News of Interest to Credit Unions Regulated by the Credit Union Department

Newsletter

No. 01-18 ★ ☆ ★ *January 17, 2018*

Credit Union Department
914 East Anderson Lane
Austin, Texas 78752
Phone: 512-837-9236
Fax: 512-832-0278
Email: info@cud.texas.gov
Web Site: www.cud.texas.gov

The Credit Union Department (CUD) is the state agency that regulates and supervises credit unions chartered by the State of Texas. The Department is professionally accredited by the National Association of State Credit Union Supervisors (NASCUS) certifying that CUD maintains the highest standards and practices in state credit union supervision.

*Our **Mission** is to safeguard the public interest, protect the interests of credit union members and promote public confidence in credit unions.*

* * * *

Credit Union Commission

The Commission is the policy making body for CUD. The Commission is a board of private citizens appointed by and responsible to the Governor of Texas.

Members:

Allyson "Missy" Morrow, Chair
Sherri Brannon Merket, Vice Chair
Beckie Stockstill Cobb
Yusuf E. Farran
Steven "Steve" Gilman
Jim Minge
Kay Stewart
Rick Ybarra

Next Commission Meeting

Friday, March 9, 2018 beginning at 9:00 a.m. in the offices of CUD.

* * * *

FFIEC Launches Industry Outreach Page

The Federal Financial Institutions Examination Council (FFIEC) has launched a new Industry Outreach website for financial institutions, trade associations, third-party providers, and consultants to share information about current issues related to financial institution supervision, and to provide updates to supervisory guidance and regulations.

The website provides access to upcoming FFIEC-sponsored webinars and includes an archive of past webinars.

The Industry Outreach program was developed to enhance communication between the FFIEC and financial institutions, trade associations, third-party service providers, consultants, and other interested parties. To learn more about the program, or sign up for FFIEC email updates, visit https://industryoutreach.ffiec.gov

~~~~~~

December 2017 Call Report

The due date for the December 31, 2017 call report is S**unday, January 28, 2018, 11:59:59 p.m. Eastern**, to avoid civil money penalties. Your credit union's profile must be reviewed, updated, and certified **prior** to submitting your 5300 Call Report. Always remember that whenever you make a change to the profile, you **must** "save and certify" to permanently save your changes.

~~~~~~

Upcoming Holiday Schedule for CUD

The Department's office will be closed on **February 19th** in observance of President's Day.

~~~~~~
~~~~~~

Information Security Risk Assessment

As information technology (IT) programs become more and more critical to the operational and financial success of credit unions, it is important that the Board and management thoroughly assess information security risks and develop a comprehensive set of policies, procedures, processes, controls, and audit programs designed to directly address those risks. Further, management should engage independent testing of key control processes with a scope and frequency commensurate with the credit union's unique IT risk profile. The information security risk assessment process includes a number of steps that should result in a comprehensive understanding of the credit union's risks and mitigating controls. At a minimum, information security risk assessment steps should include:

1. Identification of all information assets that are used to create, store, or transmit data, either in electronic or paper form. Assets will include all electronic hardware and software but should also consider paper documents and the methods to create, store, and transmit paper, such as filing cabinets or courier services. Vendors that are responsible for creation, storage, and transmission of data should also be considered an information asset.
2. Identification of specific threats and vulnerabilities to the confidentiality, integrity, and accessibility of data and to the assets that create, store, and transmit data.
3. A supportable and reasonable assessment of the likelihood that each threat could manifest itself and the potential impact that the threat could have on the confidentiality, integrity, and accessibility of data. For vulnerabilities, management should identify and understand how each vulnerability exposes credit union data and information assets to specific threats.
4. Identify current policies, procedures, processes and controls designed to: protect data and assets against threats, address the vulnerabilities that compromise data and assets, and minimize the impact to the confidentiality, integrity, and accessibility of data and assets.
5. Make a determination, based on comparison of threats, vulnerabilities, and potential impacts to current policies and controls, of the residual risks to data and assets.

The final product should provide a foundation for the Board and management to develop a comprehensive set of policies, procedures, processes, and controls that are designed to address the identified threats and vulnerabilities and mitigate the risk of loss of confidentiality, integrity, and accessibility. Timely independent testing of control processes is necessary to identify any weaknesses that may exist in the control environment. After testing it is imperative that action is taken to address any weaknesses identified to mitigate vulnerabilities.

After corrective measures are implemented, the Board and management should re-assess information security risks, re-starting a continuous risk management cycle of assessment, controls, testing, and adjustment. In addition, any new introduction of information assets into the environment (such as electronic hardware or third-party vendors), identification of significant new threats (such as ransomware), or discovery of potential vulnerabilities (such as a bulletin on a newfound weakness in an operating system) should require a re-assessment of risks between the normal risk management cycle.

~~~~~~
~~~~~~

SAR Filings – Known Criminal Activity

The Department encourages credit unions to develop a relationship with local law enforcement, as these relationships are invaluable in the fight against financial crime for both the individual institution and the credit union industry as a whole. However, when law enforcement agencies respond to an incident in process, one which may even result in an arrest of the perpetrator, the credit union is not relieved of its responsibility to file a Suspicious Activity Report (SAR) with the Financial Crimes Enforcement Network (FinCEN) when the circumstances of the activity meet federal mandatory reporting requirements.

Federally-insured credit unions are required by Federal regulations to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through a financial institution or an affiliate and aggregating $5,000 or more, if the financial institution or affiliate knows, suspects, or has reason to suspect that the transaction:
  - May involve potential money laundering or other illegal activity (e.g., terrorism financing).
  - Is designed to evade the Bank Secrecy Act or its implementing regulations.
  - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The mandatory requirements listed above would include incidents that result in the arrest of the perpetrator. SAR filings in these instances are not only mandated, but aid law enforcement agencies in their efforts. FinCEN is a robust network and investigators use SAR data to identify patterns of criminal activity that lead to detection of other bad actors or larger criminal organizations.

Texas state-chartered credit unions are reminded of Rule 91.208 (Notice of Known or Suspected Criminal Violations), which requires a credit union to provide written notice to the Department within 30 calendar days for any of the following known or suspected criminal violations:

1. Insider abuse involving any amount,
2. Other transactions, including potential money laundering or violations of the Bank Secrecy Act, aggregating $5,000 or more,
3. Losses resulting from robbery or burglary.

When applicable, a credit union may meet the reporting requirements of this rule by providing the Department a copy of a Suspicious Activity Report prepared in accordance with NCUA Rules and Regulations 12 C.F.R. Section 748.1(c).

~~~~~~
~~~~~~

Cybersecurity Issue: Smishing Attacks

"Smishing" (SMS phishing) is a text messaging scam that continues to become more prevalent. Smishing is similar to email "phishing" scams and the bottom line is identity theft.

A smishing attack uses a text message to deceive an unsuspecting target into providing valuable information, such as an account number, card number, CVV number, card expiration date, password/pin, Social Security number and other personally identifiable information. Once obtained, scammers use the information to generate, among other things, counterfeit ATM cards. Attackers may then generate a fictitious card and begin conducting fraudulent cash withdrawals, sometimes in as little as an hour. Credit unions can help fight this growing threat in the following ways:

- Educate your members about the potential threats related to this type of activity.
- Ensure card processing and fraud rule configurations are made to help reduce the likelihood counterfeit cards can be used.
- Work with law enforcement when the scam is actively occurring with your members.
- Ensure your cybersecurity incident response program, procedures and processes are up-to-date.

More information on smishing and cybersecurity can be found on the **Federal Financial Institutions Examination Council's (FFIEC) website.**

~~~~~~

Publication Deadlines

In order to meet the submission deadlines for the applicable issues of the Texas Register, it is necessary for the Department to establish the schedule shown below. Completed applications received after the deadline for the month cannot be published until the following month.

Publication Date	Application Deadline
February 2018	Friday, February 16
March 2018	Friday, March 16

~~~~~~

Applications Approved

Applications approved since **December 20, 2017** include:

Credit Union	Changes or Groups Added
Field of Membership – Approved:	
Cooperative Teachers CU (Tyler)	See Newsletter No. 10-17
Centex Citizens CU (Mexia)	See Newsletter No. 11-17
Baptist CU (San Antonio)	See Newsletter No. 11-17

Applications Approved (Continued)

Credit Union	Changes or Groups Added
Field of Membership – Withdrawn:	
Gulf CU (Groves)	See Newsletter No. 09-17
Articles of Incorporation Change – Approved:	
United Community CU (Galena Park)	See Newsletter No. 11-17

~~~~~~

Applications Received

The following applications were received and will be published in the **January 26, 2018** issue of the *Texas Register.*

Articles of Incorporation:

Employees Credit Union (Dallas) – The credit union is proposing to change its name to RelyOn Credit Union.

Merger or Consolidation:

An application was received from **Keystone Credit Union** (Tyler) seeking approval to merge with **First United Credit Union** (Tyler). Keystone Credit Union will be the surviving credit union.

Comments or a request for a meeting by any interested party relating to an application must be submitted in writing within 30 days from the date of this publication. Credit unions that wish to comment on any application must also complete a Notice of Protest form. The form may be obtained by contacting the Department at (512) 837-9236 or downloading the form at http://www.cud.texas.gov/page/bylaw-charter-applications. Any written comments must provide all information that the interested party wishes the Department to consider in evaluating the application. All information received will be weighed during consideration of the merits of an application. Comments or a request for a meeting should be addressed to the Texas Credit Union Department, 914 East Anderson Lane, Austin, Texas, 78752-1699.

This newsletter is produced monthly as a part of the Department's continued communication outreach with the credit unions it regulates. Delivery is generally provided by electronic notification of its availability on the Department's website.

Suggestions and comments concerning the newsletter or its content are welcomed.

~~~~~

To learn more about CUD click http://www.cud.texas.gov or contact us at 914 E. Anderson Lane, Austin, TX 78752