Regulatory Compliance News

MOUNTAIN WEST Credit Union Association

July 11, 2014

Compliance News

NCUA Issues Letter 14-CU-08

Interagency Guidance on Home Equity Lines of Credit Nearing Their End-of-Draw Period

As home equity lines of credit (HELOCs) approach their end-of-draw period, some borrowers may have difficulty meeting higher payments that result from principal amortization, or in renewing the existing loan. Changes in financial circumstances and declines in property value may limit options for your members.

The below interagency guidance encourages credit unions to work with borrowers where possible, consider sound risk management principles, and minimize risk while meeting the needs of your members.

The risk management principles and approach described in the guidance can help you identify potential exposures, and guide consistent, effective responses to HELOC borrowers who may be unable to meet their contractual obligations. The guidance also addresses appropriate accounting and reporting for HELOCs, as well as appropriate practices for identifying and managing associated risks.

Interagency Guidance on Home Equity Lines of Credit Nearing Their End-of-Draw Period

Source: NCUA

Civil Money Penalties Targeted to 84 Late Filers

The National Credit Union Administration reports that it has identified possible financial penalties against 84 credit unions under its "zero tolerance" policy for credit unions that filed late first-quarter call reports.

The NCUA has only notified late filers of the penalty that may be assessed, but since the process is not complete, no credit union has been 'fined' at this point, the agency emphasizes.

The Northwest Credit Union Association noted in its June 24 *Anthem* newsletter that one of the credit unions being notified is in Oregon and four are in Washington. If the five Northwest credit unions sign consent orders, their penalties will range from $243 to $1,900. The league also notes that the steepest penalty of the possible 84 could exceed $10,000 according to the NCUA, should the credit union choose not sign the consent order.

The NCUA told *News Now* that it soon will be releasing national data related to the civil money penalties.

In May, the NCUA anticipated it would begin the process of assessing civil money penalties from 104 credit unions that filed 2014 first-quarter call reports late (*News Now* May 23).

The regulator makes exceptions to its "zero tolerance" policy for credit unions able to document certain filing hardships, including a breakdown in the credit union's core operating system, a natural disaster taking place in the credit union's community, or the incapacitation of a key employee who would be responsible for filing the report.

If a credit union encountered a problem and contacted the agency help desk to report an issue with filing the report, the NCUA generally took this into account and waived the penalties, an agency spokesman told the NWCUA.

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

Suspicious Activity Reports

An effective Bank Secrecy Act compliance program will be able to recognize that certain transactions are suspicious in nature. A credit union must know its members to be able to make an informed decision as to the suspicious nature of a particular transaction and whether to file a Suspicious Activity Report (SAR).

SARs can be filed on any transaction occurring in any department. SARs must be filed no later than 30 days after the date of initial detection of facts that may constitute a basis for filing a SAR.

Remember that the Financial Crimes Enforcement Network (FinCEN) has mandated that the SAR reports (and Currency Transaction Reports) be filed electronically through the BSA E-Filing System.

For the resources your credit union needs to remain in compliance, visit the Suspicious

Any fines collected by the NCUA will be remitted to the U.S. Treasury Department and do not supplement the agency budget.

The NWCUA says it is asking the NCUA to better address issues with online filing.

"We're asking the NCUA to remind credit unions a couple of days before the reports are due that the filing deadline is approaching," said John Trull, director of the regulatory advocacy. "Furthermore, we are advocating for technical improvements to the system that would notify credit unions immediately upon hitting the submit button if there is an issue, or to confirm the report was received."

If credit unions provide evidence of previous on-time filing, Trull noted, they may be able to appeal the fine with the NCUA's Office of Examination and Insurance. If the cost of the fine would materially harm the financial health of the credit union, Trull said, that would be another circumstance for the regulator to consider.

Since January, an NCUA spokesman noted, credit unions were notified many times of the policy, and warning letters were sent to credit unions that filed their December 2013 reports late. The regulator also posted articles in the *NCUA Report*.

Overall, the zero tolerance policy is close to having its intended effect, with 98.4% of credit unions filing on time--the highest percentage since online filing began, according to the NCUA.

Source: CUNA News Now

GAO: Virtual Currencies Raise Consumer, Investor Protection Issues

Virtual currencies, while heralded by some as part of an innovative new financial system, bring with them a host of challenges and risks to financial institutions, consumers and law enforcement. The U.S. Government Accountability Office (GAO) has released a report on virtual currencies, outlining several of these issues, and urging the Consumer Financial Protection Bureau to take an active role in facing consumer issues that might arise with its use.

Virtual currencies are digital representations of value that are not government-issued, and systems operate over the Internet and use computer protocols and encryption to conduct and verify transactions. Some can be used to buy real goods and services and exchanged for dollars or other currencies.

But these currencies have also been associated with illicit activity and security breaches, which raises possible regulatory, law enforcement, and consumer protection issues.

Several of the main issues outlined in the June 26 GAO report are:

- Virtual currency systems may provide anonymity over traditional payment systems and can lack a central intermediary to maintain transaction information. This can lead to difficulties in detecting money laundering and other crimes;
- Many virtual currency systems can be accessed globally to make payments and transfer funds across borders. Consequently, law enforcement agencies investigating crimes that involving these currencies have to rely upon cooperation from international partners who may operate under different regulatory and legal principles; and
- The emergence of virtual currencies has raised a number of consumer and investor protection issues, including: reported loss of consumer funds maintained by bitcoin (one type of virtual currency) exchanges, volatility in bitcoin prices, and the development of virtual-currency-based investment products. For example, in February a Tokyo-based bitcoin exchange filed for bankruptcy after reporting it had lost more than $460 million.
- The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) released guidance in March 2013 requiring virtual currency exchanges to register with FinCEN. Federal agencies also have begun to collaborate on virtual currency issues through informal discussions and interagency working groups.

These working groups have focused on law enforcement aspects of virtual currencies, but not on emerging consumer protection issues. The GAO report states that the CFPB has "generally not participated" in these groups.

"Therefore, interagency efforts related to virtual currencies may not be consistent with key practices that can benefit interagency collaboration, such as including all relevant participants to ensure they contribute to the outcomes of the effort. As a result, future interagency efforts may not be in a position to address consumer risks associated with virtual currencies in the most timely and effective manner," the report reads.

The GAO recommended that the CFPB "take steps to identify and participate in pertinent interagency working groups addressing virtual currencies, in coordination with other participating agencies."

Activity Reports topic of InfoSight. You will find information about:

- Recordkeeping requirements
- SARs and elder abuse
- Terrorism and suspicious activity
- SAR confidentiality and subpoenas

CU Compliance Connection: CFPB Integrated Mortgage Disclosures

The CFPB has finally released the Integrated Mortgage Disclosure requirements that have been in the works for over two years. Click here for the video.

AffirmX RISK INTELLIGENCE

Our compliance partners at NeighborBench have changed their name to AffirmX.

Enhancements have been made to this cloud-based, near real-time solution that identifies risk AND provides you access to experts. This innovative tool combines call-report data, onsite visits, and document review in the areas of Operations, Lending, BSA, Deposit and Advertising. Imagine staying current with your consumer regulatory compliance risks in one easy-to-read dashboard depiction that saves you time and money. If a full suite of compliance risk assessments isn't the answer for you, we now offer a basic annual compliance package, including BSA, ACH, SAFE Act, and Website compliance for one low price.

For more information about our compliance services, please contact Melia Heimbuck at: mheimbuck@mwcua.com or (720) 479-3325 or 1 (800) 477-1697 ext. 3325

Advocacy Highlights

CUNA Seeks Feedback on CFPB Request for Information on Mobile Financial Services, Underserved Consumers

CUNA has requested a response to a recent Regulatory Call to Action by September 1 on the CFPB's recent request for information on mobile financial services, including how mobile technologies are impacting underserved consumers with limited access to traditional financial systems.

Specifically, the agency is interested in how consumers are using mobile financial services to access products and services, manage finances, and achieve their financial goals. For this request, "mobile financial services" includes mobile applications to access financial services and financial management, but does not include mobile point of sale payments, except with respect to potential benefits and risks of mobile payments that are targeted specifically for low-income and underserved consumers.

The CFPB seeks information on:

According to the GAO Virtual Currencies Report (PDF), the CFPB has agreed with this recommendation.

Source: CUNA News Now

CUs Among FIs With Increased Cybersecurity Assessments

While data breaches at retailers have made headlines recently, financial institutions of all sizes are vulnerable to cyber-attacks. With that in mind, the Federal Financial Institutions Examinations Council (FFIEC) has launched a pilot program to assess 500 financial institutions' supervisory policies and processes when it comes to cybersecurity.

The assessments will be used to develop a preliminary assessment of how community financial institutions manage cybersecurity, said National Credit Union Administration spokesman John Fairbanks. Credit unions represent about half of the institutions being examined. These credit unions range from small to very large asset sizes.

"This pilot is one of several FFIEC assessments that will ultimately benefit community financial institutions by assisting regulators in strengthening and standardizing our supervisory programs and being responsive to industry requests for supervisory guidance," Fairbanks said. "The assessments under the FFIEC pilot program are being done during the normal exam cycle using existing rules and regulations."

Should the assessments lead the NCUA to identify policies and procedures that do not meet legal requirements or supervisory expectation, the institution will be notified and concerns will be handled as they would normally be during a standard exam.

In announcing the pilot program in May, the FFIEC said its members want to provide additional support to community banks, which may not have access to the resources available to larger institutions.

NCUA Chair Debbie Matz recalled one incident in her February address at the Credit Union National Association's Governmental Affairs Conference in which hackers broke into a medium-sized credit union and used that credit union's passwords to access a large credit bureau, allowing them to steal credit reports from hundreds of consumers.

"These attacks are like poison-tipped darts. Where they hit doesn't matter. Once that poison hits your bloodstream, it moves quickly through the system," she said.

The FFIEC, which in addition to the NCUA counts as its members the Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, Federal Deposit Insurance Corp., Federal Reserve Board and a liaison committee of state regulators, has said that the pilot program will not result in any new examination rating.

Source: CUNA News Now

Treasury Reaches Largest Ever Sanctions-Related Settlement

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has announced its largest settlement to date--a $963 million agreement with BNP Paribas SA (BNPP) to settle its potential liability for apparent violations of U.S. sanctions regulations.

In an announcement of this week's settlement, Treasury said the agreement resolves an investigation into BNPP's "systemic practice of concealing, removing, omitting, or obscuring references to information about U.S.-sanctioned parties in 3,897 financial and trade transactions routed to or through banks in the United States between 2005 and 2012" in apparent violation of a series of regulations.

"Today's settlement is OFAC's largest-ever and reaffirms OFAC's determination to aggressively enforce U.S. sanctions, rules and regulations," said OFAC Director Adam J. Szubin in a release. "The settlement is the result of an interagency effort to investigate institutions that abuse the U.S. financial system and undermine U.S. sanctions programs. OFAC will continue to coordinate these efforts with other federal and state agencies in order to protect the U.S. financial infrastructure from the risks inherent in this type of illicit activity."

Under the settlement agreement, BNPP is required to put in place and maintain policies and procedures to minimize the risk of the recurrence of such conduct in the future.

Source: CUNA News Now

Canadian Anti-Spam Law Addresses Commercial Emails

Canada's anti-spam law took effect Tuesday, and while the statute is a Canadian law, it affects any commercial electronic message (CEM) sent to Canadian recipients. A CEM can be defined as any electronic message sent with the purpose of encouraging participation in a commercial activity.

Valerie Moss, senior director of compliance analysis for regulatory affairs for the Credit Union

- The general use of mobile financial services and opportunities to address the needs of consumers, including economically vulnerable populations. These opportunities include enhancing access to convenient financial services, facilitating effective account management, and building financial capability.
- Barriers to low-income, underserved, or economically vulnerable consumers accessing and using mobile technology for financial services.
- Potential consumer protection issues associated with the use of mobile technology for financial services by economically vulnerable consumers.

Source: CUNA

CUNA Regulatory Advocacy Report

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

- CUNA's ACUC: NCUA Reiterates RBC Proposal Will Change
- Credit Unions Among Community Financial Institutions with Increased Cybersecurity Assessments
- Regulators Issue Interagency Guidance on HELOCs
- FTC Releases Privacy and Data Security Report
- GAO Recommends the CFPB Join Other Agencies Already Reviewing Regulatory and Consumer Protection Concerns associated with Virtual Currencies
- IRS Releases Final Regulation Allowing Longevity Annuities

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

CUNA Credit Union National Association

2014 Compliance Calendar

July 31

- Credit Card Quarterly Agreement Submission Due to CFPB

September 1

- Labor Day - Federal Holiday

September 19

- NACHA Operating Rules Changes

October 13

- Columbus Day – Federal Holiday

October 31

- Credit Card Qtrly Agreement Submission Due to CFPB

National Association, writes on CUNA's *CompBlog* that a CEM can include emails, text messages and some social media messaging.

"We have been asked whether Canada's new anti-spam requirements will affect U.S. credit unions that send marketing messages to members who reside in Canada. The answer appears to be yes," she wrote. However, there is a grandfather clause for existing credit union members and a safe harbor for emails that comply with the U.S. CAN-SPAM Act that should help limit compliance burdens on U.S. credit unions.

Moss lists three general requirements for sending a CEM to an electronic address (defined as an email account, a telephone account, an instant messaging account and any other similar account) in Canada: the recipient's consent to receive CEMs; the sender's identification and contact information; and an unsubscribe mechanism that can be "readily performed."

Consent to send CEMs is implied for a period of at least 36 months following the law's implementation where there has previously been an existing business relationship.

Significantly for credit unions, the "implied consent" period likely extends beyond 36 months in the case of a person who is a member of the credit union on July 1, 2014, until he or she leaves the credit union's membership, because the existing business relationship remains continuous so long as the member maintains his or her membership share.

The law also contains a safe harbor if the sender is located outside of Canada, the sender reasonably believed that the recipient would access the commercial electronic message outside of Canada in a jurisdiction on the ECPR List of Foreign States schedule, which includes the United States, and the CEM was in compliance with that jurisdiction's "substantially similar" anti-spam law, that is, the CAN-SPAM Act in the case of a U.S. credit union.

The law and its implementing regulations generally prohibit:

- Sending of commercial electronic messages without the recipient's consent;
- Alteration of transmission data in an electronic message resulting in the message being delivered to a different destination without consent;
- Installation of computer programs without the express consent of the owner of the computer system or its agent;
- Use of false or misleading representations while promoting products or services;
- Collection of personal information through accessing a computer in violation of Canadian law; and
- Collection of electronic addresses by the use of computer programs or the use of such addresses, without permission.

CUNA Comp Blog: Canada's Anti-Spam Law (members only)

Also, the World Council of Credit Unions has produced an extensive summary of Canada's Anti-Spam Legislation (CASL) for non-Canadian credit unions. *Source: CUNA News Now*

MOUNTAIN WEST Credit Union Association

Training & Events Calendar

July 29
Webinar: Steps to SAFE Act Registration, Renewal & Compliance for MLOs

July 30
Webinar: Real Estate Lending Series: Avoiding HMDA Reporting Mistakes

August 5
Webinar: ACH Specialist Series: Federal Government ACH Payments: Reclamations & Garnishments

August 6
Wire Transfer Compliance

September 9 – 11
Regulatory Compliance School - Denver

September 16 – 17
Regulatory Compliance School - Casper

November 4 – 6
Regulatory Compliance School - Phoenix

November 2

• Daylight Savings Time Ends

November 11

• Veterans' Day – Federal Holiday

2014 Effective Dates
New and Revised Rules

June 30, 2014~NCUA
Credit Union Service Organization

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

Webinars

July 14

3rd Party Vendors and Regulatory Compliance Demands

July 17

Garnishments-Levies

July 22
Consumer Lending Update and Fair Lending

July 29
Mortgage Lending Update

August 10
CUNA Lending Compliance School

August 21
MIP and Account Openings

Schools and Conferences

August 10 – 14
CUNA Lending Compliance School, Las Vegas

September 14 – 19
CUNA Regulatory Compliance School Introduction & Update, Chicago, IL

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

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 Deb Larrabee