InfoSight Highlight

Internal Controls and Fraud Prevention
A study of employee frauds showed they lasted a median of 18 months before detection, with a median loss of $140,000. The study showed more than one-fifth of these caused losses of at least $1 million. The longer a perpetrator works for an organization, the higher fraud losses tend to be. CUNA Mutual Group claims records show that over a five-year period, employee dishonesty represented just 13% of fraud claims, but 45% of fraud losses.
Many credit unions believe their employees are all trustworthy and that they have strong enough internal controls to prevent internal theft from occurring. Yet, it still occurs.

Fraud does not discriminate. According to CUNA Mutual, there is no immunity to this exposure based on geography, asset size, employee tenure, or past experience.

Internal controls are plans, policies, and operational procedures that provide management with reasonable assurance that the credit union's operations and objectives will be achieved in a safe, sound, and prudent manner. A system of effective internal controls is a critical component of credit union management and the basic foundation for safe and sound credit union operation.

Review the information in the "Internal Controls and Fraud Prevention" topic in the Security channel to help your credit union get internal controls in place.

Compliance News

Mortgage Rule Published
The Consumer Financial Protection Bureau (CFPB) has published its final rule, announced on January 20, 2015, (see the January 26, 2015, edition of *InfoSight eNewsletter* for more information) that delays the deadline to the third business day for revised Loan Estimates resulting from rate locks; adds a Loan Estimate disclosure about revised estimates for some construction loans; makes some technical corrections to the final Integrated Disclosures rule; and adds the

Georgia Credit Union Affiliates

InfoSight
Compliance eNEWSLETTER
February 23, 2015
Vol. 9, Issue 8
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.

Just a reminder that Compliance videos since 2016 can be found on YouTube at the Compliance Connection

Integrated Disclosures to documents requiring loan originators' names and, if issued, NMLSR IDs.

HUD Clarifies Points and Fees Limits Adjustment
The Department of Housing and Urban Development (HUD) has published a final rule to clarify that all annual adjustments to the qualified mortgage points and fees limit issued by the CFPB apply to HUD's points and fees limit provision at 24 CFR 203.19. HUD's final rule is effective upon publication, and affects single-family residential mortgages that HUD insures, guarantees or administers. Under HUD's qualified mortgage rule, qualified mortgage status attaches at origination and insurance endorsement to those single family residential mortgages insured under the National Housing Act. For more information HUD's final rule is here.

NCUA Launches Small Business Lending Resource Center
Credit unions have a new online destination for information about member business lending thanks to a webpage released today by the National Credit Union Administration.

Available here, the Small Business Lending Resource page provides detailed information about NCUA's member business lending rules and regulations, supervisory guidance, links to the Small Business Administration's loan programs and related articles from *The NCUA Report*, NCUA's flagship publication.

NCUA and the SBA have signed a Memorandum of Understandingoutlining a series of educational initiatives during the next three years that include webinars, examiner training on SBA programs, data resources and media outreach.

This new partnership kicks off with a joint webinar, "Balancing Member Business Loan Portfolios with SBA Guarantees," on **March 4, 2015, at 2:00 p.m. EST**. Click here to register.

channel, where they are generally updated quarterly.

Compliance Calendar

March 3
Permissible Derivatives Effective Date

March 8
Daylight Savings Time Begins

March 30
NACHA Operating Rules Changes

April 24
5300 Call Report Due to NCUA

April 30
Credit Card Quarterly Agreement Submission Due to CFPB (10,000 or more open credit card accounts)

May 25
Memorial Day - Federal Holiday

Click here for upcoming compliance dates.

Compliance Training

February 25, 2015
Mandatory Repossession Letters and How to Avoid Common Mistakes - Webinar
1:00 – 2:15 p.m. EST

_____

Wrong Account Number on Tax Refund

Question: Who is liable in this situation: A member gives the IRS an incorrect account number, but the number was an actual credit union account number for another member. The tax refund was deposited in the other account in a Batch File with no exceptions. The other member spends all the money. Is the credit union liable for anything?

Answer: According to CUNA's Compliance Blog, the credit union is not liable for the misdirected funds, but the IRS does require the credit union to notify them. The IRS posts the following related FAQs on its website:

Is a Receiving Depository Financial Institution (RDFI) liable for an IRS tax refund sent to an account that does not belong to the named or intended recipient?

No. An RDFI is not liable for an IRS tax refund sent through the ACH network to an erroneous or fraudulent account since the IRS provided incorrect account information. The incorrect banking information may have been supplied to the IRS by the taxpayer on his/her signed tax return which authorized Direct Deposit. In addition, and RDFI is not liable in the event IRS directed a refund to an account based on a fraudulently filed tax return.

Can an RDFI rely strictly on the account number in the ACH Entry Detail Record when posting a tax refund payment to a customer's account?

Yes, an RDFI may post IRS tax refunds received via the Automated Clearing House (ACH) network using the account number only. Title 31 of the Code of Federal Regulations, Part 210 (31 CFR Part 210) requires Federal payments be sent to a deposit account at a financial institution in the name of the recipient. However, the RDFI is not obligated to ensure that IRS originates refunds in compliance with this requirement. Some smaller RDFIs may perform a match between the

March 4, 2015
Collection Compliance Do-s and Don't-s for the Frontline - Webinar
2:00 - 3:00 p.m. EST

March 10, 2015
8 Hour SAFE Comprehensive Mortgage Loan Originator Course #4528 (NMLS #1405021)
8:30 – 5:00 p.m.

March 11, 2015
Recognizing Financial Elder Abuse for the Frontline - Webinar
2:00 - 3:30 p.m. EST

March 23, 2015
The Director - A Guide to Effectively Working with the Supervisory Committee - Webinar
2:00 - 3:00 p.m. EST

March 25, 2015
Bankruptcy Best Practices for Credit Unions - Webinar
12:00 – 1:00 p.m. EST

March 31 – April 9, 2015
Protecting Members Under Reg E - Webinar Series
2:00 – 3:00 p.m. EST

April 1, 2015
New Accounts for the Frontline: Compliance Issues to Watch For - Webinar
2:00 - 3:00 p.m. EST

April 7, 2015
Regulation E for ACH Error Resolution - Which 60 Day Rule Will You Follow -

name on the payment and the name on the account; however 31 CFR 210 makes it clear that an RDFI is not required to perform a match.

What is an RDFI's obligation when it discovers that an IRS tax refund has been sent to the wrong account?

If the RDFI learns that an IRS tax refund has been misdirected to the wrong account, the RDFI is required under 31 CFR Part 210 to notify the Government of the error. An RDFI can satisfy this requirement by returning the original ACH credit entry to IRS with an appropriate return reason code. Alternatively, if account information is incorrect but the payment can be posted to the correct account an RDFI may choose to originate a Notification of Change (NOC) with the correct account and/or routing and transit number. Although an RDFI is not liable for a misdirected IRS tax refund sent to the wrong account because of IRS or taxpayer error, the RDFI is encouraged after it becomes aware of the error to return those funds to the IRS if the funds are still available in the account.

If IRS discovers that a refund was misdirected or fraudulent, can IRS require the RDFI to return the funds?

No. IRS may request the RDFI to return any funds available in the account, but the RDFI is not legally required to do so.

For related questions see the Direct Deposit of IRS Tax Refunds Resource Page Frequently Asked Questions.

The IRS has also posted its 2015 "Dirty Dozen" list of IRS tax scams.

_____

Privacy Policy on Website
Question: Does the new privacy rule, which allows for an alternative delivery method, require us to have a link to our privacy notice on the home page of the credit union's web site?

Webinar
2:00 - 3:00 p.m. EST

April 9, 2015
Sharpening Your Skip Tracing Skills - Webinar
12:00 – 1:30 p.m. EST

April 12-17, 2015
CUNA Regulatory Compliance School
Las Vegas, NV

April 14, 2015
Collections & Bankruptcy Update
Atlanta, Georgia

April 23, 2015
The Redaction Trap - NPI Disclosure Penalties to Avoid - Webinar
12:00 - 1:00 p.m. EST

April 28, 2015
IRA Contributions - Webinar
12:00 – 1:30 p.m. EST

May 5, 2015
Understanding and Processing Transfers and Rollovers - Webinar
12:00 – 1:30 p.m. EST

May 6, 2015
Trust Accounts - Webinar
12:00 – 1:00 p.m. EST

May 12, 2015
IRA Distributions - Webinar
12:00 – 1:30 p.m. EST

May 13, 2015
Cyber Crime - No Gun Needed, Detecting and Preventing a Corporate Account Takeover -

Answer: No, the rule does not require this. However, the CFPB **encourages** credit unions to include a link to the privacy policy on various pages of their Web sites, including the home page.

Question: The new privacy rule requires that the privacy notice be the only content on the page where we post our privacy notice. But could we include other helpful privacy-related information on that page?

Answer: Unfortunately, no. The CFPB is concerned that permitting information other than the privacy notice to be included on the Web page could detract from the prominence of the notice and make it less likely that a member would actually read it. The Bureau believes that the risk of such distracting information being included with the privacy notice outweighs any potential benefit to allowing additional content to be included on the page.

Although the rule only allows the content of the privacy notice to be on the privacy notice Web page, the CFPB notes that a link to supplemental privacy information that is located elsewhere on the credit union's website may be included as part of the navigational materials on the privacy notice Web page.

Are You Signed Up For NCUA Express?
Question: Several employees at our credit union are interested in receiving NCUA's communications as soon as they come out via email. Is that possible?

Answer: Yes! NCUA's Express system allows anyone interested in credit union issues to receive NCUA communications via e-mail. Within hours of publication, press releases, Letters to Credit Unions, Regulatory Alerts, and various other communications can be sent via e-mail. Subscribers will receive an e-mail message containing a brief description of the publication along with a link to download the publication from the www.ncua.gov web server. There is no cost for this service and it is available to anyone.

Webinar
2:00 – 3:00 p.m. EST

May 13, 2015
Estate Accounts, POAs, Rep Payee and Guardian Accounts - Webinar
12:00 - 1:00 p.m. EST

May 19, 2015
Required Minimum Distributions (RMDs) - Webinar
12:00 – 1:30 p.m. EST

May 20. 2015
Deceased Member Accounts - Webinar
12:00 – 1:00 p.m. EST

May 26, 2015
IRA Reporting - Webinar
12:00 – 1:30 p.m. EST

May 28, 2015
Indirect Lending - The CFPBs View on Auto Dealership Relationships - Webinar
12:00 – 1:00 p.m. EST

BSA Training Opportunities through GCUA
Click here for details

To subscribe or change selection options, click here.

The Difference Between Payment Card Breaches and Cyber Breaches
In 2013, the financial industry had the second highest per capita data breach cost and racked up more than $11.3 billion in card fraud expenses. What's driving these breaches? Two major categories: payment card and cyber breaches. Although both types of breaches are time-consuming and expensive to resolve, there are some critical differences between them.

PAYMENT CARD

This is defined as a compromise of the payment card data and is the type of breach that's made the news with depressing regularity over the past 12 months. The uptick in attacks started with Target in late 2013 and since that time has included Home Depot, Neiman Marcus, and Supervalu, among many, many others. The two most common methods of payment card data theft are skimming and database compromise.

- *Skimming* occurs when the thief installs a card reader device on a point of sale (POS) terminal or ATM. When the consumer uses their card, the skimming device reads and saves the magnetic stripe data. The thief retrieves the information and voila!, they're ready to create a counterfeit card. Historically, this type of skimming required a thief to physically affix a device to the POS or ATM terminal. Now clever thieves are doing it via Bluetooth and malware—which is how experts believe the 70 million+ Target thefts occurred.
- *Database compromise* occurs in one of two ways: when a thief thwarts a merchant/third-party processor's security tools or a merchant/third-party processor stores magnetic stripe data, which is subsequently stolen. This second method contributed to the TJ Maxx breach back in 2007. Although the card association's data security policies prohibit this data storage, not all merchants/processors follow their lead.

CYBER BREACH

A cyber breach involves the theft or loss of sensitive information or internal records. This could include everything from credit union

financial data and personnel files to personally identifiable member data.
Common access points include:

- *The cloud.* As the recent hacking of celebrity photos illustrates, the cloud is not as secure as we might like to think.
- *Public wi-fi.* This can be a huge point of data vulnerability, especially in conjunction with the next item.
- *Personal mobile devices.* Most companies let employees use their personal devices at work, but don't necessarily have security protocols in place to make that a smart choice. Plus, although consumers may be relatively diligent when it comes to protecting their computers or laptops from spyware, viruses and malware, few take the same precautions with their phones and tablets.
- *Active employee theft.* Much as we hate to admit it, a certain percentage of employees are active data thieves. Credit unions that don't follow best practices in data protection could be vulnerable.
- *Human error and system problems.* According to Symantec, a data security company, two-thirds of data breaches were caused by human error and system problems. Human errors could include transferring data outside the credit union or not deleting data on an appropriate schedule; system errors include inadvertent data dumps, errors in data transfer and identity and authentication failures. Employees can also cause problems by clicking on malicious links that allow malware/spyware/viruses to enter the system.
- *Operating system "holes."* Most system patches resolve security issues. If you skip the update, your system is exposed.
- *Physical data theft.* Although we tend to focus on electronic theft, paper data is also vulnerable.

Protect your credit union from data breaches! (Source: CUNA Mutual Group)

2015 CRA/HMDA Newsletter
The FFIEC has posted the 2015 CRA/HMDA Newsletter, which includes articles on:

- HOEPA changes and new edit changes

- Calendar year 2014 initial submission deadline
- Submission errors: invalid file format and invalid timestamp
- Secured e-mails notice
- Missing and overdue edit reports

FDIC Posts Mortgage Rules Video

The release of the third in a series of three technical assistance videos developed to assist bank employees in meeting regulatory requirements has been announced by the FDIC. This video focuses on the Mortgage Servicing Rules with particular emphasis on those entities that qualify for the "Small Servicer" exemption. The video series addresses compliance with certain mortgage rules issued by the CFPB.

Local Training - 8 Hour SAFE Comprehensive Mortgage Loan Originator Course

The new rules issued by the CFPB pursuant to Dodd-Frank amended Regulation Z and now **require that a loan originator must receive periodic training**. This training must cover Federal and State law requirements that relate to the individual loan originator's origination activities.

This course covers the following:

- Regulation Z (Truth-in-Lending)
- Regulation X (RESPA)
- Regulation B (Equal Credit Opportunity Act)
- Fair Housing Act
- Regulation C (Home Mortgage Disclosure Act)
- Adjustable Rate Mortgages
- Federal Housing Administration (FHA) and Veterans Administration (VA) loan programs
- Reading and Understanding Credit Reports & Scores / Fair Credit Reporting Act (FCRA)

Join us **March 10th in Atlanta** for this course, which was designed to meet the continuing education requirements of the SAFE Act inclusive of (3) hours federal laws & regulations, (3) hours ethics, consumer protection & fair lending, and (2) hours lending standards for the non-traditional mortgage product marketplace.

Please click here for more information and to register.

Comment Calls

NCUA's Risk Based Capital Proposal
The National Credit Union Administration Board has issued for a 90-day comment period a revised RBC proposal (RBC2). It would apply to federally insured credit unions with assets of over $100 million and would require them to maintain RBC based on a new formula of risk-based capital, as defined by NCUA, to total risk-weighted assets, also as defined by NCUA. A well-capitalized credit union would need to maintain a 10% RBC level (down from 10.5% in the first proposal) and an adequately capitalized credit union would need to have 8% RBC, in addition to meeting their net worth requirements. **The proposal includes other new regulatory provisions such as a requirement that covered credit unions maintain a capital adequacy plan**. The proposal does not change requirements regarding current net worth classifications, such as 7% net worth to be well capitalized.

To stay up-to-date on the latest information on NCUA's Risk Based Capital 2 proposal, please see CUNA's RBC2 Blog.

GCUA is seeking credit union comments on how the new proposal will affect their operations, and what further improvements are necessary. Please have comments to Selina Gambrell by **March 30th** at selinag@gcua.org.

The CUNA Regulatory Advocacy Report contains information from the office of the President of CUNA about regulatory issues that affect credit unions. 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 Affiliate's 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.