South Carolina Bar

2017 South Carolina Bar Convention

Real Estate Practices Section Seminar

Saturday, January 21, 2017

presented by
The South Carolina Bar
Continuing Legal Education Division

SC Supreme Court Commission on CLE Course No. 170454

South Carolina Bar

Rolling on the River: Ethics in the 21st Century

Cynthia Cooper
Brandon, MS

South Carolina Bar

Takin' Care of Business: Compliance is the New Marketing (Vendor Management in Today's World)

Moderator — Cynthia Durham Blair
Columbia, SC

Eric Biggers — Little Rock, AR
Michelle Korsmo — Washington, DC
Penny Reed — Shoreview, MN

ADDITIONAL AND AMENDED PET FIELDS

[Same as in 60 day notice]

Affected entities	SDRs, SEFs, DCMs, DCOs, SD/MSPs, non-SD/MSP reporting entities		
Burden type	Burden per respondent	Number of respondents	Total burden
Annual hours burden	200 hours	449	89,800 hours.
Annual costs	$0	449	$0.

TERMINATION OF ORIGINAL SWAPS

[Increased by 50% from 60 day notice]

Affected entities	DCOs		
Burden type	Burden per respondent	Number of respondents	Total burden
One-time hours burden	4,500 hours	12	54,000 hours.
Annual costs	$375,000	12	$4,500,000.

Increases in Hours Burdens and New Total Hours Burden

Based on an increase in annual burden hours of 89,800, Commission staff estimate that the revised aggreagate total annual time burden for the collection is 562,945 hours.

Increases in Aggregate Costs

There are three components to the aggregate increase in annual costs associated with this revision, (a) costs associated with changes to reporting systems, to be incurred by 449 entities; (b) annualized costs associated with establishing SDR connections by DCOs; and (c) costs associated with maintaining SDR connections by DCOs.

First, the Commission estimates that the costs associated with additional and amended PET fields will be $15,196 per entity (200 hours × $75.98 per hour).[4] The aggregate increase across all 449 reporting entities and SDRs for the additional and amended PET fields is therefore $6,823,004.

Second, the Commission estimates that DCO to SDR connections will require each DCO to incur a one-time start-up cost of $341,910 (4,500 hours x $75.98 per hour). The Commission estimates that DCOs will use these connections for 20 years, and therefore the annualized start-up cost for SDR connections will be $17,095 per DCO. Based on 12 DCOs, the aggregate annualized start-up cost for SDR connections will be $205,146.

Third, DCOs will incur an aggregate annual cost of $4,500,000 to maintain those SDR connections.

By combining these three components, the *aggregate increase* to annual costs associated with this collection will be $11,528,150.

Total Aggregate Costs

Commission staff estimate that the revised *aggregate total annual cost* for the collection is $99,462,062. The burden estimate represents the burden that SDRs, swap execution facilities (''SEFs''), designated contract markets (''DCMs''), DCOs, swap dealers (''SDs''), major swap participants (''MSPs''), and non-SD/MSP swap counterparties incur to operate and maintain swap recordkeeping and reporting systems to facilitate the recordkeeping and reporting of swaps.

Respondents/Affected Entities: SDRs, SEFs, DCMs, DCOs, SDs, MSPs, and non-SD/MSP swap counterparties.

Estimated Number of Respondents: 30,210.

Estimated Total Annual Burden on Respondents: 562,945 hours.

Estimated Total Annual Cost: $99,462,062.

Frequency of Collection: Ongoing.

(Authority: 44 U.S.C. 3501 *et seq.*)

Dated: October 21, 2016.

Robert N. Sidman,

Deputy Secretary of the Commission.

[FR Doc. 2016–25925 Filed 10–25–16; 8:45 am]

BILLING CODE 6351–01–P

[4] In calculating the cost figures associated with burden hours, the Commission estimated the appropriate wage rate based on salary information for the securities industry compiled by the Securities Industry and Financial Markets Association (''SIFMA''). Commission staff arrived at an hourly rate of $75.98 using figures from a weighted average of salaries and bonuses across different professions from the SIFMA Report on Management & Professional Earnings in the Securities Industry 2013, modified to account for an 1800-hour work-year and multiplied by 1.3 to account for overhead and other benefits. The Commission estimated appropriate wage rate is a weighted national average of salary and bonuses for professionals with the following titles (and their relative weight): ''programmer (senior)'' (30% weight); ''programmer'' (30%); ''compliance advisor (intermediate)'' (20%); ''systems analyst'' (10%), and ''assistant/associate general counsel'' (10%).

BUREAU OF CONSUMER FINANCIAL PROTECTION

Compliance Bulletin and Policy Guidance; 2016–02, Service Providers

AGENCY: Bureau of Consumer Financial Protection.

ACTION: Compliance bulletin and policy guidance.

SUMMARY: The Bureau is reissuing its guidance on service providers, formerly titled CFPB Bulletin 2012–03, Service Providers to clarify that the depth and formality of the risk management program for service providers may vary depending upon the service being performed—its size, scope, complexity, importance and potential for consumer harm—and the performance of the service provider in carrying out its activities in compliance with Federal consumer financial laws and regulations. This amendment is needed to clarify that supervised entities have flexibility and to allow appropriate risk management.

DATES: The Bureau released this Compliance Bulletin and Policy Guidance on its Web site on October 31, 2016.

FOR FURTHER INFORMATION CONTACT: Suzanne McQueen, Attorney Adviser, Office of Supervision Policy, 1700 G Street NW., 20552, 202–435–7439.

SUPPLEMENTARY INFORMATION:

1. Compliance Bulletin and Policy Guidance 2016–02, 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.

The Bureau expects that the depth and formality of the entity's risk management program for service providers may vary depending upon the service being performed—its size, scope, complexity, importance and potential for consumer harm—and the performance of the service provider in carrying out its activities in compliance with Federal consumer financial laws and regulations. While due diligence does not provide a shield against liability for actions by the service provider, it could help reduce the risk that the service provider will commit violations for which the supervised bank or nonbank may be liable, as discussed above.

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;
- 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]

2. Regulatory Requirements

This Compliance Bulletin and Policy Guidance is a non-binding general statement of policy articulating considerations relevant to the Bureau's exercise of its supervisory and enforcement authority. It is therefore exempt from notice and comment

[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.

[3] *http://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf* at 34 (Compliance Management Review) and 174 (Unfair, Deceptive, and Abusive Acts or Practices).

rulemaking requirements under the Administrative Procedure Act pursuant to 5 U.S.C. 553(b). Because no notice of proposed rulemaking is required, the Regulatory Flexibility Act does not require an initial or final regulatory flexibility analysis. 5 U.S.C. 603(a), 604(a). The Bureau has determined that this Compliance Bulletin and Policy Guidance does not impose any new or revise any existing recordkeeping, reporting, or disclosure requirements on covered entities or members of the public that would be collections of information requiring OMB approval under the Paperwork Reduction Act, 44 U.S.C. 3501, *et seq.*

Dated: October 19, 2016.

Richard Cordray,

Director, Bureau of Consumer Financial Protection.

[FR Doc. 2016–25856 Filed 10–25–16; 8:45 am]

BILLING CODE 4810–AM–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID DOD–2014–OS–0074]

Submission for OMB Review; Comment Request

ACTION: Notice.

SUMMARY: The Department of Defense has submitted to OMB for clearance, the following proposal for collection of information under the provisions of the Paperwork Reduction Act.

DATES: Consideration will be given to all comments received by November 25, 2016.

FOR FURTHER INFORMATION CONTACT: Fred Licari, 571–372–0493.

SUPPLEMENTARY INFORMATION:

Title, Associated Form and OMB Number: Application for Trusteeship, DD Form 2827, OMB License 0730–0013.

Type of Request: Reinstatement, without change, of a previously approved collection for which approval has expired.

Number of Respondents: 75.

Responses per Respondent: 1.

Annual Responses: 75.

Average Burden per Response: 15 minutes.

Annual Burden Hours: 19 hours.

Needs and Uses: The information collection is needed to identify the prospective trustees for active duty military and retirees. The information is required in order for the Defense Finance and Accounting Service (DFAS) to make payments on behalf of incompetent military members or retirees. DFAS is representing all services as the functional proponent for Retired and Annuitant Pay.

Affected Public: Individuals or households.

Frequency: On occasion.

Respondent's Obligation: Required to obtain or maintain benefits.

OMB Desk Officer: Ms. Jasmeet Seehra.

Comments and recommendations on the proposed information collection should be emailed to Ms. Jasmeet Seehra, DoD Desk Officer, at *Oira_submission@omb.eop.gov.* Please identify the proposed information collection by DoD Desk Officer and the Docket ID number and title of the information collection.

You may also submit comments and recommendations, identified by Docket ID number and title, by the following method:

• *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name, Docket ID number and title for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

DOD Clearance Officer: Mr. Frederick Licari.

Written requests for copies of the information collection proposal should be sent to Mr. Licari at WHS/ESD Directives Division, 4800 Mark Center Drive, East Tower, Suite 03F09, Alexandria, VA 22350–3100.

Dated: October 21, 2016.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2016–25897 Filed 10–25–16; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Department of the Navy

[Docket ID: USN–2014–0012]

Submission for OMB Review; Comment Request

ACTION: Notice.

SUMMARY: The Department of Defense has submitted to OMB for clearance, the following proposal for collection of information under the provisions of the Paperwork Reduction Act.

DATES: Consideration will be given to all comments received by November 25, 2016.

FOR FURTHER INFORMATION CONTACT: Fred Licari, 571–372–0493.

SUPPLEMENTARY INFORMATION:

Title, Associated Form and OMB Number: Application Forms and Information Guide, Naval Reserve Officers Training Corps (NROTC) Scholarship Program; OMB Control Number 0703–0026.

Type of Request: Reinstatement, with change, of a previously approved collection for which approval has expired.

Number of Respondents: 14,000.

Responses per Respondent: 7.

Annual Responses: 98,000.

Average Burden per Response: 3 hours 30 minutes.

Annual Burden Hours: 46,666.

Needs and Uses: This collection of information is used to make a determination of an applicant's academic and/or leadership potential and eligibility for an NROTC scholarship. The information collected is used to select the best-qualified candidates.

Affected Public: Individuals or Households.

Frequency: Annually.

Respondent's Obligation: Required to obtain or retain benefits.

OMB Desk Officer: Ms. Jasmeet Seehra.

Comments and recommendations on the proposed information collection should be emailed to Ms. Jasmeet Seehra, DoD Desk Officer, at *Oira_submission@omb.eop.gov.* Please identify the proposed information collection by DoD Desk Officer and the Docket ID number and title of the information collection.

You may also submit comments and recommendations, identified by Docket ID number and title, by the following method:

• *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name, Docket ID number and title for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

DOD Clearance Officer: Mr. Frederick Licari.

ALTA Best Practices
Maturity Model

Introduction to the Maturity Model

The Maturity Model is designed to help title insurance and settlement companies determine their compliance with the Best Practices.

The Maturity Model is comprised of seven tables, one for each pillar of the Best Practices. Each table highlights the policies outlined in ALTA's Title Insurance and Settlement Company Best Practices (labeled "Best Practice"). Each table also contains five columns measuring the company's adherence to the Best Practices. These columns have the following labels:

- ***Ad Hoc:*** company has not yet established any policies or procedures
- ***Planning:*** company is developing compliance. Procedures and controls exist but are not documents, or procedures and controls are documented by not completely implemented.
- ***Defined:*** company is partially compliant with the Best Practices. Some procedures and controls exist and are documented, but are not completely being followed.
- ***Managed:*** company is substantially compliant with the Best Practices. Procedures and controls exist and are documented, but are not being followed consistently.
- ***Optimized:*** company is fully compliant with the Best Practices. Procedures and controls exist, are documented, and are being followed consistently.

Applicable definitions for this Maturity Model:

- Implemented: the process/procedure has been established, is documented, and is required by the Company
- Followed: the process/procedure has been established, is documented, is required by the Company, and is being performed as intended

The Maturity Model features differentiating characteristics to help companies define where its policies and procedures fit within the Best Practices and the steps it must do to become fully compliant with the Best Practices. This Maturity Model also allows companies to represent progress towards Best Practices compliance.

Instructions

You should use this Maturity Model following an assessment of your company's compliance with the Best Practices using ALTA's Title Insurance and Settlement Company Best Practices and Assessment Procedures. Based on the results of your assessment, identify the benchmark compliance level that best describes your company's policies and procedures for each Best Practice.

Within the Maturity Model Summary, you should mark with an "X" the benchmark compliance level that best describes your company's procedures for each Best Practice. You should also indicate the steps your company is taking to improve its compliance with each Best Practice within the Progress Plan column. Identifying where your company lies on this Maturity Model will help you identify any next steps your company can take to fully comply with the Best Practices. Upon completion of this summary, you will have a high-level report that indicates your company's compliance with the Best Practices.

We hope you will find this Maturity Model a helpful tool as you evaluate your company's policies and procedures and strive to implement practices that will help your company succeed in the industry. Additional resources on ALTA's Best Practices, including ALTA's Maturity Model Explainer, are available on our website at http://www.alta.org/bestpractices. Any questions regarding this Maturity Model may be submitted to bestpractices@alta.org.

American Land Title Association
Protect your property rights

Maturity Model Summary

ALTA Best Practices	Benchmark Compliance Levels					Progress Plan
	Ad Hoc	Planning	Defined	Managed	Optimized	
Pillar 1						
Establish and maintain current license(s) as required to conduct the business of title insurance and settlement services	☐				☐	
Establish and maintain appropriate compliance with ALTA's Policy Forms Licensing requirement	☐				☐	
Pillar 2						
Written procedures and controls exist for escrow trust accounts	☐	☐	☐	☐	☐	
Escrow funds and operating accounts are separately maintained	☐		☐		☐	
Escrow Trust Accounts are prepared with Trial Balances, listing all file/escrow balances	☐	☐	☐	☐	☐	
Escrow Trust Accounts are reconciled	☐	☐	☐	☐	☐	
Escrow Trust Accounts are properly identified	☐		☐		☐	
Outstanding file balances are documented	☐	☐		☐	☐	
Transactions are conducted by authorized employees only	☐	☐		☐	☐	
Escrow Trust Accounts are maintained in Federally Insured Financial Institutions	☐				☐	
Utilize Positive Pay or Reverse Positive Pay, if available in the marketplace, and have policies and procedures in place that prohibit or control the use of Automated Clearing House and international wires	☐	☐	☐	☐	☐	
Background Checks are completed	☐		☐		☐	
Ongoing training is conducted for employees involved in the management of escrow funds and escrow accounting	☐	☐	☐	☐	☐	

For more information about the ALTA Best Practices, visit www.alta.org/bestpractices

Pillar 3						
Written privacy and information security program exists to protect non-public personal information (NPI) as required by local, state and federal law	☐	☐	☐	☐	☐	
Physical security of Non-public Personal Information	☐	☐	☐	☐	☐	
Network security of Non-public Personal Information	☐	☐	☐	☐	☐	
Disposal and maintenance of Non-public Personal Information	☐	☐	☐	☐	☐	
Establish a disaster management plan	☐	☐	☐	☐	☐	
Appropriate management and training of employees to help ensure compliance with Company's information security program	☐	☐	☐	☐	☐	
Oversight of service providers to help ensure compliance with Company's information security program	☐	☐	☐	☐	☐	
Audit and oversight procedures to help ensure compliance with a Company's information security program	☐	☐	☐	☐	☐	
Notification of security breaches to customers and law enforcement	☐	☐	☐	■	☐	
Pillar 4						
Procedures related to recording of documents	☐	☐	☐	☐	☐	
Procedures related to pricing	☐	☐	☐	☐	☐	
Procedures related to the settlement process	☐	☐	☐	☐	☐	
Procedures related to third-party signing professionals	☐	☐	☐	☐	☐	
Pillar 5						
Adopt and maintain written procedures related to title policy production, delivery, reporting and premium remittance	☐	☐	☐	☐	☐	
Title policy production and delivery; premium reporting and remittance	☐	☐	☐	☐	☐	
Pillar 6						
Maintain appropriate professional liability insurance and fidelity coverage	☐	■	☐	■	☐	
Pillar 7						
Adopt and maintain written procedures for resolving consumer complaints	☐	☐	☐	☐	☐	

American Land Title Association
Protect your property rights

ALTA Best Practices Maturity Model

Pillar 1						
Best Practice	**Related Assessment Procedures**	**Benchmark Compliance Levels**				
		Ad Hoc	**Planning**	**Defined**	**Managed**	**Optimized**
Establish and maintain current license(s) as required to conduct the business of title insurance and settlement services	1.01, 1.02	Licenses and corporate registrations are not available and active for all states and jurisdictions in which the company operates on the assessment date				Licenses and corporate registrations are available and active for all states and jurisdictions in which the company operates on the assessment date
Establish and maintain appropriate compliance with ALTA's Policy Forms Licensing requirement	1.03	Company does not maintain active ALTA Policy Forms License				Company maintains an active ALTA Policy Forms License

Pillar 2

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Written procedures and controls exist for Escrow Trust Accounts	2.01	Neither written procedures nor controls exist	Procedures and controls exist but are not documented or procedures and controls are documented but are not completely implemented	Some procedures and controls exist and are documented, but are not completely being followed	Procedures and controls exist and are documented, but are not being followed consistently	Procedures and controls exist, are documented, and are being followed consistently
Escrow funds and operating accounts are separately maintained	2.03n	Escrow and fiduciary funds are comingled with operating accounts		Underwriter premiums and/or recording fees are comingled with operating accounts		No escrow or fiduciary funds are comingled with operating accounts
Escrow Trust Accounts are prepared with Trial Balances, listing all open file/escrow balances	2.03e, 2.03h, 2.03l, 2.03m	No escrow accounts or fiduciary accounts are prepared with a Trial Balance	Some escrow accounts and fiduciary accounts are prepared with a Trial Balance	Most Escrow accounts and fiduciary accounts are prepared with a Trial Balance; however, underwriter premium and/or recording account may or may not be prepared with a Trial Balance	All escrow accounts and fiduciary accounts are prepared with a Trial Balance, including recording account, but not underwriter premium account or underwriter account but not the recording account; however, compensating controls are in place	All escrow accounts or fiduciary accounts are prepared with Trial Balances

Pillar 2

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Escrow Trust Accounts are reconciled	2.03a, 2.03b, 2.03c, 2.03d, 2.03e, 2.03i, 2.03o, 2.03p	Escrow and fiduciary accounts are not reconciled	Escrow accounts and fiduciary accounts undergo Three-Way Reconciliations less than monthly	Escrow accounts and fiduciary accounts undergo Three-Way Reconciliations monthly; however, segregation of duties may not exist and/ or are insufficient	Escrow accounts and fiduciary accounts undergo Three-Way Reconciliations monthly and segregation of duties are in place; however, reconciliations are not reviewed by management and/or daily reconciliation of receipts and disbursements is not performed	Escrow accounts and fiduciary accounts undergo Three-Way Reconciliations monthly, segregation of duties are in place, reconciliations are reviewed by management, and daily reconciliations of receipts and disbursements are performed
Escrow Trust Accounts are properly identified	2.02, 2.03f, 2.04	Escrow and fiduciary accounts are not properly identified as “escrow” or “trust”		Escrow and fiduciary accounts are properly identified as “escrow” or “trust;” however, not all account-related documentation is consistently identified as such		All escrow trust accounts and fiduciary accounts are properly identified as “escrow” or “trust” and all related documentation is also properly identified
Outstanding file balances are documented	2.03j, 2.03k, 2.03l	No documentation exists for the outstanding file balances for escrow accounts and fiduciary accounts	Some documentation exists for the outstanding file balances for escrow accounts and fiduciary accounts		Most escrow and fiduciary accounts have documentation of outstanding file balances	All escrow accounts or fiduciary accounts are prepared with documented outstanding file balances

Pillar 2

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Transactions are conducted by authorized employees only	2.02, 2.03g	There are no controls in place to prevent unauthorized employees from conducting transactions	There are some controls in place to prevent unauthorized employees from conducting transactions; however, terminated employees are not immediately deleted as listed signatories on all bank accounts		There are controls in place to prevent unauthorized employees from conducting transactions and terminated employees are immediately deleted as listed signatories on all bank accounts; however, appropriate authorization levels are not reviewed annually	All transactions are performed by authorized employees only and authorization levels are annually reviewed with terminated employees immediately deleted as listed signatories on all bank accounts.
Escrow Trust Accounts are maintained in Federally Insured Financial Institutions	2.05	Escrow Trust Accounts are not maintained in Federally Insured Financial Institutions				All Escrow Trust Accounts are maintained in Federally Insured Financial Institutions

Pillar 2

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Utilize Positive Pay or Reverse Positive Pay, if available in the marketplace, and have policies and procedures in place that prohibit or control the use of Automated Clearing House (ACH) and international wires	2.06a, 2.06b	Positive pay, reverse positive pay, ACH controls and/or international wire controls are not used on any accounts	Positive pay, reverse positive pay, ACH controls and/or international wire controls are not used on all accounts	Positive pay, reverse positive pay, ACH controls and international wire controls are used on some accounts	Positive pay, reverse positive pay, ACH controls and international wire controls are used on most accounts	Positive pay and reverse positive pay if available in the local marketplace), and ACH controls and international wire controls are used on all accounts
Background Checks are completed	2.02c	No Background Checks are performed on employees with access to customer funds		Background Checks are performed at hiring, but are not routinely updated for employees with access to customer funds		All employees with access to customer funds have undergone Background Checks either at hiring or within the past three years and Background Checks are updated at least every three years

Pillar 2						
Best Practice	**Related Assessment Procedures**	**Benchmark Compliance Levels**				
		Ad Hoc	**Planning**	**Defined**	**Managed**	**Optimized**
Ongoing training is conducted for employees involved in the management of escrow funds and escrow accounting	2.02d	No training is conducted for employees involved in the management of escrow funds and/or escrow accounting	Training is conducted for some employees involved in the management of escrow funds and escrow accounting	Training is conducted for most employees involved in the management of escrow funds and escrow accounting	Training is conducted for all employees involved in the management of escrow funds and escrow accounting, but such training is not ongoing	Ongoing training is conducted for all employees involved in the management of escrow funds and escrow accounting

Pillar 3						
Best Practice	**Related Assessment Procedures**	**Benchmark Compliance Levels**				
		Ad Hoc	**Planning**	**Defined**	**Managed**	**Optimized**
Written privacy and information security program exists to protect non-public personal information (NPI) as required by local, state and federal law	3.01, 3.03, 3.15, 3.16	No written program exists	Program exists but is not documented or program is documented but not implemented	Written program exists and is implemented but does not cover all necessary aspects to protect NPI	Written program exists and is implemented but is not being followed consistently	Written program exists, is implemented, and is followed consistently

Pillar 3

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Physical security of NPI	3.07a, 3.07b, 3.07d, 3.08, 3.09, 3.11	Company does not meet any of the below criteria: • Access to NPI is restricted to authorized employees who have undergone background checks performed upon hiring and every 3 years • Use of removable media is restricted and controlled • Procedures are in place to utilize only secured delivery methods are used when transmitting NPI	Company partially meets one or more of the below criteria: • Access to NPI is restricted to authorized employees who have undergone background checks performed upon hiring and every 3 years • Use of removable media is restricted and controlled • Procedures are in place to utilize only secured delivery methods are used when transmitting NPI	Company meets one of the below criteria and partially meets one or more of the remaining criteria: • Access to NPI is restricted to authorized employees who have undergone background checks performed upon hiring and every 3 years • Use of removable media is restricted and controlled • Procedures are in place to utilize only secured delivery methods are used when transmitting NPI	Company meets two of the below criteria and partially meets the third criteria: • Access to NPI is restricted to authorized employees who have undergone background checks performed upon hiring and every 3 years • Use of removable media is restricted and controlled • Procedures are in place to utilize only secured delivery methods are used when transmitting NPI	Company meets all three of the below criteria: • Access to NPI is restricted to authorized employees who have undergone background checks performed upon hiring and every 3 years • Use of removable media is restricted and controlled • Procedures are in place to utilize only secured delivery methods are used when transmitting NPI

Pillar 3

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Network security of NPI	3.06, 3.07c, 3.07d, 3.07e 3.09, 3.10, 3.12	Company does not meet any of the below criteria: • Maintain and secure access to Company information technology • Develop guidelines for the appropriate use of Company information technology. • Ensure secure collection and transmission of NPI	Company partially meets one or more of the below criteria: • Maintain and secure access to Company information technology • Develop guidelines for the appropriate use of Company information technology. • Ensure secure collection and transmission of NPI	Company meets one of the below criteria and partially meets the one or more of the remaining: • Maintain and secure access to Company information technology • Develop guidelines for the appropriate use of Company information technology. • Ensure secure collection and transmission of NPI	Company meets two of the below criteria and partially meets the third criteria: • Maintain and secure access to Company information technology • Develop guidelines for the appropriate use of Company information technology. • Ensure secure collection and transmission of NPI	Company meets all three of the below criteria: • Maintain and secure access to Company information technology • Develop guidelines for the appropriate use of Company information technology. • Ensure secure collection and transmission of NPI
Disposal of and maintenance of NPI	3.17	No policies or procedures in place over record disposal and maintenance	Policies and procedures exists but are not documented or are not implemented	Policies and procedures are documented but are not followed	Policies and procedures have been implemented, but are not consistently followed; third party vendor is actively managed	Policies and procedures are documented, implemented, and followed consistently regarding the Company's disposal of NPI in a manner that protects against unauthorized access to or use of the information

Pillar 3

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Establish a disaster management plan	3.13	A disaster management and business resumption plan does not exist	Some of the disaster management and business resumption procedures exist but are not documented or documented but not implemented	Some portions of the disaster management and business resumption plan exist and are documented, but are not implemented or tested	A disaster management and business resumption plan exist, are documented and implemented, however, they are not routinely tested	A disaster management and business resumption plan exist, are documented, implemented and tested on a routine basis
Appropriate management and training of employees to help ensure compliance with Company's information security program	3.02, 3.05	Training is not conducted for any employees on the Company's information security program	Training has been developed but is not conducted for employees	Training is conducted for some employees on the Company's information security program	Training is conducted for most employees on the Company's information security program	Training is conducted for all employees on the Company's information security program
Oversight of service providers to help ensure compliance with Company's information security program	3.14	No oversight of service providers	Oversight of service providers exists but there is no evidence of compliance with the Company's information security program on an ongoing basis	Oversight of service providers exists and there is some evidence of compliance with the Company's information security program on an ongoing basis	Oversight of service providers exists and adequately demonstrates evidence of compliance with the Company's information security program on a periodic basis	Oversight of service providers exists and adequately demonstrates evidence of compliance with the Company's information security program on an ongoing basis

Pillar 3						
Best Practice	**Related Assessment Procedures**	**Benchmark Compliance Levels**				
		Ad Hoc	**Planning**	**Defined**	**Managed**	**Optimized**
Audit and oversight procedures to help ensure compliance with a Company's information security program	3.04	No audit and oversight procedures exist	Oversight procedures are in development but not formalized	Oversight exists for the Company's information security program but audits are not being conducted	Oversight exists for the Company's information security program but audits are not being conducted on an ongoing basis	Oversight exists and audits ensure the Company's information security program is in compliance on an ongoing basis
Notification of security breaches to customers and required parties	3.10c, 3.15	Company has no monitoring in place to discover a security breach	Company is monitoring for security breaches but has no procedures to notify customers and required parties	Company is monitoring for security breaches and has a procedure for notification but is not following or is not followed timely.		Company is monitoring for security breaches, has notification procedures in place, and is timely notifying all parties of breaches, if occurred

Pillar 4

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Procedures related to recording of documents	4.01, 4.03	Neither written procedures nor controls exist	Some procedures and controls related to: • submitting or shipping documents for recording as required • tracking recordings • addressing rejected documents, and • verifying recordings were completed and records of the recording are maintained may be incomplete or not fully documented	Procedures and controls related to: • submitting or shipping documents for recording as required • tracking recordings • addressing rejected documents, and • verifying recordings were completed and records of the recording are maintained exist and are documented, but are not being followed	Procedures and controls exist related to: • submitting or shipping documents for recording as required • tracking recordings • addressing rejected documents, and • verifying recordings were completed and records of the recording are maintained exist and are documented, but are not being followed consistently	Procedures and controls are followed consistently and effectively related to: • submitting or shipping documents for recording as required • tracking recordings • addressing rejected documents, and • verifying recordings were completed and records of the recording are maintained
Procedures related to pricing	4.04	Neither written procedures nor controls exist	Some procedures and controls related to: • rates, • discounts, • review of charges, and • timely refunds exist but may be incomplete or not fully documented	Procedures and controls related to: • rates, • discounts, • review of charges, and • timely refunds exist and are documented, but are not being followed	Procedures and controls related to: • rates, • discounts, • review of charges, and • timely refunds exist and are documented, but are not being followed consistently	Procedures and controls are followed consistently and effectively related to: • rates, • discounts, • review of charges, and • timely refunds

Pillar 4

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Procedures related to the settlement process	4.02	Neither written procedures nor controls exist related to: • wiring funds, • receiving funds, • disbursing funds, in accordance with closing instructions and the settlement statement	Some procedures and controls exist related to: • wiring funds, • receiving funds, • disbursing funds, in accordance with closing instructions and the settlement statement but are not documented or procedures and controls are documented but are not implemented	Procedures and controls exist related to: • wiring funds, • receiving funds, • disbursing funds, in accordance with closing instructions and the settlement statement and are documented, but are not being followed	Procedures and controls exist related to: • wiring funds, • receiving funds, • disbursing funds, in accordance with closing instructions and the settlement statement and are documented, but are not being followed consistently	Procedures and controls are followed consistently and effectively related to: • wiring funds, • receiving funds, • disbursing funds, in accordance with closing instructions and the settlement statement, are documented

Pillar 4

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Procedures related to third-party signing professionals	4.05	Neither written procedures nor controls exist	Some procedures and controls related to: • Errors and Omissions insurance coverage • Notary surety bond (if required) • Licensure or recognized and verifiable industry designation • Acknowledgement of compliance with Company's instructions and information security program exist but are not documented or procedures and controls are documented but are not implemented	Procedures and controls related to: • Errors and Omissions insurance coverage • Notary surety bond (if required) • Licensure or recognized and verifiable industry designation • Acknowledgement of compliance with Company's instructions and information security program exist and are documented, but are not being followed	Procedures and controls related to: • Errors and Omissions insurance coverage • Notary surety bond (if required) • Licensure or recognized and verifiable industry designation • Acknowledgement of compliance with Company's instructions and information security program exist and are documented, but are not being followed consistently	Either third-party signing professionals engaged by the Company are directly employed by a Best Practices compliant company **or** procedures and controls are followed consistently and effectively related to: • Errors and Omissions insurance coverage • Notary surety bond (if required) • Licensure or recognized and verifiable industry designation • Acknowledgement of compliance with Company's instructions and information security program

Pillar 5

Best Practice	Related Assessment Procedures	Benchmark Compliance Levels				
		Ad Hoc	Planning	Defined	Managed	Optimized
Adopt and maintain written procedures related to title policy production, delivery, reporting and premium remittance	5.01	Neither written procedures nor controls exist	Procedures and controls exist but are not documented or procedures and controls are documented but are not completely implemented	Some procedures and controls exist and are documented, but are not completely being followed	Procedures and controls exist and are documented, but are not being followed consistently	Procedures and controls exist, are documented, and are being followed consistently
Title policy production and delivery; premium reporting and remittance	5.02	Company does not meet any of the below criteria: • timely title policy production • timely title policy delivery • timely policy reporting • timely premium remittance	Company meets one of the below criteria and partially meets one or more of the remaining criteria: • timely title policy production • timely title policy delivery • timely policy reporting • timely premium remittance	Company meets two of the below criteria and partially meets one or more of the remaining criteria: • timely title policy production • timely title policy delivery • timely policy reporting • timely premium remittance	Company meets three of the below criteria and partially meets the remaining criteria: • timely title policy production • timely title policy delivery • timely policy reporting • timely premium remittance	Company meets all four of the below criteria: • timely title policy production • timely title policy delivery • timely policy reporting • timely premium remittance

Pillar 6						
Best Practice	**Related Assessment Procedures**	**Benchmark Compliance Levels**				
		Ad Hoc	**Planning**	**Defined**	**Managed**	**Optimized**
Maintain appropriate professional liability insurance and fidelity coverage	6.01	No coverages exist		Some but not all required coverages exist		Appropriate and/or required professional liability insurance and fidelity coverage are in place

Pillar 7						
Best Practice	**Related Assessment Procedures**	**Benchmark Compliance Levels**				
		Ad Hoc	**Planning**	**Defined**	**Managed**	**Optimized**
Adopt and maintain written procedures for resolving consumer complaints	7.01, 7.02	Neither written controls nor procedures related to tracking and/or resolving consumer complaints exist	Some controls and procedures related to: • complaint intake, • documentation tracking log, • setting a single point of contact for resolving complaints exist but may be incomplete or not fully documented	Controls and procedures related to: • complaint intake, • documentation tracking log, • setting a single point of contact for resolving complaints exist and are documented, but are not being followed	Controls and procedures and related to: • complaint intake, • documentation tracking log, • setting a single point of contact for resolving complaints exist and are documented, but are not being followed consistently	Controls and procedures related to: • complaint intake, • documentation tracking log, • setting a single point of contact for resolving complaints exist, are documented, and are being followed consistently

AMERICAN
LAND TITLE
ASSOCIATION

September 16, 2016

Commissioner Adam Hamm
Chairman, Cybersecurity (EX) Task Force
National Association of Insurance Commissioners (NAIC)
c/o Sara Robben, Statistical Advisor
Via Email: Srobben@naic.org

Re: ALTA comments to the Insurance Data Security Model Law (version 2)

Dear Commissioner Hamm:

The American Land Title Association (ALTA) again appreciates the opportunity to comment on the second draft of the NAIC Cybersecurity (EX) Task Force's Insurance Data Security Model Law, which was released on August 17. In our view, a Model Law should improve upon existing state and federal requirements that licensees are already required to follow. State attorneys general, the Federal Trade Commission (FTC), National Institute of Standards and Technology (NIST) and Consumer Financial Protection Bureau (CFPB) should be consulted about this Model Law.

Data security is an important component of protecting consumers from cyber fraud. Laws and regulations around data security should protect consumers and help them understand the implication of cybersecurity breaches, be workable for industry and not duplicate existing safeguards. ALTA is committed to helping its members protect their business and clients from cyber attacks and we provide our members extensive resources and information to help them understand what they should be doing to safeguard sensitive data. ALTA supports a single, uniform standard for data security, investigation and notification of a data breach.

We want very much to collaborate with the Task Force. We continue to believe if the Task Force utilized an iterative process the Task Force has the opportunity to produce a much more useful Model Law, supported in individual state legislatures by interested parties. A more open, iterative process offers the Task Force a method to explain edits through an accompanying rationale, explanation or open dialogue. This iterative process allows the Task Force to broaden support among interested parties for the Model Law.

We are concerned that the comment periods surrounding this process have not presented opportunities for questions or dialogue on shared goals and feel that this may have the unintended consequence of hardening of each stakeholder's position. We aspire to do better together.

We appreciate that the Task Force considered and adopted suggestions from ALTA's June 3, 2016, comment letter on Version 1 of the Model Law. These improvements include clarifications to the definition of a "consumer," encryption, private rights of action, and oversight procedures of a company's Board of Directors.

However, other portions of Version 2 of the Model Law are less clear, and in some ways, we are unclear what the Model Law is trying to achieve. Below are significant issues that need to be resolved in future versions of the draft Model Law. We offer these Section-by-Section comments in a constructive nature, and we look forward to working with the Task Force in the future on the model law.

Purpose and Intent (Section 2)

State insurance commissioners should determine how the Model Law will establish the exclusive standards for licensees in a state for data security and investigation and breach notification. It is unclear how the Model Law could serve as an exclusive standard and ignore existing state and federal law or be preempted by federal law. We continue to be concerned that an insurance-only Model Law will not establish a single standard for consumer protection and is likely to create confusion and conflict among various regulators, state attorneys general, courts, industry and consumers. We are concerned that this will make it difficult for title insurance licensees to comply with all of their legal and contractual obligations.

We appreciate the attempted clarification between federal and state law. At the same time, the current language does not appear to solve questions about preemption. Simply stating if a conflict arises with state or federal law the one that provides greater consumer protection will control is not likely to meet the legal standard necessary to clarify preemption.

Definitions (Section 3)

We appreciate the clarification in Version 2 of the definition of a consumer. However, we remain concerned that the definition does not limit a consumer to state residents. A limitation to state residents would improve consistency with Section 6 (A)(2).

The term "Personal Information" in subsection (H)(2) should also be tightened. Nearly all state statutes provide a more limited definition of "Personal Information." It is unclear how a licensee would be able to monitor compliance with (H)(2)(e), a new requirement added to Version 2 from Version 1 without any explanation or justification. This new requirement transforms a licensees' legal or contractual duty into a regulatory duty even when there is no indication that the information at issue would otherwise be considered protected personal information. It is also unclear why subsections (H)(2)(g) through (j) are included in the definition of personal information since a breach notification is not required for these categories under Section 6. Inclusion of subsections (H)(2)(g) through (j) will only cause confusion and should be deleted from the definition.

We again stress that a trigger of a "reasonable likelihood of harm" is necessary. As currently drafted, Version 2 requires notification procedures to be commenced even when there is little to no likelihood that exposed information could lead to identity theft or fraudulent transactions on consumer's accounts. This creates unnecessary expense and work for the licensee, regulator and law enforcement where there is no measureable consumer benefit. Over time, the numerous ongoing notifications will likely have the affect of desensitizing consumers to breach notification notices.

Information Security Program (Section 4)

We recognize that Section 4 is well intended. At the same time, we continue to be deeply concerned about how small producers will be able to comply with these requirements of the Model Law. We again ask the Task Force to consider how to make the requirements of Section 4(A) scalable,

particularly to small producers. As we have indicated in previous comment letters, there were at least 5,454 title insurance producers who issued 50 or fewer title insurance policies in 2015, which represents an estimated 24 percent of title insurance producers in the United States.[1] The regulatory burden for each one of these small producers to "develop, implement and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for the protection of personal information" is unreasonably excessive in that it does not specify how the size and complexity of a licensee, nature and scope of the licensees' activities and sensitivity of the personal information in possession, custody or control should be identified. Absent objective standards, licensees will be identified on a subjective, state-by-state basis. The Task Force should consider whether the (NIST) Cybersecurity Framework's tiered approach can provide more objective measures of the licensee's information security program.

Compliance with Section 4(D) for small producers is equally difficult to envision. We noted that a new requirement "at a minimum" was added to Version 2 from Version 1 without any explanation or justification. Reference to the NIST Cybersecurity Framework was removed from Version 1 and replaced with "generally accepted cybersecurity principles." It is unclear why this helpful reference was removed, how the Model Law defines these generally accepted cybersecurity principles or where a licensee may find these generally accepted principles.

The physical security access controls required by Section 4(D)(1)(b) are today required by only the largest physical locations of bank vendors. In addition, 4(D)(1)(e), (f) and (h) would also present extraordinary costs and challenges to small producers and could likely have the unintended consequence of forcing many to consolidate or simply exit the business. Consolidation or the loss of small licensees would decrease consumer choice and competition.

A new and undefined term "state of the art techniques" was added to Section 4(D)(1)(e) of Version 2 from Version 1 without any definition, explanation or justification. It is unclear the intent of "state of the art techniques" required in Section 4(D)(1)(e) as opposed to "generally accepted cybersecurity principles in required in Section 4(D)(1).

Requiring a licensee to utilize multi-factor authentication procedures under Section 4(D)(1)(e) is excessive for in-house employees operating behind a licensee's own firewall. We recognize that segregation of duties works well to protect funds; however, it is also unclear what is intended by "segregation of duties," how this would protect data or how it can be applied to protect personal information.

While we appreciate that Version 2 greatly improves "Oversight of Third-Party Service Provider Arrangements" in Section 4(F), additional revisions are required to clarify how a small producer will have the capitalization and business-leverage to "be responsible for any failure by such third-party service providers to protect personal information." This type of requirement could threaten the solvency of small and even medium-sized licensees were a breach to occur. We are also concerned that language will result in a pull back by smaller licensees from technology solutions that substantially improve their

[1] This is the total number of title insurance producers that obtained an Occasional Use Waiver from ALTA for use of ALTA's copyrighted policy forms. An Occasional Use Waiver is available for those who, during the previous calendar year, wrote title insurance on 50 or fewer transactions. For more information, see: http://www.alta.org/membership/policyformslicense_FAQ.pdf.

risk profile and exposure to cyber threats. Licensees should be encouraged to adopt cost-effective technologies that can greatly reduce threats by frequent and much higher probability risks, such as wire instruction fraud in real estate transactions.

Finally, we also encourage the Task Force to consider whether cyber-insurance should be maintained by a licensee and what cyber-insurance coverage may be required by the Model Law, "commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities and the sensitivity of the personal information in the licensee's possession custody or control." Cyber insurance coverage available on the market can vary extremely. Small licensees in particular would benefit from guidance about the nature of cyber insurance coverage they should carry.

Investigation of a Data Breach (Section 5)

We appreciate substantial improvements to this section. However, additional revisions are required to clarify how a licensee will have the business-leverage to "conduct a prompt investigation" of a third-party service provider and "perform or oversee reasonable measures to restore the security of the information systems compromised in the data breach." In addition, Section 5(B)(2) should clarify that "any personal information" means "unencrypted" personal information.

Notification of a Data Breach (Section 6)

This section may require additional clarifications to make the Model Law workable. In particular, Section 6(D)(2) indicates that the "commissioner shall have the right to review the proposed communication before the licensee sends it to consumers." Although a right to edit is not expressly stated, it appears implied and there is no limit on the amount of time the commissioner has to review the proposed communication.

Further, there is still the issue of the licensee having to notice and to circulate draft consumer notices to as many as fifty state commissioners. It is likely that licensees in the title insurance industry would not have the current address of the consumer and so would not be able to identify which state regulators should receive notice with complete accuracy. As stated in our previous comment letter, it would be a more workable approach if the Model Law would employ the Lead State approach already utilized by the NAIC. As is stated in the NAIC website, "[t]he concept of Lead State is not intended to relinquish the authority of any state, nor is it intended to increase any state's statutory authority or to put any state at a disadvantage. It is intended to facilitate efficiencies when one state coordinates the regulatory processes of all states involved

The Model Law continues to require "an offer from the licensee to the consumer to provide appropriate identity theft protection services…" in Section 6(D)(2)(g). As we indicated in previous comment letters, the effectiveness of identity theft protection has been repeatedly questioned and is less favored than a credit freeze, which is a more generally agreed upon method of identity theft protection.

Consumer Protections Following a Data Breach (Section 7)

ALTA members continue to be concerned about the absence of any limitations to the power of the Commissioner under this section. Offering a regulator unchecked autonomy over what remediation to take will result in uneven, unpredictable, and possibly unsuitable outcomes. Our industry values consumer protections, but those protections should be clearly defined with an appropriate due process mechanism in place for licensees. Absent these protections, enforceability of the Model Law may be hamstrung by due process claims.

For these reasons, we again encourage the NAIC to delete this section from the draft or more clearly define what constitutes "the appropriate level of consumer protection required following the data breach and how long that protection will be provided" to ensure regulator, licensee and consumer expectations align. This section should more specifically enumerate the consumer protections the commissioner may prescribe as well as an objective standard by which the commissioner should make that prescription.

Effective Date (Section 14)

We urge the Task Force to seriously consider a workable effective date of the Model Law. As we indicated in our March 23 and June 3 comment letters:

> The Effective Date should factor in an adequate phase-in period, allowing such covered entities a minimum 24 months necessary to: (i) come to understand the new requirements (presumably through industry educational events, articles and other guidance); (ii) hire appropriate third-party information security and privacy professionals; (iii) undergo testing and remediation; and (iv) undergo a risk assurance or certification process. NAIC should also commit to a robust national and local education and support program in order for licensees, particularly small producers to have a bona fide opportunity to become compliant.

Again, ALTA members thank the Task Force for allowing our industry to offer comments on Version 2 of the Insurance Data Security Model Law. We look forward to continuing to work with the Task Force on proposed changes to the Model Law. Should you have any questions about this comment letter, please contact me at justin@alta.org or 202-261-2937.

Sincerely,

Justin Ailes
Vice President, Government and Regulatory Affairs

Draft: 8/17/2016 (version 2)
A new model: Insurance Data Security Model Law
Cybersecurity (EX) Task Force

Comments are being requested on this draft by Friday, September 16, 2016. Comments should be sent by email to Sara Robben at srobben@naic.org.

INSURANCE DATA SECURITY MODEL LAW

Table of Contents

Section 1. Title

This act shall be known and may be cited as the "Insurance Data Security Act."

Section 2. Purpose and Intent

Notwithstanding any other provision of law including [insert reference to state's general data security breach notification law], the purpose and intent of this Act is to establish the exclusive standards in this state for data security and investigation and notification of a data breach applicable to licensees, as defined in Section 3G. This Act shall not be construed as superseding, altering, or affecting any statute, regulation, order or interpretation of law in this state, except to the extent that such statute, regulation, order or interpretation is inconsistent with the provisions of this Act and then only to the extent of the inconsistency. A state statute, regulation, order or interpretation is not inconsistent with the provisions of this Act if the protection such statute, regulation, order or interpretation affords any person is greater than the protection provided under this Act.

This Act may not be construed to create or imply a private cause of action for violation of its provisions nor to curtail a private cause of action which would otherwise exist in the absence of this Act.

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

A. "Consumer" means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, certificate holders and others whose personal information is in a licensee's possession, custody or control.

B. "Consumer reporting agency" has the same meaning as "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

C. "Data breach" means the unauthorized acquisition, release or use of personal information.

The term "data breach" does not include the unauthorized acquisition, release or use of encrypted personal information if the encryption, process or key is not also acquired, released or used without authorization.

D. "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

E. "Harm or inconvenience" means any of the following or the reasonable likelihood thereof:

(1) Identity theft;

(2) Fraudulent transactions on financial accounts; or

(3) Other misuse as defined by [insert state definition of misuse or comparable term, if applicable].

Drafting Note: Several states have defined the term "misuse" in state law and can refer to this in Section 3E(3). If a state does not have this term defined, they may consider either deleting that paragraph or defining misuse above using a definition similar to that of other states. For example, see 17-A Me. Rev. Stat. § 905-A, which provides that

A person is guilty of misuse of identification if, in order to obtain confidential information, property or services, the person intentionally or knowingly:

A. Presents or uses a credit or debit card that is stolen, forged, canceled or obtained as a result of fraud or deception;
B. Presents or uses an account, credit or billing number that that person is not authorized to use or that was obtained as a result of fraud or deception; or
C. Presents or uses a form of legal identification that that person is not authorized to use.

F. "Information security program" means the safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.

G. "Licensee" means any person or entity licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state.

H. "Personal Information" means:

(1) A financial account number relating to a consumer, including a credit card number or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account; or

(2) Information including:

The first name or first initial and last name of a consumer in combination with:

(a) The consumer's non-truncated social security number;

(b) The consumer's driver's license number, passport number, military identification number, or other similar number on a government-issued document;

(c) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online or financial account of the consumer;

(d) Biometric data of the consumer that would permit access to financial accounts of the consumer;

(e) Any information of the consumer that the licensee has a legal or contractual duty to protect from unauthorized access or public disclosure;

(f) The consumer's date of birth;

(g) Information that the consumer provides to a licensee to obtain an insurance product or service used primarily for personal, family, or household purposes from the licensee;

(h) Information about the consumer resulting from a transaction involving an insurance product or service used primarily for personal, family, or household purposes between a licensee and the consumer;

(i) Information the licensee obtains about the consumer in connection with providing an insurance product or service used primarily for personal, family, or household purposes to the consumer; or

(j) A list, description, or other grouping of consumers (and publicly available information pertaining to them), that is derived using the information described in Section 3H(2)(g) through (i), that is not publicly available.

(3) Any of the data elements identified in Section 3H(2)(a) through (f) when not in connection with the consumer's first name or initial and last name, if those elements would be sufficient to permit the fraudulent assumption of the consumer's identity or unauthorized access to an account of the consumer.

(4) Any information or data except age or gender, that relates to:

(a) The past, present or future physical, mental or behavioral health or condition of a consumer;

(b) The provision of health care to a consumer; or

(c) Payment for the provision of health care to a consumer.

The term "personal information" does not include publicly available information that is lawfully made available to the general public and obtained from federal, state, or local government records; or widely distributed media.

I. "Third-party service provider" means a person or entity that contracts with a licensee to maintain, process, store or otherwise have access to personal information under the licensee's possession, custody or control.

Section 4. Information Security Program

A. Implementation of an Information Security Program

Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities and the sensitivity of the personal information in the licensee's possession, custody or control, each licensee shall develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for the protection of personal information. The licensee shall document, on an ongoing basis, compliance with its information security program.

B. Objectives of Information Security Program

A licensee's information security program shall be designed to:

(1) Protect the security and confidentiality of personal information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information;

(3) Protect against unauthorized access to or use of personal information, and minimize the likelihood of harm or inconvenience to any consumer; and

(4) Define and periodically reevaluate a schedule for retention of personal information and a mechanism for its destruction when no longer needed.

C. Risk Assessment

The licensee shall:

(1) Designate an employee or employees responsible for the information security program;

(2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of personal information or personal information systems;

(3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

(4) Assess the sufficiency of policies, procedures, personal information systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including:

(a) Employee training and management;

(b) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and

(c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(5) Implement information safeguards to manage the threats identified in its assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures.

D. Risk Management

The licensee shall, at a minimum:

(1) Design its information security program to mitigate the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities, based on generally accepted cybersecurity principles, including the following security measures, as appropriate:

(a) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent the unauthorized acquisition, release or use of personal information to or by employees or unauthorized individuals outside of the licensee;

(b) Restrict access at physical locations containing personal information, only to authorized individuals;

(c) Encrypt all personal information while being transmitted on a public internet network or wirelessly and all personal information stored on a laptop computer or other portable computing or storage device or media;

(d) Ensure that information system modifications are consistent with the licensee's information security program;

(e) Utilize state of the art techniques, such as multi-factor authentication procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, personal information;

(f) Regularly test or monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(g) Implement response procedures that specify actions to be taken when the licensee suspects or detects that unauthorized individuals have gained access to information systems;

(h) Implement measures to protect against destruction, loss, or damage of personal information due to environmental hazards, such as fire and water damage or technological failures; and

(i) Develop, implement, and maintain procedures for the secure disposal of personal information in any format.

(2) Include cybersecurity risks in the licensee's enterprise risk management process; and

(3) Use generally accepted cybersecurity principles to share information and stay informed regarding emerging threats or vulnerabilities.

E. Oversight by Board of Directors

If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(1) Oversee the development, implementation, and maintenance of the licensee's information security program, including assigning specific responsibility for the plan to the licensee's executive management; and

(2) Require the licensee's executive management to report in writing at least annually, the following information:

(a) The overall status of the information security program and the licensee's compliance with this Act; and

(b) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, data breaches or violations and management's responses thereto, and recommendations for changes in the information security program.

F. Oversight of Third-Party Service Provider Arrangements

The licensee shall contract only with third-party service providers that are capable of maintaining appropriate safeguards for personal information in the licensee's possession, custody or control, and the licensee shall be responsible for any failure by such third-party service providers to protect personal information provided by the licensee to the third-party service providers consistent with this Act.

G. Program Adjustments

The licensee shall monitor, evaluate and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its personal information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to personal information systems.

Section 5. Investigation of a Data Breach

A. If the licensee learns that a data breach has or may have occurred in relation to personal information in the possession, custody or control of the licensee or any of the licensee's third-party service providers, the licensee shall conduct a prompt investigation.

B. During the investigation, the licensee shall, at a minimum:

(1) Assess the nature and scope of the data breach or potential data breach;

(2) Identify any personal information that may have been involved in the data breach;

(3) Determine whether the personal information has been acquired, released or used without authorization; and

(4) Perform or oversee reasonable measures to restore the security of the information systems compromised in the data breach in order to prevent further unauthorized acquisition, release or use of personal information in the licensee's possession, custody or control.

Section 6. Notification of a Data Breach

A. If following an investigation under Section 5, the licensee determines that an unauthorized acquisition of personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) involved in a data breach has occurred, the licensee, or a third party acting on behalf of the licensee, shall notify:

(1) All consumers to whom the personal information relates;

(2) The insurance commissioner in the licensee's state of domicile and the insurance commissioners of all the states in which a consumer whose information was or may have been compromised resides;

(3) The relevant Federal and state law enforcement agencies, as appropriate;

(4) Any relevant payment card network, if the data breach involves payment card numbers; and

(5) Each consumer reporting agency, if the data breach involves personal information relating to 500 or more consumers.

B. Notification to the Commissioner

Notwithstanding the responsibilities prescribed in Sections 5A and 6A of this Act, no later than three (3) business days after determining that a data breach has occurred, the licensee shall notify the commissioner that a data breach has occurred. The licensee shall provide as much of the following information as possible:

(1) Date of the data breach;

(2) Description of the data breach, including how the information was exposed, whether lost, stolen, or breached;

(3) How the data breach was discovered;

(4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(5) The identity of the source of the data breach;

(6) Whether licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(7) Description of the type of information lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc.);

(8) Whether, if the information was encrypted, the encryption, redaction or protection process or key was also acquired without authorization;

(9) The period during which the information system was compromised by the data breach;

(10) The number of total consumers and consumers of each state affected by the data breach;

(11) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;

(12) Identification of efforts being undertaken to remediate the situation which permitted the data breach to occur;

(13) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the data breach; and

(14) Name of a contact person who is both familiar with the data breach and authorized to act for the licensee.

The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning the data breach.

C. Notification to Consumer Reporting Agencies

The licensee shall notify, as expediently as possible and without unreasonable delay, after determining that a data breach has occurred, each consumer reporting agency, if the data breach involves personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) relating to 500 or more consumers. Notification must include the date of the data breach, an estimate of the number of persons affected by the data breach, if known, and the actual or anticipated date that persons were or will be notified of the data breach.

D. Notification to Consumers

(1) The licensee shall notify all consumers whose personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) was affected as expediently as possible and without unreasonable delay, and in no case later than sixty (60) calendar days after determining that a data breach has occurred.

(2) Prior to sending the notification, the licensee shall provide the commissioner with a draft of the proposed written communication to consumers. The commissioner shall have the right to review the proposed communication before the licensee sends it to consumers, to ensure compliance with this subsection and to prescribe the appropriate level of consumer protection pursuant to Section 7.

The notice must be written in straightforward language and include the following information::

(a) A description of the type of information involved in the data breach;

(b) A description of the action that the licensee or third-party service provider has taken to safeguard the information;

(c) A summary of rights of victims of identity theft prepared under § 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g(d));

(d) The steps consumers can take to protect themselves from identity theft or fraud, which shall include an explanation that consumers shall have a right to do the following:

(i) Place a 90-day initial fraud alert on their consumer reports;

(ii) Place a seven-year extended fraud alert on their consumer reports;

(iii) Place a credit freeze on their consumer reports;

(iv) Have a free copy of their consumer report from each credit bureau;

(v) Receive fraudulent information related to the data breach removed (or "blocked") from their consumer reports;

(vi) Dispute fraudulent or wrong information on their consumer reports;

(vii) Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach;

(viii) Receive copies of documents related to the identity theft; and

(ix) Stop contacts from debt collectors related to the data breach;

(e) Contact information for the three nationwide consumer reporting agencies;

(f) Contact information for the licensee or its designated call center; and

(g) An offer from the licensee to the consumer to provide appropriate identity theft protection services free of cost to the consumer for a period of not less than twelve (12) months, if appropriate, or other consumer protections ordered by the commissioner pursuant to Section 7 of this Act.

(3) The licensee will provide the consumer notification:

(a) In writing by first class mail; or

(b) Electronically if the consumer has agreed to be contacted through e-mail or other means pursuant to [insert reference to state Electronic Transactions Act.]; or

(c) By substitute method, if the licensee demonstrates to the commissioner's satisfaction that the cost of providing notice by Section 6D(3)(a) or (b) would be excessive or that another legitimate reason exists for substitute notice. The substitute method must include conspicuous posting of the notice on the licensee's publicly accessible website and publication in statewide media in this state.

E. Notice Regarding Data Breaches of Third-Party Service Providers

In the event of a data breach in a system maintained by a third-party service provider, the licensee shall comply with Section 6A through D. The computation of licensee's deadlines shall begin on the day after the third-party service provider notifies the licensee of the data breach or the licensee otherwise has actual knowledge of the data breach, whichever is sooner.

F. Notwithstanding the requirements of Section 6C, D, and E, notice may be delayed where requested by an appropriate state or federal law enforcement agency. The commissioner shall be notified of any such request.

Drafting Note: Section 5 and Section 6 may be duplicative of current state law. Each state should conduct its own analysis to determine whether or not Section 5 and Section 6, in whole or in part, are necessary to be included in its statutes.

Section 7. Consumer Protections Following a Data Breach

After reviewing the licensee's data breach notification, the commissioner shall prescribe the appropriate level of consumer protection required following the data breach and how long that protection will be provided. The commissioner may order the

licensee to offer to pay for twelve (12) months or more of identity theft protection for affected consumers, pay for a credit freeze, or take other action deemed necessary to protect consumers.

Drafting Note: Many states have statutes providing that a consumer reporting agency cannot charge a fee for a credit freeze on a consumer file when the consumer is a victim of identity theft, which is shown by providing a police report. For an example, *see* Tex. Bus. & Com. Code § 20.04(b). As an alternative to having the licensee pay for the credit freeze, a state should consider referencing that law and providing that the credit freeze is free for consumers after the data breach is reported to law enforcement by the licensee, by showing a data breach notification letter from the licensee. The state may also need to amend its free credit freeze law to ensure this is covered.

If the data breach has affected consumers in other states, the commissioner shall, consistent with the requirements of [reference to statute describing the commissioner's general powers] and with the circumstances of the data breach as they affect consumers in this state, cooperate with the insurance regulators of those states in prescribing the appropriate level of consumer protection described in the previous sentence.

Section 8. Power of Commissioner

The commissioner shall have power to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the commissioner has under [insert applicable statutes governing the investigation or examination of insurers]. Any such investigation or examination shall be conducted pursuant to [insert applicable statutes governing the investigation or examination of insurers].

Section 9. Enforcement

Whenever the commissioner has reason to believe that a licensee has been or is engaged in conduct in this state which violates this Act, the commissioner may issue and serve upon such licensee a statement of charges and notice of hearing to be held at a time and place fixed in the notice. The hearing shall be conducted in accordance with [cite provisions of state administrative procedure act or insurance code applicable to administrative enforcement proceedings for serious violations].

Section 10. Confidentiality

A. Any documents, materials or other information in the control or possession of the department of insurance that are furnished by a licensee or an employee or agent thereof acting on behalf of licensee pursuant to Section 6B(2), (3), (4), (5), (6), (8), (11), and (12), or that are obtained by the insurance commissioner in an investigation or examination pursuant to Section 8 of this Act shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the insurance commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the insurance commissioner's duties.

B. Neither the insurance commissioner nor any person who received documents, materials or other information while acting under the authority of the insurance commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 10A.

C. In order to assist in the performance of the insurance commissioner's duties under this Act, the insurance commissioner:

(1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 10A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees to maintain the confidentiality and privileged status of the document, material or other information;

(2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or

domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information; and

(3) **[OPTIONAL]** May enter into agreements governing sharing and use of information consistent with this subsection.

D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in Section 10C.

E. Nothing in this Act shall prohibit the insurance commissioner from releasing final, adjudicated actions including for cause terminations that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

Drafting Note: States conducting an investigation or examination under their examination law may apply the confidentiality protections of that law to such an investigation or examination.

Section 11. Penalties

In the case of a violation of this Act a licensee may be penalized in accordance with [insert general penalty statute].

Section 12. Rules and Regulations

The commissioner may, upon notice and opportunity for all interested persons to be heard, issue such rules, regulations and orders as shall be necessary to carry out the provisions of this Act.

Section 13. Severability

If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby.

Section 14. Effective Date

This Act shall take effect on [insert a date which allows at least a one year interval between the date of enactment and the effective date].

NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
PROPOSED
23 NYCRR 500

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by Sections 102, 201, 202, 301, 302, 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules, and Regulations of the State of New York, to take effect upon publication in the State Register, to read as follows:

(ALL MATTER IS NEW)

Section 500.0 Introduction.

The New York State Department of Financial Services ("DFS") has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cyber threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

Section 500.01 Definitions.

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

(b) *Authorized User* means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(c) *Covered Entity* means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law.

(d) *Cybersecurity Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

(e) *Information System* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(f) *Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

(g) *Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is:

(1) Any business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

(2) Any information that an individual provides to a Covered Entity in connection with the seeking or obtaining of any financial product or service from the Covered Entity, or is about an individual resulting from a transaction involving a financial product or service between a Covered Entity and an individual, or a Covered Entity otherwise obtains about an individual in connection with providing a financial product or service to that individual;

(3) Any information, except age or gender, that is created by, derived or obtained from a health care provider or an individual and that relates to the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family or household, or from the provision of health care to any individual, or from payment for the provision of health care to any individual;

(4) Any information that can be used to distinguish or trace an individual’s identity, including but not limited to an individual’s name, social security number, date and place of birth, mother’s maiden name, biometric records, any information that is linked or linkable to an individual, including but not limited to medical,

educational, financial, occupational or employment information, information about an individual used for marketing purposes or any password or other authentication factor.

(h) *Person* means any individual, partnership, corporation, association or any other entity.

(i) *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System.

(j) *Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) *Risk-Based Authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(l) *Senior Officer(s)* mean the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity including a branch or agency of a foreign banking organization subject to this Part.

Section 500.02 Cybersecurity Program.

(a) Cybersecurity Program. Each Covered Entity shall establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity's Information Systems.

(b) The cybersecurity program shall be designed to perform the following core cybersecurity functions:

(1) identify internal and external cyber risks by, at a minimum, identifying the Nonpublic Information stored on the Covered Entity's Information Systems, the sensitivity of such Nonpublic Information, and how and by whom such Nonpublic Information may be accessed;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill all regulatory reporting obligations.

Section 500.03 Cybersecurity Policy.

(a) Cybersecurity Policy. Each Covered Entity shall implement and maintain a written cybersecurity policy setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall address, at a minimum, the following areas:

(1) information security;

(2) data governance and classification;

(3) access controls and identity management;

(4) business continuity and disaster recovery planning and resources;

(5) capacity and performance planning;

(6) systems operations and availability concerns;

(7) systems and network security;

(8) systems and network monitoring;

(9) systems and application development and quality assurance;

(10) physical security and environmental controls;

(11) customer data privacy;

(12) vendor and third-party service provider management;

(13) risk assessment; and

(14) incident response.

(b) The cybersecurity policy shall be reviewed by the Covered Entity's board of directors or equivalent governing body, and approved by a Senior Officer of the Covered Entity. If no such board of directors or equivalent governing body exists, the cybersecurity policy shall be reviewed and approved by a Senior Officer of the Covered Entity. Such review and approval shall occur as frequently as necessary to address the cybersecurity risks applicable to the Covered Entity, but no less frequently than annually.

Section 500.04 Chief Information Security Officer.

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual to serve as the Covered Entity's Chief Information Security Officer ("CISO") responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. To the extent this requirement is met using third party service providers, the Covered Entity shall:

(1) retain responsibility for compliance with this Part;

(2) designate a senior member of the Covered Entity's personnel responsible for oversight of the third party service provider; and

(3) require the third party service provider to maintain a cybersecurity program that meets the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall develop a report, at least bi-annually, as described herein. Such report shall be timely presented to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. Such report shall be made available to the superintendent upon request. The report shall:

(1) assess the confidentiality, integrity and availability of the Covered Entity's Information Systems;

(2) detail exceptions to the Covered Entity's cybersecurity policies and procedures;

(3) identify cyber risks to the Covered Entity;

(4) assess the effectiveness of the Covered Entity's cybersecurity program;

(5) propose steps to remediate any inadequacies identified therein; and

(6) include a summary of all material Cybersecurity Events that affected the Covered Entity during the time period addressed by the report.

Section 500.05 Penetration Testing and Vulnerability Assessments.

(a) The cybersecurity program for each Covered Entity shall, at a minimum, include:

(1) penetration testing of the Covered Entity's Information Systems at least annually; and

(2) vulnerability assessment of the Covered Entity's Information Systems at least quarterly.

Section 500.06 Audit Trail.

(a) The cybersecurity program for each Covered Entity shall, at a minimum, include implementing and maintaining audit trail systems that:

(1) track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting necessary to enable the Covered Entity to detect and respond to a Cybersecurity Event;

(2) track and maintain data logging of all privileged Authorized User access to critical systems;

(3) protect the integrity of data stored and maintained as part of any audit trail from alteration or tampering;

(4) protect the integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction;

(5) log system events including, at a minimum, access and alterations made to the audit trail systems by the systems or by an Authorized User, and all system administrator functions performed on the systems; and

(6) maintain records produced as part of the audit trail for not fewer than six years.

Section 500.07 Access Privileges.

As part of its cybersecurity program, each Covered Entity shall limit access privileges to Information Systems that provide access to Nonpublic Information solely to those individuals who require such access to such systems in order to perform their responsibilities and shall periodically review such access privileges.

Section 500.08 Application Security.

(a) Each Covered Entity's cybersecurity program shall, at a minimum, include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, as well as procedures for assessing and testing the security of all externally developed applications utilized by the Covered Entity.

(b) All such procedures, guidelines and standards shall be reviewed, assessed and updated by the CISO of the Covered Entity at least annually.

Section 500.09 Risk Assessment.

(a) At least annually, each Covered Entity shall conduct a risk assessment of the Covered Entity's Information Systems. Such risk assessment shall be carried out in accordance with written policies and procedures and shall be documented in writing.

(b) As part of such policies and procedures, each Covered Entity shall include, at a minimum:

(1) criteria for the evaluation and categorization of identified risks;

(2) criteria for the assessment of the confidentiality, integrity and availability of the Covered Entity's Information Systems, including the adequacy of existing controls in the context of identified risks; and

(3) requirements for documentation describing how identified risks will be mitigated or accepted based on the risk assessment, justifying such decisions in light of the risk assessment findings, and assigning accountability for the identified risks.

Section 500.10 Cybersecurity Personnel and Intelligence.

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in 500.04(a), each Covered Entity shall:

(1) employ cybersecurity personnel sufficient to manage the Covered Entity's cybersecurity risks and to perform the core cybersecurity functions specified in section 500.02(b)(1)-(5) of this Part;

(2) provide for and require all cybersecurity personnel to attend regular cybersecurity update and training sessions; and

(3) require key cybersecurity personnel to take steps to stay abreast of changing cybersecurity threats and countermeasures.

(b) A Covered Entity may choose to utilize a qualified third party to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

Section 500.11 Third Party Information Security Policy.

(a) Third Party Information Security Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, third parties doing business with the Covered Entity. Such policies and procedures shall address, at a minimum, the following areas:

(1) the identification and risk assessment of third parties with access to such Information Systems or such Nonpublic Information;

(2) minimum cybersecurity practices required to be met by such third parties in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such third parties; and

(4) periodic assessment, at least annually, of such third parties and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include establishing preferred provisions to be included in contracts with third party service providers, including provisions addressing, to the extent applicable:

(1) the use of Multi-Factor Authentication as set forth in Section 500.12 to limit access to sensitive systems and Nonpublic Information;

(2) the use of encryption to protect Nonpublic Information in transit and at rest;

(3) prompt notice to be provided to the Covered Entity in the event of a Cybersecurity Event affecting the third party service provider;

(4) identity protection services to be provided for any customers materially impacted by a Cybersecurity Event that results from the third party service provider's negligence or willful misconduct;

(5) representations and warranties from the third party service provider that the service or product provided to the Covered Entity is free of viruses, trap doors, time bombs and other mechanisms that would impair the security of the Covered Entity's Information Systems or Nonpublic Information; and

(6) the right of the Covered Entity or its agents to perform cybersecurity audits of the third party service provider.

Section 500.12 Multi-Factor Authentication.

(a) Multi-Factor Authentication. Each Covered Entity shall:

(1) require Multi-Factor Authentication for any individual accessing the Covered Entity's internal systems or data from an external network;

(2) require Multi-Factor Authentication for privileged access to database servers that allow access to Nonpublic Information;

(3) require Risk-Based Authentication in order to access web applications that capture, display or interface with Nonpublic Information; and

(4) support Multi-Factor Authentication for any individual accessing web applications that capture, display or interface with Nonpublic Information.

Section 500.13 Limitations on Data Retention.

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the timely destruction of any Nonpublic Information identified in 500.01(g)(2)-(4) that is no longer necessary for the provision of the products or services for which such information was provided to the Covered Entity, except where such information is otherwise required to be retained by law or regulation.

Section 500.14 Training and Monitoring.

(a) As part of its cybersecurity program, each Covered Entity shall:

(1) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and

(2) provide for and require all personnel to attend regular cybersecurity awareness training sessions that are updated to reflect risks identified by the Covered Entity in its annual assessment of risks.

Section 500.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, each Covered Entity shall encrypt all Nonpublic Information held or transmitted by the Covered Entity both in transit and at rest.

(b) To the extent encryption of Nonpublic Information in transit is currently infeasible, Covered Entities may instead secure such Nonpublic Information using appropriate alternative compensating controls reviewed and approved by the Covered Entity's CISO. Such compensating controls shall not be used in lieu of meeting the requirements of subsection 500.15(a) after one year from the date this regulation becomes effective.

(c) To the extent encryption of Nonpublic Information at rest is currently infeasible, Covered Entities may instead secure such Nonpublic Information using appropriate alternative compensating controls reviewed and approved by the Covered Entity's CISO. Such compensating controls shall not be used in lieu of meeting the requirements of subsection 500.15(a) after five years from the date this regulation becomes effective.

Section 500.16 Incident Response Plan.

(a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business.

(b) Such incident response plan shall, at a minimum, address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;

(2) the goals of the incident response plan;

(3) the definition of clear roles, responsibilities and levels of decision-making authority;

(4) external and internal communications and information sharing;

(5) remediation of any identified weaknesses in Information Systems and associated controls;

(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and

(7) the evaluation and revision of the incident response plan following a Cybersecurity Event.

Section 500.17 Notices to Superintendent.

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent of any Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that

affects Nonpublic Information. The Covered Entity must notify the superintendent as promptly as possible but in no event later than 72 hours after becoming aware of such a Cybersecurity Event. Such Cybersecurity Events include, but are not limited to:

(1) any Cybersecurity Event of which notice is provided to any government or self-regulatory agency;

(2) any Cybersecurity Event involving the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information.

(b) Annually each Covered Entity shall submit to the superintendent a written statement by January 15, in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years.

(1) To the extent a Covered Entity has identified areas, systems, or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

(2) To the extent that a Covered Entity has identified any material risk of imminent harm relating to its cybersecurity program the Covered Entity shall notify the superintendent within 72 hours and include such items in its annual report filed pursuant to this section.

Section 500.18 Limited Exemption.

(a) Limited Exemption. Each Covered Entity with:

(1) fewer than 1000 customers in each of the last three calendar years, and

(2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and

(3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates, shall be exempt from the requirements of this Part other than the requirements set forth in this section, Sections 500.02, 500.03, 500.07, 500.09, 500.11, 500.13, 500.17, 500.19, 500.20 and 500.21.

(b) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for the limited exemption as set forth in subsection 500.18(a), such Covered Entity shall have 180 days from such fiscal year end to comply with all requirements of this Part.

Section 500.19 Enforcement.

This regulation will be enforced pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

Section 500.20 Effective Date.

This part will be effective January 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under Section 500.17 commencing January 15, 2018.

Section 500.21 Transitional Period.

Transitional Period. Covered Entities shall have 180 days from the effective date of this regulation to comply with the requirements set forth in this Part, except as otherwise specified.

Section 500.22 Severability.

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.

APPENDIX A (Part 500)

_____

(**Covered Entity Name)**

January 15, 20_____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity as of_____(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended_(year for which Board Resolution or Compliance Finding is provided) complies with Part ___.

(3)
Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_____ Date: _____

[DFS Portal Filing Instructions]

ALTA Best Practices
Maturity Model Explainer

Background:

What is a maturity model?

A: *A maturity model is a business tool that measures a company's procedures against an established standard, such as the ALTA Best Practices. The term "maturity" refers to the strength of a company's procedures and whether they are followed consistently. There are several levels that benchmark a company's maturity.*

Are maturity models used in other industries?

A: *Yes. Maturity models have been used for decades in a number of industries, including technology and lending. Regulators, including the Consumer Financial Protection Bureau, use them in their compliance assessments.*

Why did ALTA create the Best Practices Maturity Model?

A: *ALTA constantly strives to produce valuable tools to help the title and settlement industry implement Best Practices. This new Maturity Model provides an alternative way of determining how a company's procedures measure against the Best Practices.*

Using the Maturity Model:

How does my company use the Maturity Model?

A: *Your company can use the Maturity Model as an internal tool for identifying progress toward complying with the Best Practices. The results are shown in a summary similar to a report card.*

How does the Maturity Model help my company improve its compliance with the Best Practices?

A: *The Maturity Model features benchmark compliance levels that measure against your company's practices to determine where they lie on a compliance spectrum. The features of higher benchmark levels provide ways to enhance your procedures and move up the spectrum.*

For more information about the Best Practices, please visit www.alta.org/bestpractices

Does completing the Maturity Model mean my company complies with the Best Practices?

A: *Along with other tools from ALTA, the Maturity Model will help you identify ways to comply with the ALTA Best Practices. A company complies with the Best Practices when its procedures achieve the highest level of maturity.*

A lender has requested a copy of my company's Best Practices certification. Can I use the Maturity Model to show the procedures my company has in place to comply with the Best Practices?

A: *You should ask your lender about what type of compliance documentation it would like to see and whether they have a preference about who performs the assessment. Some lenders may require specific types of assessments or responses. ALTA recommends that you undergo a Best Practices assessment every 24 months.*

Assessments:

Does the Maturity Model change the Best Practices or the assessment process?

A: *No. The Maturity Model does not alter the ALTA Best Practices, nor does it change the required testing for an assessment. All assessments should be performed using the Best Practices Assessment Procedures.*

Does ALTA provide any guidance on how to undergo a Best Practices assessment?

A: *Yes. If you would like more information about how to prepare for and undergo a Best Practices assessment, please refer to ALTA's Assessment Guide and FAQ Resource.*

My company already underwent a Best Practices assessment and has a compliance report. Do I need to undergo an additional assessment using the Maturity Model?

A: *The Maturity Model does not change or invalidate any assessment your company previously obtained. If your company is fully compliant with the Best Practices, you should be in the "Optimized" category of the Maturity Model for each Best Practice.*

How to Complete the Maturity Model:

How do I complete the Maturity Model for my company?

A: *To use the Maturity Model, follow the steps below:*

1. *Undergo a Best Practices assessment following the Best Practices Assessment Procedures*
2. *Match the results to the benchmark compliance level within the Maturity Model*
3. *Mark with an "X" the benchmark compliance level for each Best Practice within the Maturity Model Summary*
4. *In the Progress Plan section of the Maturity Model Summary, list the steps, if any, your company is taking to reach a higher benchmark compliance level*

What are "benchmark compliance levels"?

A: *The Maturity Model matches your company's procedures against five benchmark levels of Best Practices compliance. These levels are based on the strength of your company's procedures and the extent to which they are followed.*

The five benchmark levels of Best Practices compliance featured in the Maturity Model are:

- ***Ad Hoc**: company has not yet established any policies or procedures*
- ***Planning**: company is developing compliance. It has either established but not yet implemented written policies and procedures, or it follows policies and procedures, but has not yet written them in a manual*
- ***Defined**: company is partially compliant with the Best Practices*
- ***Managed**: company is substantially compliant with the Best Practices*
- ***Optimized**: company is fully compliant with the Best Practices*

Why do some Best Practices not have standards for each benchmark compliance level?

A: *Some of the Best Practices do not have defined standards for each of the benchmark compliance levels. For example in Pillar 1, either a company has the proper licenses or it does not. Thus, a company would fall in either the "Optimized" or "Ad hoc" category. Undefined benchmark compliance levels are empty on the Maturity Model and are shown as black boxes on the Maturity Model Summary.*

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).

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

OCC BULLETIN 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.

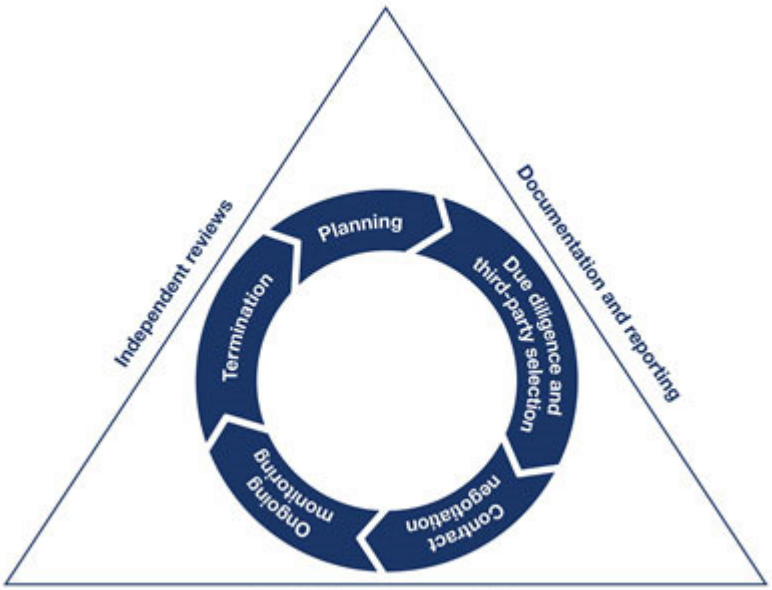
In addition, a bank should perform the following throughout the life cycle of the relationship as part of its risk management process:

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

"For further information, contact John Eckert, Director, Operational Risk and Core Policy at (202) 649-7163 or john.eckert@occ.treas.gov [mailto:john.eckert@occ.treas.gov], or (202) 649-6550.

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 Consumer Protection and Safety and Soundness	Provides guidance to enhance, clarify, and increase awareness regarding the measures the OCC expects to see in place for tax refund-related products offered 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	Provides guidance on determining if a RESPA settlement service provider (often a third-party servicer or vendor) is charging more for a settlement service

		Guidance—Mark-ups of Settlement Service Fees	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.

South Carolina Bar

We Built This City (On Rock & Roll): Community Building — Development for Small Business

Moderator — Claire T. Manning
Columbia, SC

Julia Prater — Columbia, SC
Kevin Garrison — Columbia, SC
Tyler Gregg — Columbia, SC

CLE Outline

Hospital's interest

1. Public safety
2. Lower crime rates
3. Increase in property value
4. Employees of hospital can live closer to work
5. Stimulation of local economy

Governmental Involvement

1. Eviction process of public housing residents
2. Public hearings (for traffic concerns, etc.)
3. Would roads have to changed or expanded?
4. Any implications for city concerning increased tax revenue
5. Re-zoning issues
    a. Constraints on zoning—no spot zoning allowed
        i. Cannot be for the benefit of only one person and to the detriment of everyone else
    b. Criteria for the review of special exception (if required)
        i. Whether the proposal will have a substantial adverse impact on vehicular traffic or vehicular and pedestrian safety, and whether adequate provisions are made for parking and for loading and unloading;
        ii. Whether the proposal will have a substantial adverse impact on adjoining properties in terms of environmental factors such as noise, lights, glare, vibration, fumes, odors, obstruction of air or light, and litter;
        iii. Whether the proposal will have a substantial adverse impact on the aesthetic character of the area, to include a review of the orientation and spacing of buildings;
        iv. Whether the proposal will have a substantial adverse impact on public safety or create nuisance conditions detrimental to the public interest or conditions likely to result in increased law enforcement response;
        v. Whether the proposal will create a concentration or proliferation of the same or similar types of special exception use, and if this concentration may be detrimental to the development or redevelopment of the area in which the special exception use is proposed to be developed;
        vi. Whether the proposal is consistent with the character and intent of the underlying district as indicated in the zoning district description, with any applicable zoning overlay district goals and requirements;
        vii. Whether the proposal is appropriate for its location and compatible with the permitted uses adjacent to and in the vicinity of the property; and
        viii. Whether the proposal will adversely affect the public interest.
6. Exactions—costs to local government? Would it create too much traffic?
    a. If so, can force developer to pay, but there must be rough proportionality between the purpose and the exaction (i.e., if traffic is an issue, so force developer to give up portion of land for highway use)
7. Any historic preservation issues?

Palmetto Gardens Development Sources and Uses
(PERMANENT FINANCING)

Grantee or Applicant HA: City of Forest Hills Housing Authority

Development Name and Phase: Palmetto Gardens

Unit Type:	Rental Units			
Number of Units:	**100**			

Development Sources	Federal Funds	Private Funds	Other Public Funds	Total
Low Income Housing Tax Credit Equity	$ 6,000,000	$ -	$ -	$ 6,000,000
Other: FHLB AHP Grant	$ -	$ 500,000	$ -	$ 500,000
Other: State Housing HOME Funds	$ 1,000,000	$ -	$ -	$ 1,000,000
Other: Housing Trust Fund	$	$ -	$ 1,600,000	$ 1,600,000
Other: 221 (d)(4) Permanent Mortgage	$ -	$ 7,500,000	$ -	$ 7,500,000
Other:	$ -	$ -	$ -	$ -
Other:	$ -	$ -	$ -	$ -
Other:	$ -	$ -	$ -	$ -
Other:	$ -	$ -	$ -	$ -
Total Development Sources (Part A)	$ 7,000,000	$ 8,000,000	$ 1,600,000	$ 16,600,000

Development Uses

Development Construction Costs	PH Capital Assist.	Private Funds	Other Public Funds	Total
Residential Construction	$ 4,357,805	$ 5,100,000	$ -	$ 9,457,805
Residential Rehabilitation	$ -	$ -	$ -	$ -
Builder's General Requirements	$ 261,468	$ 246,000	$ -	$ 507,468
Builder's Overhead]	$ 87,156	$ 82,000	$ -	$ 169,156
Builder's Profit	$ 261,468	$ 246,000	$ -	$ 507,468
Site Improvement	$ 1,152,102	$ -	$ 1,152,102	$ 2,304,204
Other: Community Facility	$ 140,000	$ -	$ -	$ 140,000
Subtotal: Development Construction Costs	$ 6,260,000	$ 5,674,000	$ 1,152,102	$ 13,086,102

Development Soft Costs	PH Capital Assist.	Private Funds	Other Public Funds	Total
Acquisition of Site(s)	$ -	$ 1,900,000	$ 447,898	$ 2,347,898
Accounting and Cost Certification	$ -	$ -	$ -	$ -
Appraisal Expense	$ -	$ 15,000	$ -	$ 15,000
Architect & Engineer Fees	$ 250,000	$ 100,000	$ -	$ 350,000
Environmental Assessment, Testing & Cleanup	$ 30,000	$ 20,000	$ -	$ 50,000
Financing & Application Expense, Lender	$ -	$ -	$ -	$ -
Financing & Application Expense, Tax Credit	$ -	$ -	$ -	$ -
Insurance, Construction Period	$ 10,000	$ 25,000	$ -	$ 35,000
Interest, Construction & Bridge Loan(s)	$ 50,000	$ 36,000	$ -	$ 86,000
Legal Expense, Developer & Lender(s)	$ 50,000	$ 25,000	$ -	$ 75,000
Marketing & Lease-up Expense	$ -	$ 50,000	$ -	$ 50,000
Permits, Construction & Utility Hookup	$ 335,000	$ 60,000	$ -	$ 395,000
PILOT & Taxes, Construction Period	$ -	$ 72,000	$ -	$ 72,000
Survey	$ 15,000	$ 15,000	$ -	$ 30,000
Title & Recording Fees	$ -	$ 8,000	$ -	$ 8,000
Subtotal: Development Soft Costs	$ 740,000	$ 2,326,000	$ 447,898	$ 3,513,898
Total Uses for Development (Part A)	$ 7,000,000	$ 8,000,000	$ 1,600,000	$ 16,600,000

Palmetto Gardens -- Management Operating Budget

Number of Bedrooms	Category	Rent	# Units	Annual Rent
3	50 % AMI	600	100	$720,000
Expense Inflation	3.0%	Income Inflation	2.0%	

Operating Year	1	2	3	4	5
Rental Income	720,000	734,400	749,088	764,070	779,351
Vacancy Rate 5%	(36,000)	(36,720)	(37,454)	(38,203)	(38,968)
EFFECTIVE GROSS INC	684,000	697,680	711,634	725,866	740,384
Marketing	1,500	1,545	1,591	1,639	1,688
Mgmt Fee	25,440	26,203	26,989	27,799	28,633
Legal	4,000	4,120	4,244	4,371	4,502
Audit	6,500	6,695	6,896	7,103	7,316
Telephone	500	515	530	546	562
Compliance Monitoring Fees	1,855	1,911	1,968	2,027	2,088
TOTAL ADMIN EXPENSE	39,795	40,989	42,218	43,485	44,789
Telephone	1,200	1,236	1,273	1,311	1,350
Electric	6,000	6,180	6,365	6,556	6,753
Water & Sewer	2,400	2,472	2,546	2,622	2,701
Security	1,680	1,730	1,782	1,835	1,890
TOTAL OPERATING EXP	11,280	11,618	11,966	12,324	12,694
Exterminating	1,700	1,751	1,804	1,858	1,914
Grounds Maintenance	24,000	24,720	25,462	26,226	27,013
Painting & Decorating	5,000	5,150	5,305	5,464	5,628
Structural Repairs	0	0	0	0	0
HVAC Maintenance	2,000	2,060	2,122	2,186	2,252
Plumbing Maintenance	2,000	2,060	2,122	2,186	2,252
Electrical Maint.	2,000	2,060	2,122	2,186	2,252
Clubhouse Maintenance	2,500	2,575	2,652	2,732	2,814
Maintenance Supplies	4,000	4,120	4,244	4,371	4,502
TOTAL MAINT. EXPENSE	43,200	44,496	45,833	47,209	48,627
Office & Admin Salary	25,000	25,750	26,523	27,319	28,139
Employer Payroll Tax	2,200	2,266	2,334	2,404	2,476
TOTAL PAYROLL EXPENSE	27,200	28,016	28,857	29,723	30,615
Real Estate Tax	30,000	30,900	31,827	32,782	33,765
Property & Liab Ins.	50,000	51,500	53,045	54,636	56,275
TOTAL TAXES & INS.	80,000	82,400	84,872	87,418	90,040
Replacement Reserve	13,250	13,648	14,057	14,479	14,913
TOTAL RESERVES	13,250	13,648	14,057	14,479	14,913
TOTAL OPERATING DISB.	214,725	221,167	227,803	234,638	241,678
NET OPERATING INCOME	469,275	476,513	483,831	491,228	498,706
Debt Service	404,607	404,607	404,607	404,607	404,607
TOTAL DEBT SERVICE	404,607	404,607	404,607	404,607	404,607
INCOME OVER/UNDER EXP	64,668	71,906	79,224	86,622	94,099
DEBT COVERAGE RATIO	1.16	1.18	1.20	1.21	1.23
Amortization:					

Principal	Int	Yrs	Payment	Pmt/Yr
7,500,000	4.50%	40	33,717	404,607

Household Budget Worksheet

Family of 4; Spouse 1 makes $10 per hour; Spouse 2 makes $7.50 (minimum wage in SC); one school age child, one in daycare
Budget assumes 40 hour/week employment; most minimum wage jobs are not full time; no benefits

Monthly Take Home Income	
Household wages	3163
Salary or Wages (Spouse)	
Social Security	
Military Pay	
Retirement Interest Income	
Alimony / Child Support	
Unemployment	
SNAP Benefits	
SS & tax withholding - 15%	-475
Total Take Home Income	2688

Housing Expenses 35%	
Rent	800
1st Mortgage (PITI/HOA	
2nd Mortgage (PITI)	
Heating/Cooling	100
Electric	75
Water/Sewer	50
Repairs/Improvements	
Other	
Total Expenses	**$1,025**

Transportation 20%	
Auto Loan	300
Auto Insurance	50
Gas/Maintenance	50
Public Transportation/Taxi	
Parking/Tolls	
Total Expenses	**$400**

Other Living Expenses 20%	
Groceries	500
Eating Out (snacks, meals etc)	
Household Items	25
Clothing	25
Personal Care (toiletries, haircuts, etc)	25
Education (tuition, supplies, activities)	
Entertainment	
Prescriptions	10
Medical (insurance, co-pays)	250
Contributions - tithe to church	200
Child Care	500
Other	
Total Other Living Expenses	**$1,535**

Debt 5%	
Credit Card	
Credit Card	
Credit Card	
Personal Loans	
Student Loans	
Medical Bills	
Other	
Other	
Total Unsecured Debt	**$0**

Investments and Savings	
Emergency Fund	10
Savings Account	20
Financial Goal 1	
Financial Goal 2	
Retirement Funds (IRA, Roth IRA)	
Stocks/Bonds)	
Total Savings	**$30**

Summary of Budget	
Total Take Home (Income)	**$2,688**
Total Living Expenses (-)	**$2,990**
Disposable Income or Deficit	**($302.00)**
Disposable Income as Percent	**-11.24%**

If family lived in affordable housing at 30% of adjusted monthly income, rent drops to $536 per month.

Household Budget Worksheet

Single Parent; 1 child: makes $7.50 (minimum wage in SC); one child in daycare
Budget assumes 40 hour/week employment; most minimum wage jobs are not full time; no benefits

Monthly Take Home Income	
Household wages	1257
Salary or Wages (Spouse)	
Social Security	
Military Pay	
Retirement Interest Income	
Child Support	200
Unemployment	
SNAP Benefits	100
SS & tax withholding - 15%	-188
Total Take Home Income	1369

Housing Expenses 35%	
Rent	600
1st Mortgage (PITI/HOA	
2nd Mortgage (PITI)	
Heating/Cooling	75
Electric	50
Water/Sewer	40
Repairs/Improvements	
Other	
Total Expenses	**$765**

Transportation 20%	
Auto Loan	
Auto Insurance	
Gas/Maintenance	
Public Transportation/Taxi	100
Parking/Tolls	
Total Expenses	**$100**

Other Living Expenses 20%	
Groceries	300
Eating Out (snacks, meals etc)	
Household Items	25
Clothing	25
Personal Care (toiletries, haircuts, etc)	25
Education (tuition, supplies, activities)	
Entertainment	
Prescriptions	10
Medical (insurance, co-pays)	100
Contributions - tithe to church	100
Child Care	400
Other	
Total Other Living Expenses	**$985**

Debt 5%	
Credit Card	
Credit Card	
Credit Card	
Personal Loans	
Student Loans	
Medical Bills	
Other	
Other	
Total Unsecured Debt	**$0**

Investments and Savings	
Emergency Fund	10
Savings Account	20
Financial Goal 1	
Financial Goal 2	
Retirement Funds (IRA, Roth IRA)	
Stocks/Bonds)	
Total Savings	**$30**

Summary of Budget	
Total Take Home (Income)	**$1,369**
Total Living Expenses (-)	**$1,880**
Disposable Income or Deficit	**($511.00)**
Disposable Income as Percent	**-37.33%**

If family lived in affordable housing at 30% of adjusted monthly income for rent and utilities, rent drops to $50 per month.

Development Issues to Consider for Redevelopment of Palmetto Gardens

1. Title Search (60 Years or Longer)
2. Review of Long Term Development Plan by Housing Authority
3. Infrastructure (Existing and Future)
4. Restrictive Covenants (Existing and Future)
5. Zoning
6. Fee Title versus Leasehold Interest in Real Estate
7. Financing

SBA Information Notice

TO: All SBA Employees **CONTROL NO.:** 0000-2169

SUBJECT: Rebranding the 7(a) and 504 Loan Program Names **EFFECTIVE:** November 1, 2016

The U.S. Small Business Administration today is announcing new names for its two core business loan programs. In consultation with our lending partners, SBA has begun the process of renaming and rebranding these loans to better reflect their purposes and improve borrower understanding of SBA's programs. Effective immediately, the 7(a) and 504 loan programs will be referred to by the names outlined below.

- The 7(a) Loan Program has been changed to the SBA Advantage Loan Program
- The 504 Loan Program has been changed to the SBA Grow Loan Program

There is no substantive change to either loan program at this time; today's announcement only impacts the programs' names. All policies, procedures and forms are still in effect. Any changes to the names of the delivery methods within the 7(a) or 504 loan programs will be announced in the future.

The rebranding will roll out over time. SBA expects a transition period, during which time the website, regulations, Standard Operating Procedures, forms, and vendor software will be updated. Due to the gradual introduction of the new names, some documents may continue to use the terms 7(a) and 504 during this transition period.

During the transition period, new Agency communications will reference the names 7(a) and 504 as stated below:

- SBA Advantage Loan Program (previously known as 7(a))
- SBA Grow Loan Program (previously known as 504)

All SBA offices will be responding to public inquiries on our national rebranding initiative.

Maria Contreras-Sweet
Administrator

SBA Form 1353.3 (4-93) MS Word Edition; previous editions obsolete
Must be accompanied by SBA Form 58

SBA Grow Loan Program

Overview:

- Formerly known as the SBA 504 Loan Program
- Consists of a loan secured from a private sector lender with a senior lien covering up to 50 percent of the project cost
- Consists of a loan secured from a Certified Development Corporation or CDC (backed by a 100 percent SBA-guaranteed debenture) with a junior lien covering up to 40 percent of the total cost
- Consists of a contribution from the borrower of at least 10 percent equity

Loan Proceeds can be used for:

- The purchase of land, including existing buildings
- The purchase of improvements, including grading, street improvements, utilities, parking lots and landscaping
- The construction of new facilities or modernizing, renovating or converting existing facilities
- The purchase of long-term machinery and equipment

Loan Proceeds cannot be used for:

- Working capital or inventory
- Consolidating, repaying or refinancing debt
- Speculation or investment in rental real estate

Advantages to Borrowers:

- Low equity injection
- Fixed Rate Loan for 10 years or 20 years

provident
Business Financial Services

What the SBA 504 Loan?
The SBA 504 Loan is a guaranteed loan amount representing 40% to 30% of a project need, with a bank or third party lender providing 50% of the needed amount, and the customer is responsible for 10% to 20% depending on the circumstances of the loan request. The guaranteed portion of the loan is on a long term, fixed rate with relatively low interest.

Who is eligible for a 504 Loan?
To be eligible for a 504 Loan you must be a for-profit corporation, partnership or proprietorship that meets the following small business size standards- net worth of less than $15 million, and average net profit after tax of less than $5 million averaged over two years. In addition, the small business applicant must be the user of the fixed assets being financed. Ineligible businesses are passive income companies, real estate companies, financial institutions, and non-profit businesses.

What can 504 Loan funds be used for?
Proceeds can be used to purchase of land, building, machinery and equipment, for land improvements, renovation or major addition to existing buildings, and leasehold improvements.

What about collateral?
SBA 504 loans are typically secured by a lien on fixed assets acquired with loan proceeds to reasonably assure loan repayment. The SBA's lien is subordinate to the private lender's position. In addition, the SBA requires personal guarantee(s) of the principal(s) whom own 20% of the business.

Can Start-up businesses use the SBA 504 Loan Program?
The SBA 504 Loan Program is primarily designed to assist healthy, expanding businesses that have been in operation for more than two years. The following credit requirements apply to such businesses: existing cash flow from business operations greater than debt service needed to pay both existing debt and debt resulting from the proposed loan, and strong management.

In certain instances, the SBA 504 Loan Program may also be used to finance start-up businesses (i.e. those in operation less than two years). However, such businesses must demonstrate the following: qualified management with industry related work experience, access to an adequate amount of working capital, and minimum 15% equity contribution. Projects involving a limited or single purpose building require a minimum equity contribution of 15% for businesses in operation more than two years and 20% for businesses in operation two years or less.

Any other requirements?
Generally, the SBA requires a project to create or retain one new job for each $65,000 of debenture or $100,000 for manufacturing. However, projects with a high community impact and low direct job impact may be considered when achieving one of several Public Policy Goals of the SBA.

What is our service area?
We provide guaranteed loans to South Carolina businesses. We also assist with other finance products in South Carolina as well as nationwide.

Who are we?
We are a Certified Development Corporation (CDC) specializing in the SBA 504 Loan Program. We also assist our clients with placing loan requests that do not fit the 504 Loan Program with partners who can provide the necessary funding.

Provident Business Financial Services - 3937 Sunset Blvd., Suite D - West Columbia, SC 29169 - 803-791-0071
www.providentbfs.com

Sample SBA Grow Program Costs for Restaurant

Use of Project Proceeds	Dollar Amount
(1) Purchase Land	$2,101,250.00
(2) Purchase Land and Building	$0.00
(3) Construction/Remodeling (new building L/H imp., etc.)	$2,709,073.00
(4) Purchase/Install Equipment (includes furniture, if any)	$0.00
(5) Purchase/Install Fixtures	$720,927.00
(6) Debt Refinancing	$0.00
(7) Professional Fees (appraiser, architect, legal, etc.)	$0.00
(8) Other Expenses (eligible business expenses related to Jobs Act refinancing, construction contingencies, interim interest)	$218,750.00
(9) Total Project Costs (Not including 504-related fees)	$5,750,000.00

Sources of Funds	*Dollar Amount*	*% Project Cost*	*Maturity*	*Interest Rate*	*Lien Position*
(1) Net Debenture	$2,012,500.00	35.00%	20		2
(2) Third Party Lender*	$2,875,000.00	50.00%	10	5.5%	1
(3) Other Financing (Specify):	n/a	n/a %	n/a	n/a %	n/a
(4) Borrower Contribution	$862,500.00	15.00%		%	
(5) Total Project Financing	$5,750,000.00	100.00%			

bing maps

FOREST HILLS, SC

Data from: Wikipedia · Freebase