Regulatory Compliance News

MOUNTAIN WEST Credit Union Association

October 3, 2014

Compliance News

Integrated Disclosures – Which Forms Should We Use?

Many credit unions are busy with activities to implement the new TILA-RESPA combined disclosure requirements. Some of these activities include working with core data processing vendors, mortgage software systems vendors and forms providers. However, credit unions should not overlook the obvious when getting ready for the change – whether the rule applies to your credit union at all! Many smaller credit unions make only HELOC loans which are not covered under the new rule. Other credit unions, of course, make HELOC loans as well as loans that are covered under the new rule. In either case, credit unions need to be aware that the new combined disclosures can NOT be used for HELOC loans, even after the effective date of the new rule – August 1, 2015. That is, the current forms required under Regulation Z will continue to be used for HELOCS after the effective date of the rule. The CFPB's Small Entity Compliance Guide states that "Creditors originating these types of mortgages [HELOCs] must continue to use, as applicable, the GFE, HUD-1, and Truth-in-Lending disclosures required under current law. In addition, for applications received prior to August 1, 2015 for transactions subject to the new rule and consummated AFTER the effective date, these loans must also use the forms required under current law. You can access the Small Entity Compliance Guide here for more information.

Regulation Z Now Available in Easier-to-Read Format

TILA has been added to eRegulations, our web-based application that makes regulations easier to read and understand. It can be difficult and time consuming to understand how a regulation changes over time. The "compare" feature in the eRegulations tool allows you to compare two versions of a regulation, and see exactly where the regulation has changed.

Source: CFPB

FinCEN Issues Administrative Ruling on the Application of FinCEN Regulations to Currency Transporters, Including Armored Car Services

The Financial Crimes Enforcement Network (FinCEN) issued an administrative ruling on the application of FinCEN regulations to currency transporters, including armored car services. The Ruling discusses the evolution in services that some currency transporters provide and the circumstances under which they must register with FinCEN as money transmitters and comply with the relevant aspects of the Bank Secrecy Act (BSA).

The Ruling contributes to a regulatory initiative by FinCEN to address ongoing concerns about transnational criminal organizations exploiting the lack of transparency in the movement of cash across the U.S./Mexico border via armored car services and other currency transporters as a means to launder their criminal proceeds. Previously, FinCEN issued guidance to currency transporters on the correct and complete way to file the Report of International Transportation of Currency or Monetary Instruments (CMIR) (FIN-2014-G002) and a Geographic Targeting Order (GTO), requiring enhanced BSA reporting at two ports of entry along the U.S./Mexico border.

Source: FinCEN

FFIEC Offers Guidance on Shellshock Computer Bug

The Federal Financial Institutions Examination Council (FFIEC) members are advising financial institutions of a material security vulnerability in the Bourne-again shell (Bash) system software widely used in servers and other computing devices that could allow attackers to access and gain control of operating systems.

Compliance Team

Mark Robey
Sr. VP of Regulatory Affairs
Phone: 800-477-1697, ext. 3327
Direct: 720-479-3327

Melia Heimbuck
Director of Compliance Operations
Phone: 800-477-1697, ext. 3325
Direct: 720-479-3325

Julie Kappenman
Director of Association Compliance Services
Phone: 800-477-1697, ext. 3324
Direct: 720-479-3324

Donna Gibbs
Compliance Coordinator
Phone: 800-477-1697, ext. 3281
Direct: 720-479-3281

infoSight Your Online Compliance Resource

Sectoral Sanctions Identifications List (SSI)

On July 16, 2014, OFAC introduced the Sectoral

The vulnerability, nicknamed "Shellshock," could expose organizations and individuals to potential fraud, financial loss, or access to confidential information.

Bash is a software tool found on many operating systems and is used to translate user instructions and other inputs into machine-readable commands. Financial institutions may have Bash present on a wide array of servers and network devices, including Web servers, email servers and physical security systems. On Sept. 24, security researchers reported the existence of Shellshock in Bash versions 1.14 through 4.3, which have been in use for decades.

The vulnerability potentially allows a remote attacker to run malware, or malicious code, on affected systems. Given the broad use of the Bash software tool, the vulnerability may be present in the computer systems of financial institutions, their members and customers, and those of their third-party providers.

Attackers could use the vulnerability to access and take control of systems, leading to a range of operational risks. These risks may include the loss of confidentiality, integrity, and availability of sensitive customer information and confidential business data. This access could lead to data destruction, disruption of operations and fraud, FFIEC said. (See related story: Security expert: Shellshock could cause 'chaos and mayhem.')

While vendors are working to patch and update their systems, the FFIEC member agencies expect financial institutions to conduct a risk assessment and address the Shellshock vulnerability as part of ongoing information security and incident response plans. FFIEC advices financial institutions to take the following steps, as appropriate:

- Identify all servers, systems, and appliances that use vulnerable versions of Bash and follow appropriate patch management practices, including conducting a vulnerability scan to detect if the patch is installed and testing to ensure a secure and compatable configuration;
- Apply mechanisms to filter malicious traffic to vulnerable services such as appropriate Web application firewall signatures;
- Monitor systems for malicious or anomalous activity and update signatures for intrusion detection and prevention systems;
- Ensure that all third-party service providers are taking appropriate action to identify and mitigate risk and monitor the status of vendors' efforts to address the vulnerability; and
- Review systems to determine if this vulnerability has been exploited and, if necessary, conduct a forensic examination to determine the potential effects of any breach.

The FFIEC is comprised of federal financial institution regulators, including the National Credit Union Administration.

Source: CUNA News Now

NCUA Fall Webinar Series Will Cover Product Pricing, Loan Portfolios and Internal Controls

The National Credit Union Administration will host webinars this fall for credit unions interested in learning more about product pricing, building loan portfolios and improving internal controls.

On Oct. 15, NCUA will host “Product Pricing: Getting it Right,” which will cover how loan size matters to profitability, how to set rates based on internal metrics and how some decisions made “in the name of the member” may be unprofitable.

The Nov. 19 webinar, “Building a Loan Portfolio: Four Keys to Lending,” will discuss loan products, pricing, underwriting and collections.

The Dec. 17 webinar, “Internal Controls,” will cover how to build effective internal controls with a small staff, how to minimize employee dishonesty and how to avoid common internal controls mistakes.

Hosted by staff from NCUA’s Office of Small Credit Union Initiatives, all of the webinars are free and begin at 2 p.m. Eastern. Online registration for the October webinar is now open here. Registration for the November and December webinars are also open; use this link to register. Participants will also use the registration links to log into the webinar. Registrants should allow pop-ups from this website.

Sanctions Identifications List (SSI), in order to identify persons operating in sectors of the Russian Economy identified by the Secretary of the Treasury pursuant to Executive Order 13662. The list includes directives that require U.S. persons to reject certain kinds of transactions with the persons identified on the list. This is a new list, in addition to the already existing Specially Designated Nationals (SDN), Palestinian Liberation Council (PLC), and Foreign Sanctions Evaders (FSE) lists.

Note: The SSI List is not part of the SDN list; however, persons and companies on the SSI list may also appear on the SDN list. Additional instructions will appear on the SDN list for those listed on both lists.

Executive Order 13662 gives two directives regarding persons listed on the SSI list. These directives will determine the course of action to be taken should a U.S. person find a match. These directives will state one of the following actions depending on whether or not the listed party is a person or entity:

- That “the following transactions by U.S. persons or within the United States are hereby prohibited: transacting in, providing financing for, or otherwise dealing in new debt of longer than 90 days maturity or new equity for these persons (listed here), their property, or their interests in property. All other transactions with these persons or involving any property in which one or more of these persons has an interest are permitted, provided such transactions do not otherwise involve property or interests in property of a person blocked pursuant to Executive Orders 13660, 13661, or 13662, or any other sanctions programs implemented by the Office of Foreign Assets Control.” Or
- That “the following transactions by U.S. persons or within the United States are hereby prohibited: transacting in, providing financing for, or otherwise dealing in new debt of longer than 90 days maturity for these persons (listed below), their property, or their interests in property. All other transactions with these persons or involving any property in which one or more of these persons has an interest are permitted, provided such transactions do not otherwise involve property or interests in property of a person blocked pursuant to Executive Orders 13660, 13661, or 13662, or any other sanctions programs implemented by the Office of Foreign Assets Control.

Credit unions should begin checking against this list immediately, and work with vendors to make sure that these names are added to any interdiction software.

Cloud Computing

As the need to address record and information storage demands increases, credit unions continually look for new cost effective methods of processing and storing information. Cloud computing is a

Participants may submit questions in advance at WebinarQuestions@ncua.gov. The subject line of the email should be the title of the webinar. Participants with technical questions about accessing the webinar may email audience.support@on24.com. All webinars will be archived and closed-captioned online here approximately three weeks following the live event.

NCUA's Office of Small Credit Union Initiatives fosters credit union development and the effective delivery of financial services for small credit unions, new credit unions, minority depository institutions and credit unions with a low-income designation.

Source: NCUA

Advocacy Highlight

CUNA Working For Credit Unions on Data Security

The major Home Depot breach and the more recent hit on Jimmy John's sandwich shops serve as reminders of how devastating cyber-attacks can be for credit unions. CUNA and the leagues are pursuing every avenue to ensure that merchants are held responsible for reimbursing credit unions when merchants' security lapses cause situations such as this.

In the aftermath of the Target data breach, CUNA has pressed federal and state lawmakers to enact legislation that would require merchants to bolster their cybersecurity systems and require merchants to reimburse financial institutions for costs incurred when breaches occur in retailers' systems. In fact, CUNA was among the first to knock on Congress' door to demand hearings on this issue and on creating a better data security framework.

Further, CUNA has been consulting with prominent class action attorneys from several law firms on data breach issues, while also helping credit unions reach various class action firms that are investing in this type of litigation. The Target breach resulted in more than 30 cases directly related to financial institutions, with at least 10 credit unions serving as named plaintiffs. On Home Depot, at least two cases involving credit unions have already been filed.

CUNA has also led the way gathering information about the extent of breaches. This information can be shared both with Congress and with class action attorneys that are bringing cases against merchants to demonstrate the extent of the financial harm. After the Target breach, CUNA sent out a request nationwide to credit unions to report how the major beach had affected them financially. All told, credit unions were on the hook for $30.6 million, according to CUNA's estimates, and credit unions reissued roughly 4.6 million credit and debit cards in the aftermath.

CUNA is once again urging credit unions to track the costs they incur as a result of the Home Depot incident. It will soon circulate a survey to collect the following information:

- Number of debit and credit cards affected;
- Costs incurred for card reissuance;
- Costs related to additional staffing, member notification, account monitoring, etc.;
- Changes in call volume;
- Changes in staffing; and
- Any specifically identifiable fraud-related losses.

In addition, CUNA continues to work with groups throughout the financial services industry such as the Payments Security Task Force (PST), the Payments Council, and the Electronic Payments Coalition (EPC) to address data breach issues. The PST is comprised of groups that meet weekly to discuss new security measures; the process of integration; and to create resources for merchants, consumers, and financial institutions.

The Payments Council is made up of a number of financial services trade organizations, including CUNA, and has held a number of meetings over the past few months to discuss the future of payments and cybersecurity efforts.

The EPC, a group of networks, financial services trade associations, and issuers, works together on communications messaging and public affairs advocacy, especially to inform the media and the Hill about key developments in data breaches and other issues.

CUNA Seeks Feedback on NACHA Compliance and Operational Topics Proposed Rule

CUNA is seeking feedback from credit unions through CUNA's Regulatory Call to Action until October 13 regarding a NACHA proposed rule to address certain compliance and technological advancement that can be advantageous to credit unions. This video presentation provides information on the requirements for Cloud Computing and how it impacts your credit union.

CUNA Regulatory Advocacy Report

This week's Regulatory Advocacy Report will bring you up to speed on the following issues:

- CUNA Working For Credit Unions on Data Security
- NCUA's Regulatory Modernization Initiative Turns 3
- GAO Recommends Improvements for CFPB's Privacy & Security Procedures for Data Collections
- Update on the Federal Reserve Banks' "Payment System Improvement" Initiative; CUNA Attends Chicago Fed Payments Symposium
- CUNA Seeks Feedback on NACHA Compliance and Operational Topics Proposed Rule
- Fed Governor Talks Regulatory Relief To Community Banks

Be sure to visit our new Risk-Based Capital blog for the latest from CUNA staff and guest bloggers

2014 Compliance Calendar

September 19
- NACHA Operating Rules Changes

October 13
- Columbus Day – Federal Holiday

October 17
- Master Card Limitation of Liability Change

October 24
- 5300 Call Report Due to NCUA

October 31
- Credit Card Qtrly Agreement Submission Due to CFPB (10,000 or more open credit card accounts)

November 2
- Daylight Savings Time Ends

November 11
- Veterans' Day – Federal Holiday

November 27
- Thanksgiving Day – Federal Holiday

Effective Dates
New and Revised Rules

August 1, 2015~CFPB
TILA-RESPA Integrated Disclosure Rule

December 31, 2015~IRS
"Foreign Account Tax Compliance Act" (FATCA)

operational topics on the ACH network. The proposed changes are characterized as technical amendments and the proposal is similar to proposals issued by NACHA in 2012 and 2013.

Specifically, this proposed rule would amend the following areas of the NACHA Operating Rules: (1) Recrediting Receiver, (2) TEL entries, (3) Clarification of RDFI warranties for Notification of Change, (4) Valid characters for ACH records, and (5) Disclosure requirements for POS entries. NACHA believes these changes would benefit ACH network participants. CUNA is interested in how this proposed rule would affect credit union operations and compliance on the ACH network.

For further details, please visit the NACHA request for comment summary; their proposed modifications to the NACHA Rules; their summary presentation; and their ACH participant survey.

MOUNTAIN WEST Credit Union Association

Training & Events Calendar

October 8

Compliance Networking Council – Casper, Denver & Phoenix – contact Shay Jacobs sjacobs@mwcua.com

October 29

Webinar: Social Media Update: Facebook, LinkedIn, YouTube and Twitter

November 4 – 6

Regulatory Compliance School - Phoenix

Rule

CUNA Comment Calls
Due Dates on Proposed Rules

September 22, 2014~FinCEN
Customer Due Diligence

October 1, 2014~NCUA
Fixed Assets

October 15, 2014~CFPB
Proposed Regulation on HMDA (Reg C)

CUNA Schools and Webinars

October 26 – 29
CUNA Bank Secrecy Act Conference, Las Vegas, NV

October 7
Webinar: ACH Fundamentals

October 16
Webinar: ACH Basics

Please respond to Mark Robey with any questions or concerns regarding content of this newsletter.
Sign up to receive Regulatory Compliance News by sending an email to Donna Gibbs