

## InfoSight Highlight

### Same Day ACH

In 2016, NACHA and the Federal Reserve Board amended their operating rules to support Same Day ACH payments.

The rule will enable ACH originating depository financial institutions (ODFIs) that want to utilize same-day processing the option to send same-day ACH transactions to accounts at any receiving depository financial institution (RDFI). Offering same-day ACH products and services will be optional for ODFIs, but receipt of same-day entries will be required for RDFIs.

Besides requiring mandatory participation by RDFIs, the rule requires an interbank fee paid by the ODFI to the RDFI for each same-day ACH forward transaction. The fee will allow RDFIs to recover some of their costs for enabling and supporting mandatory receipt of same-day ACH transactions. The interbank fee is set at \$0.052 cents per transaction.

ODFIs will be able to submit files of same-day ACH payments through two new clearing windows provided by the ACH Operators:

- A morning submission deadline at 10:30 a.m. (ET), with settlement occurring at 1 p.m. (ET); and
- An afternoon submission deadline at 2:45 p.m. (ET), with settlement occurring at 5 p.m. (ET)

Virtually all types of ACH payments, including both credits and debits, will be eligible for same-day processing. Only international ACH transactions (IATs) and high-value transactions above \$25,000 will not be eligible.

[Click here to view the topic](#), and to ensure your credit union is in compliance.

## Compliance News

### Caution on prospective Venezuelan digital currency

OFAC has posted a new [Frequently Asked Question](#) relating to a December 2017 announcement by Venezuelan President Nicolas Maduro of plans for the Venezuelan government to launch a digital currency. Because the proposed currency would reportedly carry rights to receive commodities in specified quantities at a later date, OFAC has determined

## InfoSight Compliance eNEWSLETTER January 26, 2018 Vol. 12, Issue 4

Created in partnership with the



Credit Union National  
Association

## Compliance Videos

### Compliance Outlook for Q4 2017

In this video, Glory LeDu provides a [brief summary of the key changes of the new HMDA rules](#) becoming effective in January. You won't want to miss this important overview!

Just a reminder that Compliance videos since 2016 can be found on YouTube at [the Compliance Connection channel](#), where they are generally updated quarterly.

## Compliance Calendar

January, 2018

- January 28th, 2018: [5300 Call Report Due to NCUA](#)

February, 2018

that the currency would appear to be an extension of credit to the Venezuelan government, and U.S. persons that deal in the prospective Venezuelan digital currency may be exposed to U.S. sanctions risk.

Source: [Treasury.gov](https://www.treasury.gov)

### Detecting and Preventing Ransomware Starts with Four Key Steps

Ransomware is a type of trojan—malware designed to provide unauthorized, remote access to a user’s computer—that was first seen in 1989 and dubbed the AIDS Trojan. The original infection was found on floppy disks that were handed out at a conference. Once the user’s machine was infected, the trojan laid in wait counting the number of times the machine rebooted. Once the machine hit 90 reboots, malware hid the directories and encrypted the names of the files. The ransom demand for a “licensing fee” of \$189 was to be paid using the twentieth century, black-box equivalent of bitcoin—by sending money to a Panamanian P.O. Box.

With the proliferation of the internet, ransomware has expanded. However, the method of infection today remains the same as it did in the original AIDS Trojan of the late 1980s. After encrypting files or directories following a phishing attack, the perpetrator seeks a ransom usually in the form of a virtual currency like bitcoin. Increasingly, however, ransomware perpetrators only partially unlock files in an effort to extract an even larger payment, or simply keep the money and never provide the key.

Recent changes to the ransomware model have incorporated a worm that allows the infection to spread through peer-to-peer computer networks, as in the case with the recent WannaCry virus. Here, attackers used exploits exposed by the ShadowBrokers hacker network to infect even larger numbers of machines.

What hasn’t changed though is that it is still possible to detect and prevent an attack using the following methods. Here are four ways you can better protect your credit union from ransomware:

- **Monitoring**—Researchers have found that when ransomware attacks, there is a significant amount of changes to the file system. By monitoring the system-file logs, you can detect the creation, encryption or deletion of files.
- **Behavior Analytics**—Endpoint solutions, like virus protection, can’t block unknown ransomware variants so it is best to move to user behavior analytics. Baseline normal user activity and setting

- February 19th, 2018: President's Day - Federal Holiday

March, 2018

- March 16th, 2018: [Same-day ACH \(NACHA\) – Phase 3 of the implementation period for the rule.](#)

April, 2018

- April 1st, 2018: [Prepaid Accounts under the Electronic Fund Transfer Act/Regulation E and the Truth In Lending Act/Regulation Z \(Date Extended\)](#)
- April 29th, 2018: [5300 Call Report Due to NCUA](#)

May, 2018

- May 11th, 2018: [Customer Due Diligence – CDD \(FinCEN\) – Effective date](#)
- May 28th, 2018: Memorial Day - Federal Holiday

July, 2018

- July 4th, 2018: Independence Day - Federal Holiday

up a tripwire to find variances will enable you to catch the infection in near real time.

- **Honeypots**—Create honeypots. Since it is quicker and, often more cost effective, to encrypt recently accessed files in a ransomware attack, creating a fake file repository will often lure the ransomware into encrypting those files and allow you to enact your security measures. This can also help if you don't have the resources to monitor file access activity.
- **Access controls**—Getting rid of global access groups from your IT network's access controls can greatly reduce the ability of the virus to spread. These access groups are known as "open shares," and open to misuse.

Additionally, if you find yourself a victim of ransomware, the first thing is to go to law enforcement. You will often find that you are not alone, and there may be a known decryption system available for the specific ransomware that you are facing. Also, there are many decryption tools on the market, and often these are built into your security software suite or available online for free.

Credit unions can find additional information and resources on NCUA's Cybersecurity Resource Center to help them be better protected against ransomware and other cyber threats. Go to NCUA's [Cybersecurity Resource Center](#) for additional information.

Source: NCUA

### Advocacy Highlight

#### CUNA Advocacy Related to ADA Threats

Nearly 1,000 credit union stakeholders tuned into to CUNA's members-only webinar on website accessibility under the Americans with Disabilities Act (ADA) Thursday. For those unable to attend, [Click here to register and view the recorded webinar](#).

Credit unions have been facing increasing legal threats due to uncertainty over the ADA's application to websites. One potential solution is for credit unions to ensure their websites are in compliance with Web Content Accessibility Guidelines (WCAG) 2.0.

"We're working hard to get the government to provide a resolution that helps all credit unions, but it's important to know, and this can't be over-emphasized, that the best thing a credit union can today to protect itself is to update your website to the WCAG 2.0 standards," said Ryan Donovan, CUNA's chief advocacy officer. "Frankly, a government solution may take

- July 29th, 2018: [5300 Call Report Due to NCUA](#)

September, 2018

- September 3rd, 2018: Labor Day - Federal Holiday

### Compliance Training

#### NCUA webinar on Credit Union Diversity

The NCUA presented a webinar on November 2, titled "What, Why and How: Credit Union Diversity." An [archived recording of the webinar](#) is available online. The webinar featured credit union board members and staff leaders from Municipal Credit Union, Brooklyn, New York, Self Help Credit Union, Durham, North Carolina, and North Side Community Federal Credit Union, Chicago, Illinois. The webinar also discussed how to use the NCUA's Voluntary Credit Union Diversity Self-Assessment tool. This 28-question checklist is designed to support credit unions' diversity efforts. All credit unions, but especially those with at least 100 employees, are encouraged to complete the checklist and submit it electronically to the NCUA's Office of Minority and Women Inclusion by Dec. 30.

a long time, but we believe if a credit union's website is WCAG 2.0 compliant the risk of being sued is reduced."

Leah Dempsey, CUNA senior director of advocacy and counsel, said credit unions are facing more than threats, as law firms have moved on to seeking litigation against credit unions they say are not in compliance.

"If you settle with one law firm, nothing precludes you from getting hit with another threat, from a different or even the same law firm," she said. "CUNA is looking for opportunities for our legal advocacy team to get involved, and we need to hear from you if those opportunities arise."

Jared Ihrig, CUNA's chief compliance officer, recommended credit unions conduct an ADA compliance audit of their websites and other digital content, post an accessibility statement on their websites and implement a long-term accessibility strategy among other strategies.

He pointed members to CUNA's [FAQ document](#) on ADA accessibility, eGuide on the ADA, and CUNA's Compliance Community.

Going forward, Donovan said this has become a top advocacy priority for CUNA, and it will continue its work with the House Judiciary Committee, Department of Justice and individual members of Congress to come up with a solution.

To date, CUNA has:

- Launched an ADA advocacy page earlier last week;
- Outlined concerns with the ADA lawsuits in several meetings with DOJ officials;
- Followed up with a letter highlighting those concerns;
- Backed a bill that would address these threats;
- Written to the House and Senate Judiciary Committees;
- Spearheaded efforts that resulted in 61 members of Congress raising ADA concerns in a letter to DOJ; and
- Scheduled a breakout session at this year's CUNA Governmental Affairs Conference with the latest developments, scheduled for Monday, Feb. 26 from 2:45 to 4 p.m. (ET).

*Source: CUNA*

---

**CUNA Advocacy Update**

## **CUNA and CUNA Webinars**

CUNA offers hundreds of online training events that make it easy for you to learn 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!](#)

## **CFPB'S Amendments to the Mortgage Servicing Rules Webinar (Recorded)**

Credit unions that service mortgage loans saw an increase in their servicing responsibilities in October 2017 and will see additional requirements take effect in April 2018. [Click here to register for this recorded webinar.](#)

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. To receive this update, click on “Get CUNA Updates” on the [CUNA Advocacy page](#). Additional Advocacy efforts may also be found under [CUNA’s Removing Barriers blog](#). With the recent updates to CUNA’s website, Advocacy information has also changed. To view recent advocacy issues and see ways your credit union can become involved, visit the [Priorities](#) or [Actions](#) pages.

---

### **NEW COMPLYSIGHT TRAINING VIDEOS ARE NOW AVAILABLE**

We are happy to announce that our training webinars have been updated! We have created a video series with shorter segments to help our users get the most out of ComplySight! These video tutorials are available 24/7!

We have created **seven** new video tutorials ranging in length from 5 to 23 minutes:

- ComplySight Overview and Set Up
- Set Up and Manage Users
- Assigning Compliance Reviews
- Factor Grading
- Automatic Action Items (AAI) and Manual Action Items (MAI)
- Examiner/Audit Findings
- Regulatory Alerts

To access the tutorials, log into ComplySight and click on the “Help” page, then choose “Video Tutorials.” We are also in the process of revising our User Guide, so be sure to keep an eye out for those changes too. If you have any questions, please feel free to contact [info@complysight.com](mailto:info@complysight.com).

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

If you’re interested in a “trial run” of ComplySight, League InfoSight is offering a free, 30-day trial so you can see the benefits first-hand. It’s easy to get started. [Just visit us online and click on Free Trial Offer.](#)