, or through their broader corporate organizations.
Bulletin 2008-4	February 2, 2008	Flood Disaster Protection Act: Flood Hazard Determination Practices	Provides guidance to banks that outsource flood hazard determinations to third-party servicers to ensure that appropriate information is used when performing flood determinations and that revision dates be included in the determination form. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2006-47	December 13, 2006	Allowance for Loan and Lease Losses (ALLL): Guidance and Frequently Asked Questions (FAQs) on the ALLL	Includes guidance for when some or the entire loan review function and the validation of the ALLL methodology is outsourced to a qualified external party, and identifies the minimum objectives of a loan review program. **Applies to FSAs.**
Bulletin 2006-39	September 1, 2006	Automated Clearing House Activities: Risk Management Guidance	Provides guidance for banks and examiners on managing the risks of automated clearing house (ACH) activity, which can include new and evolving types of ACH transactions as well as new participants in the ACH network, including certain merchants and third parties known as third-party senders. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2005-35	October 12, 2005	Authentication in an Internet Banking Environment: Interagency Guidance	Highlights requirements for banks to use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a technology service provider. **Applies to FSAs.**
Bulletin 2005-27	August 4, 2005	Real Estate Settlement Procedures Act (RESPA): Sham Controlled Business Arrangements	Provides guidance on determining if a RESPA settlement service provider (often a third-party servicer or vendor) is a “controlled business arrangement” and therefore entitled to certain exemptions. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2005-22	May 16, 2005	Home Equity Lending: Credit Risk Management Guidance	Sets forth regulatory expectations for enhanced risk management practices, including management of third-party originations. **Applies to FSAs.**
Bulletin 2005-13	April 14, 2005	Response Programs for Unauthorized Access to Customer Information and Customer Notice: Final Guidance: Interagency Guidance	Provides guidance on banks implementing a response program to address unauthorized access to customer information maintained by the institution or its service providers. **Applies to FSAs.**

Bulletin 2005-1	January 12, 2005	Proper Disposal of Consumer Information: Final Rule	Sets standards for information security. Requires agreements with service providers on disposal. Describes duties of users of consumer reports regarding identity theft. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2004-47	October 27, 2004	FFIEC Guidance: Risk Management for the Use of Free and Open Source Software (FOSS)	Provides guidance for institutions considering using or deploying FOSS regardless of whether it will be provided internally or by a third-party service provider. **Applies to FSAs.**
Bulletin 2004-20	May 10, 2004	Risk Management of New, Expanded, or Modified Bank Products and Services: Risk Management Process	Reminds banks of the risk management process they should follow to prudently manage the risks associated with new, expanded, or modified bank products and services, including those provided by third parties.
Bulletin 2003-15	April 23, 2003	Weblinking: Interagency Guidance on Weblinking Activity	Provides guidance to institutions that develop and maintain their own Web sites, as well as institutions that use third-party service providers for this function. **Applies to FSAs.**
Bulletin 2003-12	March 17, 2003	Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing	Reflects developments within the financial, audit, and regulatory industries, particularly the Sarbanes–Oxley Act of 2002 that established numerous independence parameters for audit firms that provide external audit, outsourced internal audit, and other non-audit services for financial institutions. **Applies to FSAs.**
Bulletin 2002-16	May 15, 2002	Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance	Provides guidance on managing the risks that may arise from outsourcing relationships with foreign-based third-party service providers, and addresses the need for banks to establish relationships with foreign-based third-party service providers in a way that does not diminish the ability of the OCC to timely access data or information needed for supervisory activities. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2002-03	January 15, 2002	Real Estate Settlement Procedures Act: Examiner Guidance—Mark-ups of Settlement Service Fees	Provides guidance on determining if a RESPA settlement service provider (often a third-party servicer or vendor) is charging more for a settlement service provided by a third party than is actually paid to the third party and the third party is not involved in the mark-up, which is prohibited by RESPA Section 8 (b) (implemented by Regulation X) in most but not all states. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2001-51	December 12, 2001	Privacy of Consumer Financial Information: Small Bank Compliance Guide	Includes guidance for banks to evaluate agreements with nonaffiliated third parties that involve the disclosure of consumer information. **Applies to FSAs.**
Bulletin 2001-12	February 28, 2001	Bank-Provided Account Aggregation Services: Guidance to Banks	Includes guidance for banks that offer aggregation services through third-party service providers.
Bulletin 2001-8	February 15, 2001	Guidelines Establishing Standards for Safeguarding Customer Information: Final Guidelines	Alerts banks that oversight program of service providers should include confirmation that the providers have implemented appropriate measures designed to meet the objectives of the guidelines. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 2000-25	September 8, 2000	Privacy Laws and Regulations: Summary of Requirements	Includes guidance for banks to evaluate agreements with third parties that involve the disclosure of consumer information. **Applies to FSAs with the issuance of this bulletin.**

Bulletin 2000-14	May 15, 2000	Infrastructure Threats—Intrusion Risks: Message to Bankers and Examiners	Provides guidance on how to prevent, detect, and respond to intrusions into bank computer systems, including outsourced systems.
Bulletin 1999-14	March 29, 1999	Real Estate Settlement Procedures Act: Statement of Policy—Lender Payments to Mortgage Brokers	Provides guidance on services normally performed in loan origination, including those often performed by a third-party servicer or vendor. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 1998-3	March 17, 1998	Technology Risk Management: Guidance for Bankers and Examiners	Includes a short description of a bank's responsibility with regard to outsourcing its technology products and services. **Applies to FSAs with the issuance of this bulletin.**
Bulletin 1996-48	September 3, 1996	Stored Value Card Systems: Information for Bankers and Examiners	Provides basic information to assist banks in identifying and managing risks involved in stored value systems. **Applies to FSAs with the issuance of this bulletin.**
Advisory Letter 2004-6	May 6, 2004	Payroll Card Systems	Advises banks engaged in payroll cards systems involving nonbank third parties to fully comply with OCC guidance on third-party relationships.
Advisory Letter 2002-3	March 22, 2002	Guidance on Unfair or Deceptive Acts or Practices	Describes legal standards and provides guidance on unfair or deceptive acts and practices. Cross references other OCC guidance on: selecting a third-party vendor; monitoring vendor performance; maintaining proper documentation about vendor management; review of contractual arrangements; compensation concerns; monitoring consumer complaints; payment procedures; and loan collection activities.
Advisory Letter 2000-11	November 27, 2000	Title Loan Programs	Alerts banks to OCC concerns over title loan programs, including the involvement of third-party vendors.
Advisory Letter 2000-10	November 27, 2000	Payday Lending	Alerts banks to OCC concerns over payday lending programs, including the involvement of third-party vendors. **Applies to FSAs.**
Banking Circular 181	August 2, 1984	Purchases of Loans in Whole or in Part-Participations	Describes prudent purchases of loans from and loan participations with third parties. **Applies to FSAs with the issuance of this bulletin.**

FFIEC Handbooks

Issuance	Date	Subject	Description
FFIEC Bank Secrecy Act/ Anti-Money Laundering Examination Manual	April 29, 2010	Bank Secrecy Act and Anti-Money Laundering	Provides guidance on identifying and controlling risks associated with money laundering and terrorist financing, including third-party payment processors and professional service providers.
FFIEC Information Technology Examination Handbook	Various	"Outsourcing Technology Services" and "Supervision of Technology Service Providers"	Provides guidance on managing risks associated with the outsourcing of IT services. Several other booklets of the FFIEC IT Examination Handbook also provide guidance addressing third-party relationships.

[1] Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records. Affiliate relationships are also subject to sections 23A and 23B of the Federal

Reserve Act (12 USC 371c and 12 USC 371c-1) as implemented in Regulation W (12 CFR 223). Third-party relationships generally do not include customer relationships.

[2] An OCC-supervised bank that provides services to another OCC-supervised bank is held to the same standards of due diligence, controls, and oversight as is a non-bank entity.

[3] For example, in franchising arrangements, the bank lends its name or regulated entity status to activities originated or predominantly conducted by others. Thus, the bank is permitting its attributes to be used in connection with the products and services of a third party. The risks to the bank from these franchising arrangements vary based on the terms of the agreement between the bank and the third party and the nature of the services offered. When a bank is offering products and services originated by third parties as its own, the bank can be exposed to substantial financial loss and damage to its reputation if it fails to maintain adequate quality control over those products and services and adequate oversight over the third-party activities. Risk may also increase when the third party relies on the bank's regulated entity status and offers services or products through the bank with fees, interest rates, or other terms that cannot be offered by the third party directly.

[4] Refer to appendix A for a discussion of risks associated with third-party relationships.

[5] Except for nondisclosure agreements that may be required in order for the bank to conduct due diligence.

[6] Dual employees are employed by both the bank and the third party.

[7] If the bank enters into a written arrangement under which a broker registered under the securities laws offers brokerage services on or off the premises of the bank, the bank should ensure that the arrangement qualifies for the exception in the Securities and Exchange Act of 1934, 15 USC 78c(a)(4)(B)(i), and Regulation R, 12 CFR 218.700-701 and 17 CFR 247.700-701, for third-party brokerage arrangements. Otherwise, the bank may be required to register as a securities broker under the federal securities laws. The bank also should ensure compliance with regulatory requirements if bank employees receive fees for referrals to the third-party broker.

[8] Before conducting an examination of a third party that is a functionally regulated affiliate (FRA), the OCC is required to give notice to and consult with the FRA's primary regulator and, to the fullest extent possible, avoid duplication of examination activities, reporting requirements, and requests for information. See 12 USC 1831v.

[9] When a third-party relationship involves critical activities, a bank may need to consider appointing a senior officer to provide oversight of that relationship.

[10] Under 12 USC 1867(c)(2), national banks are required to notify the OCC of the existence of a servicing relationship. FSAs are subject to similar requirements set forth in 12 USC 1464(d)(7)(D)(ii) and 12 USC 1867(c)(2). The OCC implements this notification requirement by requiring banks to maintain a current inventory of all third-party relationships and make it available to examiners upon request.

[11] In addition to the functional business units, this may include information technology, identity and access management, physical security, information security, business continuity, compliance, legal, risk management, and human resources.

[12] The CAMELS rating is an overall assessment of a bank based on six individual ratings; the word CAMELS is an acronym for these individual elements of regulatory assessment (capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk).

[13] All guidance applies to national banks. Guidance not currently applicable to FSAs (as noted in this appendix) is undergoing review through the OCC's policy integration efforts.