



InfoSight Highlight

Social Media Security

Social Media Risk Management Program

Credit unions should have a “risk management program” that permits it to “identify, measure, monitor, and control the risks related to social media.” The risk management program should also include the involvement of “compliance, technology, information security, legal, human resources, and marketing” departments. According to the FFIEC, these risk management programs should have the following components:

- A governance structure with clear roles and responsibilities;
- Policies and procedures regarding the use and monitoring of social media and compliance with all applicable consumer protection laws, regulations, and guidance;
- A due diligence process for selecting and managing third-party service provider relationships in connection with social media;
- An employee training program that incorporates the institution’s policies and procedures for official, work-related use of social media, and potentially for other uses of social media;
- An oversight process for monitoring information posted to proprietary social media sites administered by the financial institution or a contracted third party;
- Audit and compliance functions to ensure ongoing compliance with internal policies and all applicable laws, regulations, and guidance; and
- Parameters for providing appropriate reporting to the financial institution’s board of directors or senior management that enable periodic evaluation of the effectiveness of the social media program and whether the program is achieving its stated objectives.

Even if the credit union does not participate in social media, it should be prepared to respond to potential negative comments or complaints that may be posted on social media platforms. Credit unions must also provide guidance to employees regarding use of social media.

For additional information, click [here](#) for the topic.

Review the information today to help your credit union remain in compliance.

Compliance News

Q&A: Subordination Agreements and the GRMA Fee

Q. Would the recording lender be required to pay the Georgia Residential Mortgage Act (GRMA) fee on Subordination Agreements recorded in Georgia? What about Loan Modifications?



InfoSight
Compliance eNEWSLETTER
September 6, 2016
Vol. 10, Issue 36

Created in partnership with the



Credit Union National Association

Compliance Video

CU Compliance Connection

Military Lending and 3rd Quarter 2016 Review (NEW!)

This video provides an overview of the key changes made to the Military Lending Act that credit unions are going to need to consider and implement prior to the compliance effective date of October 3, 2016. View the video [here](#).

Be sure to view this [new video](#), where Glory LeDu, Manager of League System Relations, provides an overview of the compliance challenges your credit union is facing now in the 3rd quarter of 2016.

New Compliance Video: Same Day ACH Preview

In this newly released video, Amy Smith, VP and Executive Director of The Clearing House Payments Authority, provides background information on the current batch-and-forward ACH payment system and introduces the "Phased Approach" of the Same Day ACH

A. Yes in both cases. According to O.C.G.A. [§ 7-1-1000\(21\)](#) if the loan is secured by a deed to secure debt, security deed, mortgage, security instrument, deed of trust, a modification of a security deed, or other form or modification of a security interest which has been recorded, then the credit union would need to collect the \$10 GRMA fee, because the credit union is being modified in their position with either a Subordination Agreement or a Loan Modification. See 80-5-1-.04 below.

Rule 80-5-1-.04. Levy, Collection, and Remittance of Georgia Residential Mortgage Act Per Loan Fee

(a) Each borrower who obtains a mortgage loan as defined in O.C.G.A. § 7-1-1000(21) shall pay to the department a per loan fee of \$10.00. The \$10.00 fee will be due if the loan is secured by a deed to secure debt, security deed, mortgage, security instrument, deed of trust, a modification of a security deed, or other form or modification of a security interest which has been recorded. A change to a security instrument made solely for the purpose of correcting a clerical error will not be subject to a \$10.00 fee. Any person who closes mortgage loans that are subject to regulation under Article 13, regardless of whether said person is required to be licensed or registered under the Georgia Residential Mortgage Act, shall act as collecting agent for payment to the department of said per loan fee for each mortgage loan closed by that person. A mortgage loan shall be deemed to have been closed by a person if such person is indicated as the secured party on the security deed or any other loan document that establishes a lien on the residential real estate taken as collateral for the mortgage loan.

Wire Transfers Reminder from the Georgia Department of Banking and Finance

Using a financial institution to send funds electronically has become a fast, convenient, and frequently used tool for customers and members of financial institutions. Wire transfers have additional risk exposure because the transactions are both immediate and irrevocable. In addition, wire transfer fraud continues to rise and evolve. Social engineering plays an increasingly large role in wire transfer fraud, with perpetrators researching companies and financial institutions for weaknesses in controls that can be manipulated. Most vulnerable are the financial institutions and business customers that have not implemented and adhered to robust solutions to mitigate risk. The Board of Directors (Board) of each financial institution should ensure that adequate policies are in place, and management should implement appropriate risk management practices.

The Board should also fully understand the limits of the fidelity bond coverage. Financial institutions are audited and examined to determine if security procedures satisfy prevailing standards. If an institution does not have adequate controls or does not adhere to them, fraudulent transactions that might otherwise be covered may be disallowed. For example, policies that do not include appropriate limits could be considered to be ineffective controls. The dollar amount authorized in the Board's policy may be "unlimited" or so large that it is effectively unlimited which results in no reasonable mitigation of the loss exposure amount. Also, authorization or other access to wire transfers

program, which will begin in September of 2016. You will want to pay special attention to Amy's suggestion to review current ACH files you may be transmitting. View the video [here](#).

Compliance Calendar

October 3, 2016:
[DOD Military Lending Act Regulation - Effective Date](#)

October 3, 2016:
[NACHA's Network Quality Rule](#)

October 10, 2016:
Columbus Day - Federal Holiday

October 24, 2016:
[5300 Call Report Due to NCUA](#)

November 6, 2016:
Daylight Saving Time Ends

November 11, 2016:
Veterans' Day - Federal Holiday

November 24, 2016:
Thanksgiving Day - Federal Holiday

December 1, 2016:
Overtime Rule - Department of Labor

December 25, 2016:
Christmas Day - Federal Holiday

[Click here for upcoming compliance dates.](#)

Compliance Training

September 7, 2016
[Financial Literacy Part 1: Understanding the NCUA Regulation & the 7 Critical Risk Areas Directors Should Track](#)
Webinar
3:00 - 4:30 ET

September 8, 2016
[Lending Series: Writing Effective](#)

may not be limited to personnel whose job responsibilities require access, resulting in the lack of appropriate risk mitigation practices. The Department encourages the Boards of financial institutions to review policies for internal controls addressing wire transfers. In addition, the Board should periodically assess the adequacy of insurance coverage to limit the financial exposure to wire transfer fraud. Moreover, the Board should read its policy closely to determine if coverage specifically excludes loss from certain funds transfer transactions such as a forgery exclusion. If such an exclusion is present, the Board may want to consider adding a rider to the policy.

Management should look closely at wire transfer operations, ensuring not only that adequate internal controls are developed, but also that controls are not being circumvented for convenience and a desire to make the transactions more user friendly for the customer or member. In the short run, these results may seem desirable, but neglect of the established controls can result in losses that may not be recoverable. Department examiners report instances in which the list of individuals authorized to execute wires includes individuals who no longer work for the financial institution, controls requiring two individuals to approve the transfer are circumvented when one of authorized individuals provides the information necessary to another individual without actually reviewing the transaction, confirmations are not performed, or contact information has been changed by someone not affiliated with the customer. Management should consider customer or member education as a valuable component of risk mitigation. The Board should take steps to implement an effective system to evaluate compliance with established internal controls that ensures continuous updates to policies, as appropriate.

One of the more frequent scams is known as a corporate account takeover (CATO), which involves the perpetrator posing as a company executive calling to request a wire transfer, frequently to a foreign financial entity, that needs to be executed quickly. The perpetrator is counting on weaknesses in controls that would lead to failure to confirm the wire transfer request. This scam was discussed in a previous Financial Institutions Today article, with links to guidance that discussed appropriate internal controls that would mitigate risk to financial institutions that are targeted for fraudulent wire transfers.

http://dbf.georgia.gov/sites/dbf.georgia.gov/files/related_files/document/February2013Bulletin.pdf. A variation on CATO that recently emerged has been business email compromise (BEC). FS-ISAC and federal law enforcement agencies have released a joint alert warning companies of BEC which is available at https://www.fsisac.com/sites/default/files/news/BEC_Joint_Product_Final.pdf.

FinCEN Proposes End of AML Program Exemption

FinCEN has published at **81 FR 58425** in today's *Federal Register* a proposed rule that would amend portions of 31 CFR parts 1010 and 1020 to remove the anti-money laundering program exemption for banks that lack a Federal functional regulator, including, but not limited to, private banks, non-federally insured credit unions, and certain trust companies. The proposed rule would prescribe minimum standards for anti-money laundering programs for banks without a Federal functional regulator to ensure that all banks, regardless of whether they are subject to Federal regulation and oversight, are required to

Credit Memos & Loan Narratives Webinar

3:00 - 4:30 ET

September 12, 2016

New Customer Due Diligence
Rules for Beneficial Ownership:
Implementation Game Plan

Webinar

3:00 - 4:30 ET

September 12-14, 2016

Georgia Compliance Road Trip
North and South ATL, Macon and
Savannah
Check link for times

September 13, 2016

Navigating Compliance Issues for
Promotions, Bonuses, Contests &
Sweepstakes

Webinar

3:00 - 4:30 ET

September 19, 2016

HMDA Roadmap Part 1: Impact,
Important Changes &
Implementation Considerations for
Lenders

Webinar

3:00 - 4:30 ET

September 20, 2016

Director Series: Director & Officer
Liability: Rules, Risks & Trends

Webinar

3:00 - 4:30 ET

September 21, 2016

ACH for the Frontline

Webinar

3:00 - 4:30 ET

September 22, 2016

Debt Collection Series: Best
Practices for Garnishments &
Levies: Getting It Right!

Webinar

3:00 - 4:30 ET

September 27, 2016

Cyber Series: Mobile Remote
Deposit Strategies: Technology,
Deployment Models & Risks

establish and implement anti-money laundering programs, and would extend customer identification program requirements and beneficial ownership requirements to those banks not already subject to these requirements. Comments on the proposal are due by October 24, 2016.

New NACHA Rule Requires ACH Originators to Provide Third- Party Sender Information

Effective September 29, 2017, NACHA's newly approved Third-Party Sender Registration Rule will require originating depository financial institutions (ODFIs) to submit and maintain a basic set of information on each third-party sender with which it maintains a relationship. The stated intent of this requirement is to maintain ACH network quality. The information required for all third-party senders includes:

- The name and principal business location of the Third-Party Sender;
- The routing number used in ACH transactions originated for the Third-Party Sender;
- The Company Identification(s) of the Third-Party Sender.

It seems reasonable to assume the ODFI already has this information on file. If the ODFI does not provide services to any third-party senders, it will be required to submit a statement to that effect.

The rule becomes somewhat more complex in its requirement to similarly register "nested" third-party senders, i.e. third parties that are transacting via a relationship with another third-party sender, rather than with the ODFI itself.

The ODFI will be further obligated to provide more detailed supplemental information on third-party senders within ten banking days of written notice, in cases where NACHA believes a given third-party sender "poses an escalated risk" to the network.

While the rule makes no mention of Same Day ACH (slated to launch September 23, 2016), it seems reasonable to assume that such added protections take on added importance in a same-day environment. More generally, the rule helps to address the increasing role of third-party senders in the system and the concern voiced by regulators like the FFIEC and OCC regarding those risks.

Additional Information:

[NACHA Press Release: NACHA Announces Approval of Rule that Establishes Third-Party Sender Registration Requirements](#)

[Third-Party Sender Registration Information](#)

Need Help with Your Cybersecurity Assessment?

Last June, the [FFIEC agencies](#) released an [extensive Cybersecurity Assessment Tool](#) to help financial institutions evaluate their overall cybersecurity risk, as well as assess and monitor their cyber-preparedness.

Webinar

3:00 - 4:30 ET

September 28, 2016

[Clarifying Signature Card Confusion for Personal & Business Accounts: Compliance, Account Titling & Ownership](#)
Webinar

3:00 - 4:30 ET

September 29, 2016

[Maximizing LinkedIn to Build a "Social Selling" Culture](#)
Webinar

3:00 - 4:30 ET

October 3, 2016

[New CFPB Amended Mortgage Servicing Rules: What You Must Know Now & Why Advance Planning is Critical](#)
Webinar

3:00 - 4:30 ET

October 4, 2016

[Handling Dormant Accounts, Unclaimed Property & Escheatment](#)
Webinar

3:00 - 4:30 ET

October 5, 2016

[Essential Compliance Regulations for Deposit Operations](#)
Webinar

3:00 - 4:30 ET

October 6, 2016

[Avoiding the Top 10 Legal & Compliance Mistakes in the E-Statement Process](#)
Webinar

3:00 - 4:30 ET

October 11, 2016

[HMDA Roadmap Part 2: Operations Systems, Audit & Reporting Implications](#)
Webinar

3:00 - 4:30 ET

October 12, 2016

[Frontline Series: Skills & Tools for](#)

NCUA encourages credit unions of all sizes to use the FFIEC [tool](#) to manage cybersecurity risk. NCUA examiners are receiving training and will begin incorporating the tool into examinations this year. (See [NCUA's 2016 supervisory priorities](#) released in January).

CUNA Strategic Services provider [TraceSecurity](#) has developed an automated tool to assist credit unions with implementation of the complex FFIEC cyber-assessment. The TraceSecurity tool incorporates all aspects of the assessment into a user-friendly, easily accessible application. And guess what? **It's free!**

Upon assessment completion, results are compiled into an export of the data as well as a report that evaluates the credit union's results and includes TraceSecurity's recommendations to improve cybersecurity maturity.

[Click here](#) to access TraceSecurity's Free Cybersecurity Assessment Tool

See also: CUNA's e-Guide - [Cybersecurity](#) for more information.

Your CU Should Know...

Discussion Points for Compliance Road Trip in Georgia

- Form Management (Putting Compliance to Paper)
- Military Lending Act (Where are we now and what about setoff?)
- Fair Credit Reporting Act (The invisible compliance killer)
- Social Media and Website Marketing (There are rules on this stuff!)
- Collections Compliance and Lender Liability (Ouch ... just ouch)
- Compliance Management/Quality Assurance (Putting Knowledge Into Action)

In four locations, September 12 - 14
North and South Atlanta, Macon and Savannah

Click [here](#) for the event flier (PDF).

To register go to www.gcua.org, the second scrolling banner will take you to an information page along with a link for registration.

Unclaimed Property Deadline Reminder

This is a reminder to all credit unions with unclaimed property to remit to the State of Georgia. The property is due by **November 1, 2016** to the Georgia Department of Revenue (DOR). If your credit union cannot complete the due diligence requirements in order to meet the November 1st deadline, you can request an extension by contacting the Unclaimed Property Division of the Department of Revenue at (404) 968-0490.

For the appropriate reporting guidelines, see the [July 25, 2016](#) issue of InfoSight Compliance eNEWSLETTER. The 2016 filing requirements and report forms are available on the [DOR's website](#). Questions to the Unclaimed Property Division can be made to the phone number above or emailed

[Improving Teller Performance](#) Webinar

3:00 - 4:30 ET

October 13, 2016

[Proper Repossession, Notice & Sale of Non-Real Estate Collateral](#) Webinar

3:00 - 4:30 ET

October 17, 2016

[Countdown to the New Overtime Rules: How to Bring Your Credit Union into Compliance by the December 1, 2016 Deadline](#) Webinar

3:00 - 4:30 ET

October 18, 2016

[Liquidity Funding Concerns in a Rising Interest Rate Market](#) Webinar

3:00 - 4:30 ET

October 19, 2016

[Understanding Title Insurance Policies, Commitments & ALTA Endorsements](#) Webinar

3:00 - 4:30 ET

October 20, 2016

[Conducting the 2016 ACH Audit](#) Webinar

3:00 - 4:30 ET

October 24, 2016

[New CFPB Amended Rules for Mortgage Foreclosure & Bankruptcy Protections: Preparing Now for the 2017 Effective Date](#) Webinar

3:00 - 4:30 ET

November 2, 2016

[Notary Essentials & Legalities for Credit Unions](#) Webinar

3:00 - 4:30 ET

November 3, 2016

[Cyber Series: Member Authentication & Validation: The New Normal in Risk Mitigation](#)

to ucpmail@dor.qa.gov.

NCUA Encourages Flexibility in Post-Flood Assistance

The NCUA has **encouraged** credit unions to work with their members and consider options for assisting them that include offering new loans with special loan terms or rates and reduced documentation, providing payment flexibility for current loans, or potentially restructuring existing loans. Federal credit unions with questions about these options should contact their examiners. Credit Unions are also reminded that **NCUA Letter 11-CU-13** provides they may provide emergency financial services to nonmembers as part of their authority to engage in charitable activities under their incidental powers. Such services could include check cashing for nonmembers, access to ATM networks, or other means to access cash, to meet the short-term, emergency needs of nonmembers. Federal credit unions providing these emergency services must do so on a charitable basis, meaning that service charges cannot exceed direct costs.

FFIEC BSA Manual

Have you ever wanted a copy of the Bank Secrecy Act Manual? There are two ways to get a copy:

You can purchase direct from the Government Printing Office, https://bookstore.gpo.gov/search/apachesolr_search/Bank%20Secrecy%20Act \$19 + shipping.

Or; here is a link to the FFIEC Manual that is easily searchable, <http://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/ffiec-bsa-aml-examination-manual.pdf>

Either way it is a great resource to have at your fingertips.

Same Day ACH Return Items Info

Federal Reserve Financial Services has **posted a notice** concerning how FedACH will deliver non-future-dated return items beginning with the September 23, 2016, implementation of Same Day ACH processing.

CFPB Focus on Elder Financial Abuse

The Consumer Financial Protection Bureau has issued a **press release** and posted an **article** concerning elder financial abuse. A guide and best practices to help communities create partnerships for senior and ways individuals can support community efforts to fight elder financial exploitation are discussed.

Omaha Bank Pays for Card Add-On Practices

The First National Bank of Omaha has been issued orders by the Office of the Comptroller of the Currency and the Consumer Financial Protection Bureau to pay a total of \$7.5 million in civil money penalties and approximately \$27.75 million in restitution to affected consumers for unfair or deceptive acts or practice under the Federal Trade Commission Act (OCC order) and unfair, deceptive or abusive acts or practices under the Consumer Protection Act (Bureau) in the marketing and sale of debt-cancellation add-on products and the billing of consumers for credit monitoring services they did not receive. This is the eighth action the Bureau has taken in coordination with another regulator to address illegal practices with respect to credit card add-on products and the 12th action the Bureau has taken in total to address such practices. See "[FNB of Omaha hit with \\$7.5 CMPs and \\$27.75 M restitution](#)" Penalties pages, for more on this story.

Webinar
3:00 - 4:30 ET

November 9, 2016
[Form 1099 Reporting: Third-Party Vendors, Foreclosures, Debt Forgiveness & More](#)
Webinar
3:00 - 4:30 ET

BSA Training Opportunities through GCUA
[Click here for details](#)

Bureau Snapshot Focuses on Bank Account and Service Complaints

The CFPB has [released](#) its monthly [complaint snapshot](#), this time highlighting consumer complaints about bank accounts and services. The report shows that consumers continue to experience problems managing their accounts. This month's report also highlights trends seen in complaints coming from Ohio.

Comment Calls

Small-Dollar Payday, Vehicle Title and Certain High-Cost Installment Loans

On June 2, in conjunction with a field hearing in Kansas City, Missouri, the CFPB released a more than 1300-page rule for Payday, Vehicle Title, and Certain High-Cost Installment Loans. The CFPB released the Small Business Regulatory Enforcement Fairness Act (SBREFA) proposals, prior to a Small Businesses Review Panel, for this rule more than a year ago. We have concerns that the rule will sweep in consumer friendly credit union small dollar loan products.

While the CFPB's proposed rule addresses some of the concerns raised by CUNA and credit unions prior to its release, and purports to exempt the National Credit Unions Administration's (NCUA) Payday Alternative Loan (PAL) program as requested, in actuality it adds many new regulatory and compliance burdens for federal and state-chartered credit unions working to underwrite consumer friendly small dollar options. The added requirements and changes to the PAL program eliminate flexibility in offering these loans, and will likely make many credit unions reevaluate their participation in the program. The rule also does not account for the diverse and unique structure of consumer friendly small dollar loans offered at state-chartered credit unions. To read CUNA's summary of the proposal [click here](#). GCUA would like to know your thoughts and/or concerns with this proposal. Please email Selina Gambrell at selinaq@gcua.org by **September 16th**.

The [CUNA Advocacy Update](#) keeps you on top of the most important changes in Washington for credit unions - and what CUNA is doing to monitor, analyze, and influence government agencies and federal law. You can view the current report and past reports from the archive.

Click [here](#) to request to be added to the mailing list for this and/or other GCUA email publications.

Bookmark InfoSight

No need to go through the Georgia Credit Union Affiliates home page to access InfoSight. Simply add the following link to your bookmarks: <http://ga.leagueinfosight.com/>.

Need a BSA, ACH or Website review? Email compliance@gcua.org.