

## InfoSight Highlight

### Wire Transfers/Transportation of Currency

The Bank Secrecy Act requires credit unions to collect and retain certain information in connection with “funds transfers” of \$3,000 or more. The term “funds transfers” generally refers to wire transfers.

The BSA’s “Travel Rule” requires a credit union to include certain information in payment orders relating to transmittals of funds (mostly wires) of \$3,000 or more, whether or not currency is involved. In other words, certain information must “travel” with the wire. Funds transfers governed by Regulation E or the Automated Clearing House rules are **not** covered by the Travel Rule.

*Note: NACHA ACH rules require all international payments made via the ACH Network to be identified as International ACH Transactions using the Standard Entry Class (SEC) Code – IAT. The rules also require that all IAT payments include the specific data elements defined by the BSA’s “Travel Rule”.*

Under the Travel Rule, all “transmitter’s financial institutions” (generally speaking, the originating financial institution) must include and send the following in the transmittal order:

- The transmitter’s name, account number, and address;
- The identity of the transmitter’s financial institution;
- The amount of the transmittal order;
- The execution date of the transmittal order; **and**
- The identity of the recipient’s financial institution.

If received, the transmitter’s financial institution must also include the name, address, account number and any other specific identifier of the recipient. In addition, an intermediary financial institution must pass on all of the information it receives from a transmitter’s financial institution or the preceding intermediary financial institution.

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

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

## Compliance News

## InfoSight Compliance eNEWSLETTER January 27, 2017 Vol. 11, Issue 4

Created in partnership with the



Credit Union National Association

## Compliance Videos

### Q4 2016 Overview and Q1 2017 Changes Coming

In this [recent video](#), Glory LeDu reminds us of the regulatory changes that became effective in the 4<sup>th</sup> quarter of 2016 (which includes the DELAY of the DOL Overtime rules). Glory also provides a review of the changes effective in the 1<sup>st</sup> Quarter of 2017 including the updates to Member Business Lending and the new requirements for HMDA reporting for 2017. This also includes the updated threshold changes effective on 1/1/2017.

### Member Business Lending

[This video](#) provides the details you will need to know to comply with the NCUA’s

## Management Responsibilities for MBL

NCUA's new MBL rule became effective last week, and the NCUA has decided to take a closer look at the rule's new expectations for Board of Directors and Management responsibilities in Section 723.3.

### Board of Directors:

723.3 states that a federally insured credit union's board of directors must:

- Approve the loan policy;
- Ensure the credit union appropriately staffs its commercial lending program in compliance with 723.3(b); and
- Understand and remain informed about the nature and level of risk in the commercial loan portfolio, including its potential impact on the credit union's earnings and net worth.

The guidance provides a bit more detail on how the Board can satisfy these requirements. The Board must periodically reassess the loan policy, and it should be reviewed at least annually (more frequently if there are changes in portfolio performance or economic conditions). The board and senior management must also ensure that their commercial lending program is staffed with personnel that have the appropriate expertise in managing the type of commercial lending in which the credit union is engaged. For example, if a credit union is financing farm equipment or production expenses related to farming, it needs to have staff with experience in underwriting, servicing and managing risks associated with such agricultural loans. Lastly, to understand the nature and level of risk in the commercial loan portfolio, the board must receive periodic updates from credit union management on the performance of the commercial loan portfolio. The updates should include things like credit risk rating distribution and migration, loan growth, delinquencies, charge offs, workout activities, concentration by loan types, policy exceptions, watch list

Member Business Lending rules.

## Compliance Calendar

January, 2017

- January 29th, 2017: [5300 Call Report Due to NCUA](#)

February, 2017

- February 6th, 2017: [NCUA Charting and Field of Membership Manual](#)
- February 20th, 2017: President's Day - Federal Holiday

April, 2017

- April 10th, 2017: [Fiduciary Rule \(Department of Labor\) – Compliance date](#)
- April 30th, 2017: [5300 Call Report Due to NCUA](#)

May, 2017

- May 29th, 2017: Memorial Day - Federal Holiday

July, 2017

- July 4th, 2017: Independence Day - Federal Holiday

loans, status of individual loan review and other risk monitoring, and adherence to policy and regulations.

### **Senior Management:**

723.3(b) states that a federally insured credit union's executive officers responsible for overseeing the commercial lending function must:

- Understand the credit union's commercial activities;
- Have a comprehensive understanding of the role of commercial lending in the credit union's overall business model; and
- Establish risk management processes and controls necessary to safely conduct commercial lending activities.

The guidance notes that any staff involved in a CU's commercial loan program must have sufficient expertise in assessing and managing the types of risks associated with the type of commercial lending, and skills should be commensurate with each particular position and level of responsibility. The guidance goes into a bit more detail as to the expectations for those individuals at the manager level that are responsible for commercial lending.

Managers overseeing the commercial lending program should have demonstrated experience in the following:

- Overseeing commercial credit risk assessment and underwriting;
- Managing and administering a credit risk rating system;
- Managing a commercial loan portfolio and being held accountable for the risk in that portfolio; and
- Managing commercial lenders and other risk managers.

### **Qualified Lending Personnel:**

The MBL rule also requires credit unions to employ "qualified lending personnel" with experience in each of the following areas:

- July 30th, 2017: [5300 Call Report Due to NCUA](#)

September, 2017

- September 4th, 2017: Labor Day - Federal Holiday
- September 15th, 2017: [Same-day ACH \(NACHA\) – Phase 2 of the implementation period for the rule.](#)

October, 2017

- October 1st, 2017: [Prepaid Accounts under the Electronic Fund Transfer Act/Regulation E and the Truth In Lending Act/Regulation Z](#)
- October 3rd, 2017: [Military Lending Act for Credit Cards](#)

### **Compliance Training**

#### **Regulatory Compliance Training**

[Cybersecurity](#) – Intrusion threats and vulnerabilities (recorded webinar)

#### **CUNA AND CUNA Webinars**

CUNA offers hundreds of online training events that make it easy for you to learn

- Underwriting and processing for the types of commercial lending in which the CU is engaged;
- Overseeing and evaluating the performance of a commercial loan portfolio, including rating and quantifying risk through a credit risk rating system; and
- Conducting collection and loss mitigation activities for the types of commercial lending in which the CU is engaged.

The guidance goes on to say that examiners will evaluate staff experience primarily by focusing on the overall type and relevance of staff experience for those persons involved in the commercial loan program, with an emphasis on experience in commercial loan risk management. Specifically, credit unions should have qualified lending personnel with:

- Experience directly related to the specific types of commercial lending in which the CU is engaged;
- Demonstrated experience in conducting commercial credit analysis and evaluating the risk of a borrowing relationship using a credit risk rating system;
- Demonstrated experience in underwriting, processing, and conducting workout activities for the types of commercial lending in which the CU is engaged; and
- Knowledge of the legal documentation necessary to protect the CU from legal liability, and all relevant law and regulation impacting commercial lending activities.

So how does a credit union meet all the above experience requirements? Well, according to the guidance, a credit union has several options, including training and developing existing staff, hiring experienced professionals, or using a third party such as a CUSO or independent contractor. Which option a CU chooses will depend on a variety of factors particular to that CU's situation, however the guidance does state that it is generally not

right at your desk. Whether you are looking for a beginner course or want a comprehensive understanding on a specific topic, CUNA webinars, audio conferences and eSchools have what you need.

[Click here](#) for updates on compliance, operations, lending topics and more!

prudent for a CU with a newly adopted commercial lending policy to rely solely on training and developing existing staff, unless existing staff already possess the required experience. Additionally, if using a third party, a credit union must verify that the third party possesses the required experience, as the credit union is ultimately responsible for the services provided by the third party. Lastly, CUs must ensure that there are no potential conflicts of interest between a third party and any borrower or associated borrowers. All of these considerations should be taken into account when determining how to satisfy the experience requirements in 723.3.

For more information, see the MBL guidance in the online Examiner's Guide, available [here](#).

*Source: CUNA Compliance Blog*

---

### **Western Union pays \$586M for fraud and money laundering**

The Federal Trade Commission has [announced](#) that the Western Union Company, a global money services business headquartered in Englewood, Colorado, has agreed to forfeit \$586 million and enter into agreements with the Federal Trade Commission, the Justice Department, and the U.S. Attorneys' Offices of the Middle District of Pennsylvania, the Central District of California, the Eastern District of Pennsylvania and the Southern District of Florida. In its agreement with the Justice Department, Western Union admits to criminal violations including willfully failing to maintain an effective anti-money laundering program and aiding and abetting wire fraud. The forfeited money will fund restitution payments to consumers who were harmed by the company's unlawful actions.

In a related action, FinCEN [announced](#) it has issued a consent assessment of a civil money penalty of \$184 million against Western Union Financial Services, Inc. (WUFSI). WUFSI consented to FinCEN's determination that prior to 2012, WUFSI willfully violated the Bank Secrecy Act's anti-money laundering (AML) requirements by failing to implement and maintain an effective, risk-based AML program and by failing to file timely suspicious activity reports (SARs). FinCEN's penalty is in conjunction with the actions by the U.S. Department of

Justice (DOJ) and the U.S. Federal Trade Commission (FTC), and will be satisfied by Western Union's forfeiture to the U.S. Treasury.

*Source: Federal Trade Commission and FinCEN*

---

### **CFPB sues TCF National Bank for overdraft opt-in practices**

The Consumer Financial Protection Bureau has [announced](#) it brought suit against TCF National Bank, Sioux Falls, South Dakota (per FDIC records -- the CFPB press release lists the headquarters in Wayzata, Minnesota), for tricking consumers into costly overdraft services. The Bureau alleges that TCF designed its application process to obscure the fees and make overdraft service seem mandatory for new customers to open an account. The CFPB also believes that TCF adopted a loose definition of consent for existing customers in order to opt them into the service and pushed back on any customer who questioned the process. The lawsuit seeks redress for consumers, an injunction to prevent future violations, and a civil money penalty.

As described in the Bureau's [complaint](#), TCF relied on overdraft fee revenue more than most other banks its size and recognized early on that the opt-in rule could negatively impact its business. In late 2009, Bank management estimated that approximately \$182 million in annual revenue was "at risk" because of the opt-in rule. Through consumer testing, the bank determined that the less information it gave consumers about opting in, the more likely consumers would opt in.

The Bureau's complaint alleges that TCF's strategy also consisted of bonuses to branch staff who got consumers to sign on. For example, in 2010, branch managers at the larger branches could earn up to \$7,000 in bonuses for getting a high number of opt-ins on new checking accounts. After the bank phased out the bonuses, certain regional managers instituted opt-in goals for branch employees. Staff had to achieve extremely high opt-in rates of 80 percent or higher for all new accounts. While the bank's official policy was that an employee could not be terminated for low opt-in rates, many employees still believed they could lose their job if they did not meet their sales goals.

The Bureau alleges that the bank's strategy worked and that by mid-2014, about 66 percent of the bank's customers had opted in, a rate more than triple that of other banks. According to the Bureau's complaint, the chief executive officer of the bank even named his boat the "Overdraft." TCF's senior executives were so pleased with the bank's effectiveness at

convincing consumers to opt in that they had parties to celebrate reaching milestones, such as getting 500,000 consumers to sign up.

The Bureau's complaint alleges that TCF violated the Electronic Fund Transfer Act and the Dodd-Frank Wall Street Reform and Consumer Protection Act. TCF National Bank reported total assets of \$21 billion as of 9/30/16, with 360 retail branches across Minnesota, Wisconsin, Illinois, Michigan, Colorado, Arizona, and South Dakota.

---

### **Back-2-Basics: Responding to a Data Breach**

Cybersecurity remains a top priority for regulators and the entire financial services industry. The Federal Financial Institutions Examination Council (FFIEC) agencies introduced a [cybersecurity assessment tool](#) in 2015 to help institutions determine their level of cybersecurity preparedness. Use of the tool by credit unions is recommended but voluntary, [although it is being incorporated into NCUA's exam process later this year](#) (3rd or 4th Quarter 2017).

[Part 748 of NCUA's regulations](#) requires federally insured credit unions to develop and implement "risk-based" response programs to address "instances of unauthorized access to member information in member information systems" (i.e., data breach). "Member information systems" consist of "all of the methods used to access, collect, store, use, transmit, protect, or dispose of member information," including systems maintained by the credit union's service providers (12 CFR Part 748, Appendix A, Paragraph I.C.2.d.). Appendix B to Part 748 provides credit unions with direction on how to meet this regulatory requirement.

When a credit union becomes aware of an incident of unauthorized access to "sensitive member information" in member information systems, the institution is required to conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. Sensitive member information includes data such as a member's name, address, or telephone number used in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account; or any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or password and account number. The credit union's response program must also include procedures to notify members about incidents of unauthorized access to member information systems that



could result in substantial harm or inconvenience to the member (e.g., identity theft).

### Components of a response program

At a minimum, a credit union's response program should contain procedures for:

- Assessing the nature and scope of an incident, and identifying what member information systems and types of member information have been accessed or misused.
- Notifying the appropriate NCUA Regional Director, and, in the case of federally insured state-chartered credit unions, its applicable state supervisory authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of "sensitive" member information.
- Notifying appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report (SAR) in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is on-going.
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information (e.g., monitoring, freezing, or closing affected accounts) while preserving records and other evidence.
- Notifying members when warranted (i.e., the breach could result in substantial harm or inconvenience to the member).

Note that when an incident of unauthorized access to member information involves member information systems maintained by a contracted service provider(s), it is the credit union's responsibility to notify its members and regulator. However, a credit union may authorize or contract with its service provider to notify the credit union's members or regulators on its behalf.

Check out the following resources for more detailed information:

- [CUNA's e-Guide: Cybersecurity](#)
- [NCUA Cybersecurity Resources](#)
- [FFIEC Cybersecurity Assessment Tool](#)
- [FFIEC Cybersecurity Assessment Tool Frequently Asked Questions](#)

*Source: CU Compliance Community*



### **Trump Administration Rescinds Order to Cut FHA Insurance Premiums**

In one of the new Administration's first actions, the Department of Housing and Urban Development (HUD) announced Saturday that a cut in Federal Housing Administration (FHA) mortgage insurance premiums scheduled to go into effect January 27 would not happen as planned. FHA assesses these premiums to insure these government-backed mortgages, particularly for first time and low income homebuyers, against default.

Whereas the FHA had argued the premium cuts, which could affect between 750,000 and 850,000 borrowers, according to estimates by the National Association of Realtors, were warranted given the strengthened capital position of the FHA insurance fund, there is concern in some circles that the FHA's share of new mortgages has grown too large, potentially crowding out private investment. HUD's move to rescind the cuts could be seen as an attempt to help rebalance the market.

As with the guarantee or "G" fees charged by government sponsored enterprises Fannie and Freddie to protect investors against default, CUNA has long argued that FHA insurance premiums should be set at a level that naturally reflects the aggregate risk to government backers of mortgages. We will continue to monitor the health of these entities and the broader mortgage market, and advocate for an appropriate balance between protecting taxpayers and ensuring adequate and equitable access to mortgage credit for credit union members.

---

### **Supplemental Capital and Public Funds Bills Pending in Washington**

At the behest of the Northwest Credit Union Association, Washington lawmakers are considering H 1318, which would permit state-chartered credit unions to accept supplemental capital immediately upon a change at the Federal level. Supplemental capital, which is also known as alternative capital, represents the portion of a credit union's assets which is uncommitted and therefore available to cover losses. The Federal Credit Union Act requires all federally insured credit unions, including state-chartered credit unions, to rely on retained earnings to build net worth. Credit unions designated as low income can accept supplemental capital, however. If the Federal Credit Union Act is amended and H 1318 is enacted, Washington's federally insured credit unions would be permitted to access alternative capital which would enhance their safety

and soundness by providing them with a cushion to absorb operating losses and asset write-downs during economic downturns. Supplemental capital would also enhance the ability of Washington credit unions to serve their members by taking deposits, making loans, opening new branch locations and expanding service offerings for members.

Another league-supported Washington bill, H 1209, would create conditions for the state's credit unions to accept public deposits that exceed the maximum deposit insured by the national credit union share insurance fund. Public deposits are public funds deposited in a financial institution by the treasurer of a state or local government, or any agency thereof. State and local governments deposit billions of dollars in financial institutions, primarily in banks. However, Washington is one of the 25 states that permits credit unions to accept public deposits and permits government entities to deposit public funds in credit unions.

---

### **Lawmakers Ponder Bills Impacting Credit Unions in Nebraska and in New Mexico**

This week, bills were introduced in Nebraska and New Mexico that would positively impact the ability of credit unions to serve their members.

The Nebraska League spearheaded the introduction of four bills that would create a flexible operating environment for the state's credit unions. If L 375 is enacted, credit unions would be permitted to purchase the assets and liabilities of other financial institutions and to grant joint account holders full memberships. A Nebraska field of membership bill, L 582, would add "persons within a well-defined geographical boundary" to the list of common bonds for credit union memberships. Another measure, L 454, would permit state chartered credit unions to opt-out of the state's loan officer license application requirement. An amendment to the Nebraska Real Estate Licensing Act, L 208, would list credit unions as permissible depositories for real estate trust accounts for real estate brokers.

The Data Breach Notification Act, H 15, was introduced in New Mexico. The measure would require:

- Notification to persons affected by breaches within 30 days
- Storage and disposal of personal information in a secure manner

- Notification to credit agencies, the attorney general and card processors

The bill would also permit civil penalties for violations of the Act. New Mexico is one of three states that does not have a data breach notification law. The other two states are Alabama and South Dakota.

*Source: CUNA Advocacy*

---

### **CUNA Advocacy Update**

The [CUNA Advocacy Update](#) is published at the beginning of every week and 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. Additional Advocacy efforts may also be found under CUNA's [Removing Barriers](#) blog.

---

### **ComplySight: 30 Day Free Trial!**

League InfoSight is offering a free, 30-day trial of ComplySight so you can see the benefits first hand. It's easy to get started. [Just visit us online.](#)

### **FREE Webinars on ComplySight, the League's latest compliance resource**

Registration is now open for your front row seat to learn about ComplySight, League InfoSight's newest addition to your compliance toolbox. If you're looking for a solution to the compliance tidal wave, this system is for you!

### ***RECORDED WEBINARS – Available ANY Time!***

For “recorded” webinars, click on the title of the webinar to listen. Users may be asked to download WebEx, which is a safe download for viewing the webinars. These are also available on the Dashboard in ComplySight and are available 24/7!

### [Introduction to ComplySight](#)

Designed to introduce and show the many features and benefits of ComplySight.

### [ComplySight Training & Tips – Where to Start?](#)

This webinar will: suggest a starting point as a new ComplySight user, discuss how Factor Grading works, review the Action Item Build/Edit process, and discuss the need for a compliance management tool that regulators - and you - will appreciate.

### [ComplySight Training & Tips – Regulatory Alerts, Assigning Employees, Preview of L2.5, Tools in the Help Area](#)

What should be done when you get an email about a Regulatory Alert? Where are “old” Regulatory Alerts? How do I assign an employee to an Area, and what will be different with the upcoming Level 2.5? And – what tools are available in the Help area? This webinar will explore all of this – and more!

### [ComplySight Training & Tips – How to Export Data](#)

When you need to archive or copy data out of ComplySight for a fresh start or to provide information for a Board meeting, this webinar will explain the process.

### [ComplySight Training & Tips – Reports in ComplySight](#)

What information is contained on the reports in ComplySight and how are they used?

### [Factor Selection Navigation Screens](#)

To simplify the ability to access Factor Grading screens and Item information, the Factor Selection screens have been redesigned. Check out this short webinar for details!

### [Access Level 2.5 and How to Use It](#)

Introducing the newest access level, allowing the L1 Administrator to set L2.5 access and then assign specific Areas that only that user may review.