InfoSight
Your Online Compliance Resource
Compliance eNEWSLETTER
powered by the Georgia Credit Union Affiliates

InfoSight Highlight

Compliance News

Week Five Supervisory Priority Highlight:
Information Systems and Assurance
Credit unions rely on various applications to ensure accurate, timely, and confidential processing of their data. Areas of vulnerabilities, especially web-based services, continue to be an area of attack for those looking to commit fraud and identity theft. Web-based services are most often associated with Internet banking products, like bill pay, credit cards, member applications, and cash management services. These programs are targeted for the following reasons:

- Easy Internet access by all (members, non-members, employees, servicers and vendors);
- Traditional network defenses (firewalls, intrusion detection/prevention systems) may not detect or prohibit unauthorized activity;

Georgia Credit Union Affiliates

InfoSight
Compliance eNEWSLETTER
February 19, 2019
Vol. 13, Issue 7
Created in partnership with the

Credit Union National Association

Compliance Video

Compliance Connection Video

In this video, League InfoSight CEO Glory LeDu talks about the highlights from the 4th Quarter of 2018 and the 1st Quarter of 2019.

When S.2155, the Economic Growth, Regulatory Relief, and Consumer Protection Act, passed in 2018 there was a lot to understand! Glory LeDu, League InfoSight CEO, provides Part 1 in this short video to break it down for you.

Compliance videos can be found on YouTube at the Compliance

- Breached applications may provide perpetrators unauthorized access to sensitive data that supports the application (member nonpublic personal information, financial records), and
- Known vulnerabilities due to weaknesses in application development, testing and quality assurance processes.

It is important to develop applications that mitigate application security risk by incorporating security into the development and quality assurance processes. Make sure your plan includes testing and a well-defined recurring process that identifies and monitors vulnerabilities, notifies users of vulnerabilities, and has corrective measures in place. The FFEIC provides two Information Examination Handbooks that provide basic guidance on application security.

FFIEC Information Security and Development and Acquisition

Risk Management

Two areas of supervisory focus for 2019 are the assessment of credit union IT risk management to ensure it effectively identifies, remediates and controls inherent risks to appropriate residual risk levels, and oversight of service provider arrangements to ensure credit unions implement effective risk-based supply chain management.

Management is responsible for determining that all applications are developed and maintained in a way that appropriately addresses risk to the confidentiality, availability and integrity of data. The risk assessment should address application security, which is required by NCUA rules and regulation, Part 748, Appendix A. Below are some key factors when considering the risk of an application:

- Internet accessibility of the application;
- Ability to process or have access to sensitive data;
- Source of the application's development (e.g., in-house, vendor-acquired or contracted);
- Extent of the secure practices used in the application's development process;
- Existence of an effective, recurring process to monitor, identify and remediate or correct vulnerabilities (e.g., patch program, etc.), and
- Existence of a periodic assurance process (e.g., independent audit, code review, etc.) to independently validate the security of the applications.

If your credit union relies on a vendor to provide secure applications, remember that management remains responsible for ensuring the

Connection channel, where they are generally updated quarterly.

Credit Union Compliance Help

Need a BSA, ACH, SAFE Act or website audit? GCUA has certified Compliance Specialists who can help. For scheduling and pricing information contact compliance@gcua.org.

Compliance Calendar

March 2019

March 1st
New InfoSight Rollout
March 10th
Daylight-Saving Time Begins

Click here for upcom

Compliance Training

February 19, 2019
Determining Cash Flow from Personal Tax Returns After 2018 Tax Reform Part 2: Schedules D, E & F
3:00 pm - 4:30 pm ET

February 20, 2019
Credit Analysis & Underwriting Series: Debt Service Coverage Calculations in Underwriting
3:00 pm - 4:30 pm ET

February 21, 2019
The New NIST Digital Identity Guidelines: Impact on Passwords, Security Questions & Account Lockouts
3:00 pm - 4:30 pm ET

February 25, 2019
Debit Card

application meets your security requirements. As part of the due diligence process, the credit union should request an attestation in writing from the vendor that their software development process follows secure development practices and is periodically tested. When considering higher risk applications, require that the vendor show proof of adherence to sound processes and validation through third-party testing or audits. Consider the following when evaluating applications for purchase:

- What are the vendor's risk-based processes for development and validation of the application security before, during and after it is purchased?
- What are the vendor's notification processes whenever security vulnerabilities are identified by the vendor, reported by credit unions, other customers, or reported in media by others?
- Will the vendor provide timely mitigation or remediation solutions to identified security vulnerabilities?
- Does the vendor have an industry-recognized third party who conducts application vulnerability assessments on the applications, including security? If so, credit union management should before purchase or during the RFI/RFP process:
    - obtain the third party's name,
    - determine how often the assessment is conducted,
    - determine the date of the last assessment,
    - secure a copy of the most recent assessment, if possible,
    - determine whether the application has any known open vulnerabilities,
    - determine the nature of the vulnerabilities, and
    - determine if the vendor is willing to share its secure coding processes and practices.
- If the vendor does not have a third party who conducts application vulnerability assessments, including security, can the vendor describe their internal methodology?
- Is the vendor willing to conduct, or contract for, an assessment to provide assurance to the credit union regarding the security of the application?
- Where appropriate, management should include in the contract language the need for current and ongoing application vulnerability assessments, including security, and who will conduct the assessments. Depending on the risk profile of the application, management may request the full vulnerability assessment report or a summary.

If your credit union developed its own in-house application, consider the following elements to ensure a coordinated effort across business lines:

Chargebacks: Understanding Visa Claims Resolution
3:00 pm - 4:30 pm ET

February 27, 2019
ACH Specialist Series: ACH Dispute Resolution
3:00 pm - 4:30 pm ET

February 28, 2019
Flood Insurance Compliance Update & FAQs
3:00 pm - 4:30 pm ET

March 4, 2019
Banking Marijuana-Related Businesses
3:00 pm - 4:30 pm ET

March 5, 2019
C-Suite Series: Strategic Decisions Regarding CECL Methodologies, Processes & Governance
3:00 pm - 4:30 pm ET

March 6, 2019
Board Reporting Series: Essential Board Reporting: Requirements, Timing, Delivery Options, Risks & Concerns
3:00 pm - 4:30 pm ET

March 7, 2019
Federal Requirements for Tech-Based Marketing: Websites, Social Media, Robo Calls & More
3:00 pm - 4:30 pm ET

March 11, 2019
Teller Training Series: Cross Selling: The Key to Accountholder Satisfaction & Retention

- Incorporate appropriate attack model/threats in the risk assessment to assist in determining the security and assurance requirements for the application;
- Analyze the environment in which the application will reside. As the environment changes, the security requirements and assurance needs for the application may also change;
- Ensure any open-source applications are also subject to appropriate development and assurance processes;
- Ensure appropriate personnel (i.e., management, developers, security, and auditors) are trained sufficiently to understand and be aware of risks associated with the credit union's technology environment;
- Engage in periodic application testing or validation based on a current risk assessment to ensure the ongoing and appropriate protection of transactions and member data. Testing consideration may include:
    - Static, dynamic and functional evaluations, depending on the type and criticality of the application;
    - Automated evaluations using commercial or freeware tools, as well as manual interaction to supplement application tools;
    - Authenticated and non-authenticated user scenarios;
    - Comprehensive testing in a simulated production environment including appropriate operating systems and associated databases. The weakest link in several connected components may expose the entire system to compromise;
    - Implementation of lessons learned iteratively throughout the development and periodic testing process; and
    - Identification and monitoring of developed applications for vulnerabilities through an ongoing and defined process that includes appropriate communications and remediation.

Management should also establish a mechanism to receive and respond appropriately to vulnerability reports from public and private sources.

Examiners will continue conducting information security maturity assessments with the Automated Cybersecurity Examination Toolbox (ACET). Examiners will use the ACET to assess credit unions with over $250 million in assets that have not previously received an assessment.

3:00 pm - 4:30 pm ET

March 12, 2019
Synthetic ID Fraud: What It Is, How It Works & Real-Life Scenarios
3:00 pm - 4:30 pm ET

March 13, 2019
ACH Specialist Series: 2019 ACH Rules Update
3:00 pm - 4:30 pm ET

March 14, 2019
Debit Card Chargebacks: Understanding Mastercard Dispute Resolution
3:00 pm - 4:30 pm ET

BSA Training Opportunities through GCUA
Click here for details

Reminder: 2018 Home Mortgage Disclosure Act Data Must Be Submitted by March 1
Credit unions with offices located in metropolitan areas that engage in certain types and volume of residential mortgage lending, and that had assets exceeding $45 million as of December 31, 2017, must file a Home Mortgage Disclosure Act loan/application register for calendar year 2018 loan activity by March 1.

Credit unions must submit their HMDA data using a web-based platform provided and maintained by the Consumer Financial Protection Bureau. HMDA is implemented by the Consumer Financial Protection Bureau's Regulation C.

You can learn more by accessing the amendments to Regulation C and additional information in the Fair Lending Compliance Resources section of the NCUA's Consumer Compliance Regulatory Resources webpage.

DBF Issues State-Chartered Credit Union Guidance
The Department of Banking and Finance recently issued guidance for state-chartered credit unions regarding the geographic common bond field of membership. This guidance provides details of the criteria the Department uses when reviewing applications from a credit union requesting the addition of a geographic common bond to its field of membership. The DBF website also offers a statement of policies that houses information intended to provide a better understanding on the decisions made by the Department. The statement of policies gives insight on why the Department makes certain decisions and how those decisions impact your credit union. Click here to read the most recent Guidance letter.

Click here to view the Statement of Policies.

Your CU Should Know

New Rule Covers Private Flood Insurance
The National Credit Union Administration Board unanimously approved a final rule allowing federally insured credit unions, under certain conditions, to accept private flood insurance policies in addition to National Flood Insurance Program policies. The Board approved the rule by notation vote on Jan. 31. It will take effect July 1, 2019.

CFPB Publishes the 2019 Lists of Rural or Underserved Counties
The Bureau has published on its website the 2019 list of rural and underserved counties and a separate 2019 list that includes only rural counties. The Bureau has also updated the rural and underserved areas website tool for 2019. The lists and the tool help creditors determine whether a property is located in a rural or underserved area for purposes of applying certain regulatory provisions related to mortgage loans. A creditor that makes a first-lien mortgage loan secured by a property located in a rural or underserved area during 2019 meets the requirements to be a creditor that operates in rural or underserved areas during 2020 and for loan applications received before April 1, 2021.

The 2019 lists can be found here. The rural and underserved areas tool can be found here.

CFPB Lists New Protections for Servicemembers and Veterans
The CFPB has posted an article discussing free credit monitoring, medical debt credit reporting restrictions, and mortgage protections for servicemembers. A provision of EGRRCPA that went into effect on September 21, 2018 requires free security freezes and one-year fraud alerts at the three nationwide credit reporting agencies.

In addition, other EGRRCPA provisions address a number of key financial issues for the military, including:

- Holding lenders to more stringent requirements when they participate in VA's refinance programs
- Ensuring continued foreclosure protections for servicemembers up to one year after they leave active duty
- Prohibiting medical debt that should have been paid by the VA to be reported as part of a veteran's credit history
- Providing free credit monitoring for active duty military, including the National Guard

Proposals to Rescind and Delay Portion of Payday Loan Rule
A press release from the Consumer Financial Protection Bureau states that the Bureau is proposing to rescind certain provisions of its 2017 final rule governing "Payday, Vehicle Title, and Certain High-Cost Installment Loans." Specifically, the Bureau is proposing to rescind the rule's requirements that lenders make certain underwriting determinations before issuing payday, single-payment vehicle title, and longer-term balloon payment loans. The CFPB is preliminarily finding that rescinding this requirement would increase consumer access to credit. The Bureau is also proposing to delay the August 19, 2019, compliance date for the mandatory underwriting provisions of the 2017 final rule to November 19, 2020. Neither of the proposals would reconsider or delay the provisions of the 2017 final rule governing payments, including reconsidering the scope of their coverage. These provisions are intended to increase consumer protections from harm associated with lenders' payment collection practices. The proposals:

- Rescission of underwriting requirements (Comments due 90 days following publication)
- Delay of underwriting requirements (Comments due 30 days following publication)

Additionally, on February 6, 2019, the CFPB posted the "Unofficial Redline of the Reconsideration NPRM's Proposed Amendments to the Payday Lending Rule" which provides the changes under consideration.

Also published that day was the "Table of Contents for Payday Reconsideration NPRM."

Security Spotlight

Sweetheart Scams Are On the Rise
Sweetheart scammers are con artists who prey on lonely people by pretending to fall in love with them in order to win their trust and steal their money. Fraudulent acts may involve access to the victims' money, credit union accounts, credit cards, passports, e-mail accounts, social security number or by getting the victims to commit financial fraud on their behalf.

While sweetheart scams can happen face-to-face, today's sweetheart scams often take place at online dating sites. Scammers frequently create fake identities on dating websites and social media (for example, say they are U.S. soldiers) - some have even created phony dating websites to capture credit card numbers and other private information. Thousands of people have been victimized by online romance scams and wind up not only embarrassed but with financial losses averaging more than $10,000 per person.

The FBI and Federal Trade Commission logged 15,000 romance-scam complaints in one year. It's reported

that only 15 percent of fraud victims report the crime, so the extent of confidence fraud is likely much higher. Since the scammers are usually corresponding with the victim from outside of the United States, it's close to impossible for U.S. authorities to identify or prosecute them. Once the scammer has achieved their financial goal, they will drop the unsuspecting victim and disappear.

Also, worth noting, it is not only those with wealth that are victimized. While a victim without financial resources may seem undesirable, scammers will still attempt to use their deceptive tricks to milk them for all they're worth. In some cases, they even succeed in getting their victims to allow them to move in rent-free, hand over their Social Security checks or make risky financial moves, such as taking out a reverse mortgage, in order to get their hands on some sort of assets or income.

Once the victim becomes attached, the scammer looks for ways to dupe the person into sending money, which can happen in two basic ways:

- The scammer may indirectly ask for money. For instance, some romance scammers express concern about their financial situation: can't afford an airline ticket to visit victim, can't afford bribes necessary to leave the country, need money for school tuition so they can graduate and come to the U.S. Their plan is for the victim to offer to send the funds.
- The scammer asks for money directly. A scammer may beg for hundreds or thousands of dollars, claiming a family member became suddenly ill, he or she was robbed, or the person is having difficulty obtaining travel documents after spending all his or her money on a plane ticket to visit the victim. A victim may even get a call from an accomplice who claims to be a lawyer or doctor to lend credibility to the tale.

Remember that Georgia law requires that as an employee of a financial institution, you are a mandated reporter of elder financial exploitation. If you suspect something, say something. For suspected abuse of adults in the community (living on their own) contact Adult Protective Services by phone at 1-866-552-4464 or online here.

For abuse in long-term care facilities, contact Healthcare Facility Regulation by phone at 1-800-878-6442. Both facilities are open from 8-5, Monday-Friday.

Pending Regulatory Comment Calls

For more information regarding these proposals, please follow the links below:

Issues	Comment Period Deadline	Agency	CUNA Staff Contact
Validation and Approval of Credit Score Models	Mar. 21, 2019	CFPB	Mitria Wilson
Consumer Credit Card Market	May 1, 2019	CFPB	Alexander Monterrubio
Payday, Vehicle Title, and Certain High-Cost Installment Loans	TBD	CFPB	Alexander Monterrubio
Payday, Vehicle Title, and Certain High-Cost Installment Loans; Delay of Compliance Date	TBD	CFPB	Alexander Monterrubio

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.