A TIMELY INFORMATION AND IDEAS STATEMENT

FINANCIAL INSTITUTIONS INSIGHTS

Delivering bimonthly information critical to community banking professionals while tackling issues ranging from IT security to regulatory compliance to operational improvements

In this issue:

For full detail of the included articles or for additional articles, please visit: http://rsmus.com/our-insights/newsletters/financial-institutions-insights.html

Dodd-Frank, shifting demographics drive a new emphasis on diversity

Why financial institutions should focus on inclusion and compliance now

One aspect of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) that has attracted relatively little attention until now is Dodd-Frank section 342, which addresses the diversity policies and practices of several federal agencies and of the companies that those agencies regulate or with which they contract. While there so far has been little enforcement or compliance action related to section 342, there has already been some reporting on diversity among financial institutions by the Government Accountability Office (GAO), and many expect increased attention from regulators soon.

Home Mortgage Disclosure Act (HMDA) requires financial institutions to report data collection on mortgage applications received from individuals acquiring a home. The regulation change increases the amount of data to be reported and will allow regulators to determine if disparate treatment exists in the lending practices of financial institutions. In 2016, financial institutions considered this their biggest risk and concern, exceeding even the Truth in Lending Disclosure (TRID). Such reporting of data, if required by section 342, could lead to the same scrutiny by a regulator. Regulated entities are only required to voluntarily submit section 342 data. If such data is required to be reported, the door will be open for more scrutiny by regulators.

LaPorte CPAs & BUSINESS ADVISORS

RSM US Alliance | RSM

Potential regulatory attention is not the only reason for financial institutions to pay attention to sections 342 and HMDA. Shifting demographics mean that banks need to focus increasingly on women and minorities in both hiring and lending practices if they wish to compete in evolving talent and lending marketplaces.

Though compliance to date has been voluntary, lawmakers are taking note of lackluster progress since Dodd-Frank was enacted. In response, regulators are considering new frameworks to review and assess practices and outcomes.

How section 342 works

Section 342 calls for the establishment of Offices of Minority and Women Inclusion (OMWIs) at 20 different government agencies:

1. Department of the Treasury (DOT)
2. Consumer Financial Protection Bureau (CFPB)
3. Federal Deposit Insurance Corporation (FDIC)
4. Federal Housing Finance Organization (FHFO)
5. National Credit Union Administration (NCUA)
6. Office of the Controller of the Currency (OCC)
7. Securities and Exchange Commission (SEC)
8. Board of Governors of the Federal Reserve (the Fed)
9. 12 regional Fed banks

The OMWIs are tasked with oversight of all agency matters relating to diversity in management, employment and business activities involving:

- The employment practices of the agency
- The diversity policies and practices of the entities with which the agencies contract
- The diversity policies and practices of the entities the agency regulates

Section 342 further mandates that the OMWIs develop and implement standards and procedures to ensure the fair inclusion of minorities, women, and minority- and women-owned businesses in all business and activity of each agency. It also grants the OMWIs the power to refer contractors to the agency administrator if the OMWI determines a contractor has not made good-faith diversity efforts. Financial entities subject to the oversight by OMWIs include:

- Financial institutions
- Investment banking firms
- Mortgage banking firms
- Asset management firms
- Broker/dealers
- Financial services entities
- Underwriters
- Accountants
- Investment consultants
- Law firms

To read the complete article, go to: http://rsmus.com/our-insights/newsletters/financial-institutions-insights/dodd-frank-shifting-demographics-drive-a-new-emphasis-on.html

Effective cybersecurity means more than protecting your perimeter

Coordinated response to detect and contain breaches is vital

Too many financial institutions focus the bulk of their cybersecurity efforts on preventing infiltration of their systems. Which isn't to say that preventing penetration should not be a key security focus; it should. But being overly reliant on your perimeter defenses doesn't address the full threat. According to Trustwave Global Security Reports, Verizon Data Breach Investigations Reports, Symantec Internet Security Threat Reports, and Cisco Annual Security Reports, only 1–2 percent of breaches are detected in the first 24 hours, and over 14 percent are not detected for two years or more. In fact, in 80 percent of cases, financial institutions didn't even discover breaches themselves; instead they learned of them from third parties. When you consider the volume and sophistication of today's cyberthreats, and the fact that that 64 percent of breaches result in data loss within the first 24 hours, the need for your financial institution to be ready to uncover, contain and address attacks that get past your first line of defense is clear.

Cyberattacks generally are carried out in four stages:

- Infiltration (breaching your perimeter defenses)
- Propagation (spreading through your systems to gain access to targeted data)
- Aggregation (gathering targeted data)
- Exfiltration (transferring data out of your system)

Looking beyond your perimeter

Your controls need to be deployed throughout your environment in order to impede cybercriminals at every stage of the breach cycle. And you need to break down silos and communication barriers that prevent various parts of your security apparatus from coordinating their response to attacks. Focus on prevention, yes. But also plan for your prevention to fail.

Where to focus beyond the perimeter? At the propagation stage of an attack, you need three effective sets of controls:

- Network controls, including access control lists (ACLs) which selectively permit or deny traffic to specific areas, intrusion prevention systems (IPSs) which detect and drop malicious traffic and block further traffic from those sources, and network access controls (NACs) which control access to various areas of your network based both on appropriate configuration of the requesting device (such as updated anti-virus software) and on the role of the requesting party
- Domain controls, such as secure password storage and effective group policies
- System and application controls, such as endpoint security, vulnerability management and application security

To read the complete article, go to: http://rsmus.com/our-insights/newsletters/financial-institutions-insights/effective-cybersecurity-for-financial-institutions-means-more-th.html

Build relationships with digital banking
3 steps to develop a digital banking road map

Strong customer relationships are fundamental to the success of all financial institutions. Community banks and credit unions have made personal service a cornerstone of success, and have differentiated themselves from larger competitors through an emphasis on member and customer service. Consumers now have rapidly changing expectations for how they communicate and how they interact with all businesses, and your institution must keep pace with those expectations to engage customers and increase loyalty.

Enhancements in technology, including the ubiquitous access to smartphones, have fundamentally changed how financial institutions must interact with consumers. Digital banking options span a wide range of delivery channels, products and services that can be deployed. What is the right strategy for your organization? Below are three steps that you can take to develop an effective road map for digital banking investment.

Step 1: Identify your goals

It is important to align digital banking initiatives with your strategic plan. Your target market segments, deposit and lending growth goals, and product strategies must be considered when evaluating and prioritizing digital banking options. Self-service capabilities in branches can lower expenses and support expansion to more markets.

In addition, applications supported through online and mobile banking channels can drive loan and deposit growth. Online functionality support tailored to small businesses can improve your ability to acquire and retain these profitable relationships and garner additional fee income. Developing a digital banking road map that supports your business goals will serve as the basis for prioritizing future investment and managing the implementation of new digital banking services.

To read the complete article, go to: http://rsmus.com/our-insights/newsletters/financial-institutions-insights/Build_relationships_with_digital_banking.html

NCUA supervisory priorities for 2016 raise two key focus areas—BSA compliance, new TILA-RESPA rule are key areas of concern

In its January 2016 letter on supervisory priorities for 2016, the National Credit Union Administration (NCUA) identified six areas of focus for the year:

- Cybersecurity assessment
- Response programs for unauthorized access to member information
- Bank Secrecy Act (BSA) compliance
- Interest rate risk
- TILA-RESPA integrated disclosure rule
- Credit Union Service Organization (CUSO) reporting

While all of these are key concerns for every credit union, our experience shows that two of these issues, BSA compliance and dealing with the Consumer Financial Protection Bureau's new TILA-RESPA integrated disclosure (TRID) rule, bear particular scrutiny.

MSBs, effective risk assessments highlight BSA concerns

Dealing with money service business (MSB) customers and ensuring an effective BSA risk assessment are two BSA areas where credit unions should focus particular attention.

To read the complete article, go to: http://rsmus.com/what-we-do/industries/financial-institutions/credit-unions/ncua-supervisory-priorities-for-2016-raise-two-key-focus-areas.html

The importance of the CIO role: Can you benefit from a virtual CIO?

Financial institutions face growing regulatory responsibilities and shrinking margins, and many are evaluating ways to better manage costs. However, when assessing technology investments, institutions should not lose sight of the importance of the chief information officer (CIO) to help ensure compliance and increase security and efficiency. Even institutions with limited resources require a technology executive to make strategic IT decisions, and in many cases, a virtual CIO is an optimal solution.

The CIO fills many key roles for an institution, serving as a business partner, strategist and innovator. In many cases, a technology disconnect exists with many institutions where key stakeholders are not satisfied with technology, but the IT department does not have an effective plan in place.

A recent study showed that stakeholders are 3.5 times more likely to be highly satisfied with IT if an effective IT strategy is in place.[1] However, 47 percent of business leaders feel that business goals are unsupported by IT and 92 percent of IT departments claim their strategies are less than adequate. Stakeholders and IT both want improved strategic planning and alignment with the business, but many institutions fail to accomplish these goals.

A CIO's role is to eliminate that divide between business executives and IT, developing and implementing an effective technology strategy that aligns with institutional objectives.

Note: For more information on what to look for when selecting an institution's CIO, read RSM's article Beyond the techie—CIOs must be versatile leaders.

1 "Define an IT strategy and Roadmap," Info-Tech Research Group, www.infotech.com

To read the complete article, go to: http://rsmus.com/what-we-do/services/technology/infrastructure/managed-services-it-vision/the-importance-of-CIO-role_can-you-benefit-from-a-virtual-CIO.html

For full detail of the included articles or for additional articles, please visit:
http://rsmus.com/our-insights/newsletters/financial-institutions-insights.html

111 Veterans Memorial Blvd., Suite 600
Metairie, LA 70005

Address Service Requested

For additional copies or change of address, contact LaPorte CPAs & Business Advisors. For more information, contact Leslie Paull, at (504) 835-5522 or e-mail her at lpaull@laporte.com. Visit our website at www.laporte.com.

Financial Institutions Insights

November/December 2016

Printed in the U.S.A.

NL-NT-ALL-FS-XX16