2018 NACUSAC Conference
Louisville, Kentucky

MANAGING THE RISKS ASSOCIATED WITH THIRD-PARTY VENDOR RELATIONSHIPS

Thursday; June 14, 2018
Concurrent Sessions:
10:30am & 1:20pm

Presenter:
Mike Richards, CPA
Richards & Associates, CPAs

Significant Vendor Breaches

- **Target 2013 Cyber Attack**
  70 million customers
  The attackers gained access through a third-party vendor
- **Equifax Data Breach**
  143 million people, nearly half the population of the United States
- **Facebook – Cambridge Analytical Data Scandal**
  87 million members
  Information used for political advertising
- **Indirect Lending / Military Lending Act**
- **NCUA Examiner Caused Data Breach** for credit union

2

Retailers Hacked in 2017

- Best Buy
- Delta Airlines
- Forever 21
- Kmart
- Lord & Taylor
- Panera Bread
- SAKs Fifth Avenue
- Sears
- Sonic
- Under Armour
- Whole Foods Market

3

Common Types of Third-Party Vendor Relationships

- **Third-party product providers:** mortgage brokers, automobile dealers, and credit card providers
- **Loan servicing providers:** debt collection, loss mitigation, and foreclosure activities
- **Disclosure preparers:** disclosure preparation software and third-party documentation preparers
- **Technology providers:** software vendors and website developers
- **Providers of outsourced compliance functions:** companies that provide compliance audits, fair lending reviews, and compliance monitoring activities

4

Risks Associated with Third-Party Vendors

- **Compliance risks:** violations of laws, rules or regulations, or non-compliance with policies and procedures
- **Reputation risks:** dissatisfied members or violations of law or regulations that lead to public enforcement actions
- **Operational risks:** losses from failed processes or systems or losses of data that result in privacy issues
- **Transaction risks:** problems with service or delivery
- **Credit risks:** inability of a third party to meet its contractual obligations

5

Best Practices for Managing Third Party Relationships

- Due Diligence
- Risk Assessment
- Clear Contractual Expectations
- Monitoring Program

6

Best Practices – Due Diligence

- **Due Diligence.** Credit unions should have a successful due diligence process which includes:
  - *Obtaining references viewing financial records of the vendor*
  - *Ensuring that the vendor has backup systems, and continuity and contingency plans*
  - *Researching the background, qualifications, and reputation of the vendor's principals and their overall reputation*
  - *Determining whether or not lawsuits may have been filed against the vendor*

7

Best Practices – Risk Assessment

- **Risk Assessment.** A detailed risk assessment should be developed based on the initial due diligence and should be provided to senior management and to the board of directors. The risk assessment should include all factors including:
  - *Compliance*
  - *Reputation risk*
  - *Operational risks*
  - *Credit and transaction risks*

8

Best Practices – Clear Contractual Expectations

- **Clear Contractual Expectations.** Some issues to undertake as part of the contract review include but are not limited to the following:
  - *The scope of outsourced services*
  - *The procedures a vendor must follow*
  - *The credit union's level of expectation*
  - *The credit union's approval of a vendor's use of subcontractors*
  - *The credit union's right to conduct audits or request third-party reviews*
  - *The confidentiality of data*
  - *The vendor warranties, liability, and disclaimers*
  - *Dispute resolution mechanisms*
  - *Default and termination provisions*
  - *Complaint or dispute process*

9

Best Practices – Monitoring Program

- **Monitoring Program.** The last part of best practices is a comprehensive monitoring program.
  - *Too often a vendor contract is placed in the file and only reviewed after it is "automatically renewed" or after there is a dispute.*
  - *There should be periodic/risk-based monitoring so that the frequency and type of monitoring would depend on each vendor and the assignments of the vendor.*

10

Privacy Issues under Gramm-Leach-Bliley Act (GLBA)

GLBA privacy considerations affect consumers in the following ways:

- Financial institutions are required to:
  - *Ensure the security and confidentiality of customer information*
  - *Protect against any anticipated threats or hazards to the security or integrity of such information*
  - *Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.*

11

Privacy Issues under Gramm-Leach-Bliley Act (GLBA)
- continued

- The law requires these institutions to explain how they use and share personal information. The law also allows consumers to stop or "opt out" of certain information sharing.
- The law requires that financial institutions describe how they will protect the confidentiality and security of information.

12

General Data Protection Regulation (GDPR)

- The General Data Protection Regulation (**GDPR**) is a regulation in European Union law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA.
- The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. **GDPR is effective as of May 25, 2018.**
- The GDPR applies to any financial institution that serves even a single EU customer.

13

Best Practices for GDPR

- **Appoint a data protection officer** responsible for:
  - *Educating and training staff about compliance requirements*
  - *Conducting audits and monitoring data privacy compliance*
  - *Coordinating communications to members about how their data is being used, their rights to have it erased, as well as the protective measures the credit union has developed*
- **Map the flow of data**. Credit unions should track and analyze the data sources, data available and with whom they have shared the data.

14

Best Practices for GDPR - *continued*

- **Review existing plans.** It is likely security, disaster recovery, and other identified plans will have to be adjusted to ensure data privacy is addressed within.
- **Keep up to date** on policies and issues that impact data privacy

15

SOC 2 Compliance

- **Service Organization Control Reports – Type 2** (SOC 2) is an auditing procedure that ensures your service providers securely manage your data to protect the interests of your credit union and the privacy of its members.
- For security-conscious businesses, SOC 2 compliance is a minimal requirement when considering a Software as a Service provider.

16

About the Presenter
Michael E. Richards, CPA

Mike Richards has held the position of CEO of Richards & Associates, CPAs since 1978. He joined the firm in 1973 after earning a bachelors degree in business administration from the California State University at Los Angeles and becoming a Certified Public Accountant. In addition to introducing many new services, he is responsible for quality control of all professional services offered by the firm.

RICHARDS & ASSOCIATES, CPAs
21520 Yorba Linda Blvd, #G-516
Yorba Linda, CA 92887
mrichards@richardscpas.com

17