



The New Normal- **Taking Responsibility for** **Your Vendors**

April 16, 2013 | Richard P. Eckman, Jeffrey G. Matthews

The New Normal- Taking Responsibility for Your Vendors

Hit the 'Escape'
key to return to
the normal view.

April 16, 2013 | Richard P. Eckman, Jeffrey G. Matthews

CRA Charles River
Associates

Pepper Hamilton LLP
Attorneys at Law

Click this icon to
view the slide in full
screen mode.



Feel free to submit text questions throughout the webinar

The New Normal- Taking Responsibility for Your Vendors

April 16, 2013 | Richard P. Eckman, Jeffrey G. Matthews

CRA Charles River
Associates

Pepper Hamilton LLP
Attorneys at Law

The New Normal- Taking Responsibility for Your Vendors



April 16, 2013 | Richard P. Eckman, Jeffrey G. Matthews

CRA Charles River
Associates

**Click the printer icon
to download/print
the slides.**

Pepper Hamilton LLP
Attorneys at Law

Connect with Pepper

Interested in learning more about the latest developments in financial services reform?

- Visit our Dodd-Frank Act and Financial Services Reform Resource Center at www.pepperlaw.com
- Visit the Financial Services Group's "Publications" page at www.pepperlaw.com
- Like us on Facebook
- View us on YouTube:
<http://www.youtube.com/user/PepperHamiltonLaw>
- Listen to us at www.pepperpodcasts.com
- Follow us on twitter [@Pepper_Law](https://twitter.com/Pepper_Law)





We will be starting momentarily...



Listen to the audio portion of today's webinar by dialing:

North America: +1.866.322.1348

International: +1.706.679.5933

Audio Conference ID: # 36529735



If you experience technical difficulties, hit *0 on your telephone keypad and an operator will assist you.

Or you can dial:

For Web Support:

+1.877.812.4520 or
+1.706.645.8758

For Audio Support:

+1.800.374.2440 or
+1.706.645.6500

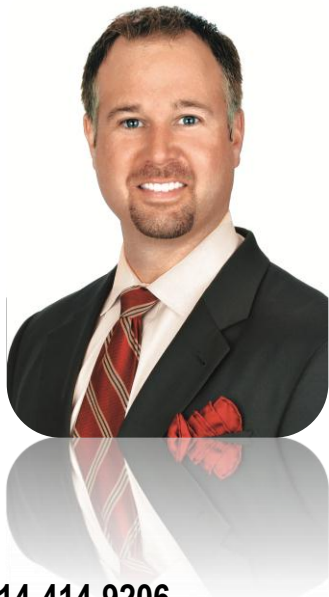
Speaker: Richard P. Eckman



302.777.6560
eckmanr@pepperlaw.com

- Partner in the Wilmington office of Pepper Hamilton LLP
- Finance and transactional lawyer and chairs the firm's Financial Services Practice Group, which includes over 40 lawyers practicing in the areas of investment management, commercial and consumer financial services, public finance and affordable housing
- Transactional practice focuses on representing financial institutions, corporations and other entities in complex financing transactions, including mergers and acquisitions, asset securitizations and other lending and venture transactions.

Speaker: Jeffrey G. Matthews



214-414-9206
jmatthews@crai.com

- Vice president in Financial Accounting & Valuation Practice at Charles River Associates
- Significant experience in compliance matters, financial investigations, forensic accounting, and litigation support. Mr. Matthews has spent many years practicing for Big Four accounting firms, state, local, and federal governmental bodies.
- Has investigated and provided oversight for investigations of federal and state criminal violations, including the implementation of compliance and anti-fraud programs. He has also calculated damages in various disputes, ranging from breach of contract to theft of trade secrets.

Introduction to Third-Party Vendors



- Financial institutions are increasingly relying on third parties to perform product functions
 - Third Party Functions:
 - New to the industry, and/or
 - Traditionally performed by the institutions themselves
 - Benefits:
 - Cost considerations, and
 - Additional areas of expertise

Introduction to Third Party Vendors



- Along with the benefits of vendor relationships come enhanced responsibilities:
 - Must monitor vendors to ensure that they comply with federal and state consumer financial laws
 - Use of vendors does not shield financial institutions from financial responsibility for a vendor's action
 - Financial institutions are solely responsible to regulators for vendors' actions to the same extent as if the actions were taken by the institutions themselves

Regulatory Guidance on Vendors



- FDIC Guidance on Payment Processors
 - Issued Financial Institution Letter on January 31, 2012
 - Letter discusses potential risks, risk mitigation, due diligence, underwriting and ongoing monitoring in the context of payment processors
 - Provides a warning that financial institutions that fail to adequately manage payment processor relationships may be viewed as facilitating these parties' fraudulent or unlawful activity

Regulatory Guidance on Vendors



- FDIC Guidance on Payment Processors (cont.)
 - Risk profiles of payment processors can vary significantly
 - Institutions must look for indicia of fraudulent activity:
 - Deal with telemarketing and online merchants;
 - Use more than one financial institution to process merchant client payments;
 - Solicit business relationships with troubled financial institutions; and
 - Have high levels of consumer complaints, returns or charge-backs.

Regulatory Guidance on Vendors



- CFPB Guidance on Service Providers
 - Bulletin issued April 13, 2012
 - Provided guidance on compliance for banks' and nonbanks' relationships with service providers
 - Clarified that service providers are subject to the CFPB's supervisory and enforcement authority, which includes on-site examination of operations and authority to police unfair, deceptive or abusive acts or practices

Regulatory Guidance on Vendors



- CFPB Guidance on Service Providers (cont.)
 - Consumer financial law violations by service providers can result in legal responsibility for bank or nonbank
 - To avoid being held responsible for the actions of service providers, banks and nonbanks must have an effective process for managing risks:
 - Due diligence on provider's compliance capabilities;
 - Review servicer's policies and procedures;
 - Establish internal controls and ongoing monitoring; and
 - Take prompt action in response to any violations.

Regulatory Guidance on Vendors



- CFPB Guidance on Marketing of Credit Card Add-ons
 - Bulletin issued July 18, 2012
 - Emphasizes steps that institutions must take to ensure that they market and sell add-on products lawfully
 - Examples of violations include:
 - Failing to adequately disclose terms and conditions;
 - Enrolling consumer in programs without consent;
 - Billing for services not performed; and
 - Using misleading marketing and sales practices.

Regulatory Guidance on Vendors



- CFPB Guidance on Marketing of Credit Card Add-ons (cont.)
 - Financial institutions must:
 - Ensure that all marketing materials reflect the actual terms and conditions of products;
 - Structure employee compensation programs so as to not create incentives to provide inaccurate product information;
 - Review scripts and manuals used by telemarketing and customer service centers for compliance with laws and regulations.

Vendor-Related Enforcement Actions



- Capital One Bank (U.S.A.), N.A.
 - CFPB's first public enforcement action announced July 18, 2012
 - Found that Capital One's vendors utilized deceptive marketing tactics to sell credit card add-ons
 - Add-ons included: payment protection, credit monitoring and access to credit specialists
 - Consumers were: misled about benefits, deceived about products' nature, misinformed about costs and enrolled without consent.
 - Capital One forced to pay \$140 million to consumers and a \$25 million civil penalty.

Vendor-Related Enforcement Actions



- Discover Bank
 - CFPB joint enforcement action with FDIC on September 24, 2012
 - Similar to Capital One action, deceptive telemarketing and sales tactics used to mislead consumers into paying for credit card add-on products
 - Telemarketing scripts contained misleading language and language that downplayed key terms and conditions
 - Discover forced to institute changes to its telemarketing practices, pay \$200 million in restitution to consumers and pay \$14 million civil penalty

Vendor-Related Enforcement Actions



- American Express
 - CFPB enforcement action completed October 1, 2012
 - Violations uncovered in subsidiaries during routine examinations
 - Violations at every stage of the consumer experience:
 - Deceived and misled consumers;
 - Charged unlawful late fees;
 - Unlawfully discriminated on the basis of age; and
 - Failed to report disputes to reporting agencies.
 - American Express forced to repay \$85 million to consumers and a civil penalty of \$27.5 million

Vendor-Related Enforcement Actions



- First Bank of Delaware (FBOD)
 - FDIC action announced November 19, 2012 for violations of Bank Secrecy Act and anti-money laundering laws and regulations
 - FBOD failed to adequately oversee third-party payment processor relationships and related products and services
 - As a result, FBOD originated withdrawal transactions on behalf of fraudulent merchants and caused money to be taken from accounts based on fraudulent authorizations
 - Forced to pay \$15 million to U.S. Treasury and \$500,000 for consumer claims



Third Party Risk

April, 2013

CRA Charles River
Associates

Third Party Risk

- The CFPB is clear
 - The use of third-party relationships does not relinquish responsibility of the board of directors and management for compliance with federal consumer law to avoid consumer harm
- The FDIC takes it further
 - The institution's officials are to have ***a clearly defined system of risk management controls*** that governs the institution's compliance operations, ***including controls over activities conducted by affiliates and third-party vendors***
 - All applicable activities conducted through third-party relationships are evaluated as though activities were performed by the institution itself
 - Resources
 - <http://www.fdic.gov/news/news/financial/2008/fil08044a.html>
 - <http://www.fdic.gov/news/news/financial/2008/fil08044a.html>

Third Party Risk

- The OCC further suggests that the risk management system should reflect the complexity of its third-party activities and the overall level of risk involved
 - Resource
 - <http://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-47.html>
- Each institution's risk profile is unique and requires a tailored risk management approach appropriate for:
 - The scale of its particular third-party relationships
 - The materiality of the risks present
 - The ability of the institution to manage those risk

Third Party Risk

- The FDIC offers a broad definition of third-party service providers

All entities that have entered into a business relationship with the institution, whether the third party is a bank or nonbank, affiliated or not affiliated, regulated or nonregulated, a wholly or partially-owned subsidiary, or a domestic or foreign institution.

- Organizations must use their institution knowledge to determine whether the relationship is “significant”

Third Party Risk

- The FDIC suggests that, among other things, factors such as the following could be used to determine whether the relationship is “significant”:
 - Involves new activities
 - Has material effect on the institution’s revenues or expenses
 - The third party performs critical functions
 - Stores or has access to sensitive customer data
- Studies show an organization may also analyze:
 - Whether the service provider delivers customer facing products or services
 - How much reliance is being placed on the service provider
 - The difficulty in monitoring/overseeing the operations of the service provider

Third Party Risk


- The CFPB expects, at a minimum, the following steps in addressing risks:
 1. Conducting due diligence to verify that the service provider understands and is capable of complying with federal consumer laws
 2. Requesting and reviewing the services providers policies, procedures, internal controls and training materials to ensure that the provider conducts appropriate training and oversight of employees or agents that have consumer contact or compliance responsibilities
 3. Including in the contract clear expectations about compliance
 4. **Establishing internal controls and on-going monitoring to determine whether the service provider is complying with federal consumer financial law**
 5. Take prompt action to address problems

Third Party Risk




- Establishing internal controls and on-going monitoring
 1. Identify and risk rank service providers
 2. Perform risk assessment
 3. Due diligence
 4. Contract review and assessment
 5. Performance monitoring


Third Party Risk

- 
- Establishing internal controls and on-going monitoring
 1. Identify and risk rank service providers
 - a) Determine whether the vendor is a high, medium or low risk, based on **YOUR** criteria
 - b) Document rationale for risk ranking
 - c) If medium or high, then perform the review


Third Party Risk

- 
- Establishing internal controls and on-going monitoring
 - 2. Perform risk assessment—identify the risks
 - a) Compliance risk: Risk arising from violation of laws
 - b) Strategic risk: Risk arising from business decisions
 - c) Transactional risk: Risk arising from problems with the service or product delivery—can you deliver
 - d) Operational risk: Risk arising from inadequate or failed internal processes
 - e) Credit risk: Risk arising from creditors or impact from failed funding
 - f) Reputation risk: Risk arising from public opinion
 - g) Fraud risks: Risk of fraud and misconduct—all encompassing
 - h) Country risk/geographical risk/other

Third Party Risk

- 
- Establishing internal controls and on-going monitoring
 3. Due diligence—ideally before a contract is entered
 - a) Audited financial statements
 - b) Significant issues, complaints, lawsuits
 - c) Qualifications and experience of those significant to the vendor's operations and yours
 - d) Their use of third parties, contractors or others

Third Party Risk

- 
- Establishing internal controls and on-going monitoring
 - 4. Contract review and assessment
 - a) Are contracts reviewed by attorneys and approved by the board?
 - Is that process documented?
 - b) Are there clearly defined performance objectives and deliverables?
 - If not, what will you audit?
 - c) What checklist is followed in auditing the contract language?
 - This is different by service

Third Party Risk



- Establishing internal controls and on-going monitoring
 - 5. Performance monitoring—before launching a third-party audit, determine:
 - a) Whether you have sufficient and qualified resources to do so
 - b) Whether there have been previous audits and/or unresolved issues
 - c) How funds leave your organization and reach theirs
 - d) Whether they have provided you with sufficient documentation to compile a work plan

Third Party Risk

- Prior to documenting issues, discuss with counsel and determine:
 - Risks of documenting versus not documenting
 - Intended and probable audiences
 - Are recommendations reasonably achievable?
 - Your responsibility in their remediation

Third Party Risk

- We can learn through CFPB, FDIC, and FTC sanctions, yet the most telling revelation may come from the DOJ and their position on FCPA compliance and compliance programs in general. In February 2013, a principal deputy chief and the department head warned that:
 - Robust corporate compliance programs can be used by companies to prevent prosecution, yet
 - Many companies have not put “muscle behind the programs”
 - Compliance is only one component, but companies creating basic, “cookie-cutter” compliance programs will not be given much weight

Questions & Answers



Thank You!



Richard P. Eckman
302.777.6560
eckmanr@pepperlaw.com



Jeffrey G. Matthews
214-414-9206
jmatthews@crai.com

For more information visit

**www.pepperlaw.com
or
www.crai.com**

