

CFPB Readiness Series: Compliant Vendor Management Overview

Legal Disclaimer

This information is not intended to be legal advice and may not be used as legal advice. Legal advice must be tailored to the specific circumstances of each case. Every effort has been made to assure that this information is up-to-date as of the date of publication. It is not intended to be a full and exhaustive explanation of the law in any area, nor should it be used to replace the advice of your own legal counsel.



Who is KirkpatrickPrice?

KirkpatrickPrice is a licensed CPA firm, providing assurance services to over 200 clients in more than 40 states, Canada, Asia and Europe. The firm has over 10 years of experience in information assurance by performing assessments, audits, and tests that strengthen information security, and compliance controls.



Welcome

Todd Stephenson is an Information Security Specialist helping collection agencies and law firms prepare for a CFPB examination.

- Certified Information Systems Auditor (CISA)
- Information Security Specialist
- Over four years working with the ARM industry



What's Changed?

- In the past:
 - Vendor compliance managed contractually
 - Compliance risk/responsibility was transferred
 - Compliance activity kept at arms length



What's Changed?

Now:

- Full chain of custody
- The CFPB expects you to "oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law..."
- "Effective Process"
- CFPB Bulletin 2012-03 dated April 13, 2012



Who's Responsible for What?

- If you have "any person (i.e. service provider) that provides a
 material service to a covered person (i.e. you) in connection
 with the offering or provision by such covered person of a
 consumer financial product or service" then you are
 responsible for their compliance to all relevant CFPB
 requirements.
- The service provider is also responsible to the CFPB.
- No one gets a free pass Its both!
- "The CFPB's exercise of its supervisory and enforcement authority will closely reflect this orientation and emphasis."



Welcome

Jessie Skibbe is a Certified Credit and Collections Compliance Officer & former Chief Compliance Officer with 10 years of ARM industry experience. A recent addition to the KirkpatrickPrice team, she is focused on assisting the ARM Industry in meeting regulatory compliance & information security objectives.

- Certified Credit & Collections Compliance Officer (CCCO)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)



Vendor Compliance Managment

- 5 Core Components
 - Risk Assessment
 - Due Diligence in Onboarding
 - Written Contractual Requirements
 - Ongoing Monitoring and Audit
 - Termination



Before you Begin

- Risk Assessment
 - Evaluate the risk associated with the outsourced function.
 - Determine vendor types & areas of risk to consider
 - Vendors performing consumer facing activities
 - Vendor receiving & storing confidential information
 - Vendors requiring unattended access



- Risk Assessment Policy & Procedure
 - Requires the review of the dependency of the function
 - Review of applicable federal and state law(s) associated with the function
 - Defined frequency



- Risk Assessment Template or Worksheet
 - Evaluation of estimated account volume
 - Evaluation of the data elements required to perform the services
 - Information Security Assessment
 - Business Continuity Plan
 - Insurance Coverage
 - Is the use of subcontractors required to perform the services



- Due Diligence in Onboarding
 - Policy listing the requirement
 - Procedure detailing:
 - Responsibility for performing a checklist of functions
 - Formal evaluation of risk and management sign off
 - Templates



- Due Diligence in Onboarding
 - Policy and Procedure
 - RFP or Questionnaire is used to gather information for utilization in the risk assessment process.
 - Requirement for formal risk assessment and acceptance of risk by executive management
 - Corresponds with the contract review stage
 - Corresponds to the monitoring and audit phase



- Written Contractual Requirements
 - Policy, Procedure & Checklists
 - Clear expectations about compliance with applicable federal and state consumer financial protection laws.
 - Clear definition of each party's responsibilities for information security and privacy of consumer data including maintaining fully documented information security policies and procedures.



- Written Contractual Requirements
 - Policy, Procedure & Checklists
 - The third party's responsibility to conduct employee background checks for all employees
 - The third party's responsibility to conduct adequate employee training. Training on policies, procedures, applicable state and federal consumer financial laws and information security awareness training is required.
 - The third party's responsibility to notify you upon any suspected data breach.



KirkpatrickPrice

- Written Contractual Requirements
 - Policy, Procedure and Checklists
 - The third party's responsibility to obtain permission from you prior to sharing confidential consumer data with any other entity.
 - The right for you to terminate the contract upon reasonable notice and without penalty.
 - Instructions for data destruction if applicable.



- Ongoing Monitoring and Audit
 - Policy and Procedure
 - Define the requirement for monitoring and audit
 - Define the responsibility for the function
 - Define the audit report requirements
 - What to Monitor
 - Telephone Calls
 - Employee Training
 - Consumer Complaints



KirkpatrickPrice

Prepare for Audit

- Retain copies of formal risk assessments
- Perform a review of your vendor contracts now to ensure the required components are met. Have them readily available.
- Retain copies of contract review checklists
- Retain copies of monitoring efforts and audits performed
- Ensure retention period match with documented policy and procedure.



- Termination
 - Policy and Procedure
 - Define the process of terminating a relationship to tie up loose ends.
 - Destruction of the data
 - Cancellation of the contract
 - Extension of Non Disclosure Agreements if applicable.



Thank you for attending our Webinar

Q & A

For further information contact: Todd Stephenson

t.stephenson@kirkpatrickprice.com

800.977.3154 Ext. 202



KirkpatrickPrice Services

- Compliance Management System
 - Program development and consulting
 - Policy & procedure drafting
 - Risk assessment guidance
 - Internal audit plan development
 - CFPB Readiness Audit
- Information Security Audit
 - Guidance and audit services:
 - PCI DSS 3.0
 - SSAE 16
 - SOC 2
 - FISMA
 - ISO 27001 / 27002



Coming up Next

CFPB Readiness Series: Complaint Resolution and Tracking

When: September 24th

The CFPB Examination Procedures for Debt Collection indicates a review of "the comprehensiveness of systems, procedures and/or flowcharts for capturing, logging, tracking, handling, and reporting disputes and/or complaints and their resolutions" will be performed. Will you be ready?

