

## Regulatory Compliance News



**MOUNTAIN WEST**  
Credit Union Association

November 6, 2015

### Compliance News

#### CFPB Penalizes Employment Background Screening Providers for Inaccuracies

The Consumer Financial Protection Bureau has [announced](#) it has taken action against two of the largest employment background screening report providers—General Information Services (GIS) and its affiliate, e-Background-checks.com, Inc. (BGC)—for failing to take basic steps to assure the information reported about job applicants was accurate. The CFPB is ordering the companies to correct their practices, provide \$10.5 million in relief to harmed consumers, and pay a \$2.5 million civil penalty.

The CFPB found that GIS and BGC violated the Fair Credit Reporting Act by, among other things, failing to employ reasonable procedures to assure the maximum possible accuracy of the information contained in reports provided to consumers' potential employers.

*Source: CFPB*

#### Telephone Consumer Protection Act (TCPA) – Guidance from CUNA

A recent (June, 2015) [ruling](#) by the FCC regarding the Telephone Consumer Protection Act (TCPA) continues to prompt questions regarding its interpretation. Below are several resources that may provide assistance and answer many questions:

[How will FCC's TCPA Ruling Affect Credit Unions?](#)

[What's an Autodialer?](#)

[TCPA Prior Express Consent Rules](#)

[TCPA Exemptions?](#)

*Source: CUNA*

#### Credit Unions Can Learn How FFIEC Cybersecurity Assessment Tool Works

Credit unions now have another resource from the National Credit Union Administration to help them use the Federal Financial Institutions Examination Council's [cybersecurity assessment tool](#) to evaluate their ability to address cyber risks.

The video, available [here](#), provides an overview of how the assessment tool works. The assessment tool can help credit unions pinpoint strengths and weaknesses in their cyber security programs.

"The increasing volume and sophistication of cyber threats pose real risks to the credit union system," NCUA Board Chairman Debbie Matz said. "NCUA has created this new video to supplement the online information found on our Cyber Security Resources webpage and to encourage credit unions to take steps to identify, assess and mitigate risks. Cyber security continues to be a core focus for NCUA, and I encourage all credit unions to

### Your Credit Union's Regulatory Compliance Support Staff

#### Mark Robey

**Sr. VP of Regulatory Affairs**

Phone: 800-477-1697, ext. 3327

Direct: 720-479-3327

#### Melia Heimbuck

**Director of Compliance Operations**

Phone: 800-477-1697, ext. 3325

Direct: 720-479-3325

#### Julie Kappenman

**Director of Association Compliance Services**

Phone: 800-477-1697, ext. 3324

Direct: 720-479-3324

#### Donna Gibbs

**Coordinator Association Services/Compliance**

Phone: 800-477-1697, ext. 3281

Direct: 720-479-3281

### Association Compliance Forums

Click on one of the below links to subscribe

[Compliance Forum](#)

[BSA Compliance Officer Forum](#)

Please provide the subscriber's name, credit union, title and email address. The subscriber will receive a welcome e-mail that details how to access the forum.



### What's New at AffirmX

Since launching its revolutionary Risk Intel Center platform a few years ago, AffirmX has continued to enhance its patented solution based on user input and to meet ever-expanding regulatory requirements. If you're unfamiliar with AffirmX's innovative solution, or if it has been awhile since you've seen what it can do, here is your chance to get quickly up to speed on how it can help your financial institution reduce workloads,

take steps to protect themselves, their members and the entire financial system.”

The FFIEC’s cybersecurity assessment tool is designed to enhance cyber security oversight and management capabilities, identify gaps in risk management practices and inform associated risk management strategies. The assessment tool is meant to be an enterprise-wide risk management tool that credit unions can use and revisit periodically as significant technological changes occur.

The video also directs credit unions to the [FFIEC webpage](#) for additional resources like joint statements, webinars and other information about cyber security.

*Source: NCUA*

## 10 Data Security Lessons of 2015

Protecting payment card data is a never-ending struggle, and the fraudsters are only getting more creative. So far this year several incidents and studies have demonstrated the evolving nature of cybercrime.

**Data Doesn't Disappear.** Ashley Madison, a dating site for cheaters, made a promise it couldn't keep: It said that it could delete users' data without a trace (for a fee) if they choose to leave the site. But its breach proved the data was still out there, and this is a problem other companies face with containing payment data as well.

**Crime Never Stops.** After a massive data breach in 2008 prompted Heartland Payment Systems to scour its systems for any previously overlooked vulnerabilities, the payment processor still wasn't able to shore up its defenses completely. This year, it dealt with a different kind of breach — a physical burglary, in which four computers were stolen from a payroll office. The machines might have contained personal data of 2,200 people.

**Fingerprints Don't Do Enough.** Apple popularized the use of fingerprint authentication for mobile devices and payments, but even its Touch ID system isn't foolproof. Phones protected with Touch ID can still be unlocked with a PIN, so Apple plans to raise the minimum PIN length to six characters when it updates iOS this year.

**A Small Breach is a Big Deal.** There's no such thing anymore as a breach that is too small to report, which is why Vermont's Attorney General stepped in when the 17 victims of a breach at Embassy Suites did not receive notification of the incident within the timeframe mandated by the state.

**Glitches Make Headlines.** The so-called glitchfest, a series of tech outages affecting an airline, a newspaper and the New York Stock Exchange, raised red flags throughout the financial services industry. Though the problems were chalked up to coincidence, regulators still took notice and reached out to banks to check in. Those banks had to make sure they had a plan in place in case something nefarious was going on.

**PCI Compliance is Hard to Hold.** Staying compliant with the Payment Card Industry data security standard is tough work; Verizon's 2015 report on PCI trends found that less than a third of companies overall are found to be fully PCI-compliant less than a year after a successful validation. Richard Moulds, vice president of product strategy at Thales e-Security, put it

anxieties and costs.

This webinar will cover:

- The six top features of the Risk Intel Center, including two new features clients love
- An overview of the new compliance solution option called AffirmX Lite
- An introduction of the new Vendor Management Module

For your convenience, this one-hour webinar will be offered at your choice of two times – register below.

[November 17 -- 11am – Noon Eastern](#)

[November 19 – 2pm – 3pm Eastern](#)

For more information about our compliance services, please contact Melia Heimbeck at: [mheimbeck@mwcua.com](mailto:mheimbeck@mwcua.com) or (720) 479-3325 or 1 (800) 477-1697 ext. 3325



## InfoSight Highlight

### Truth in Lending

Many changes were made to InfoSight as a result of the recent TILA-RESPA Integrated Disclosure requirements, effective in October, 2015. This highlights one of the changed topics.

The purpose of the Truth in Lending Act (Act), implemented by Regulation Z, is to promote the informed use of consumer credit by requiring disclosures about its terms and costs in clear and conspicuous disclosures. The Act has evolved into an extremely complex set of rules.

The Act provides members with the ability to shop for the best credit available by:

- Requiring lenders to make disclosures about the terms and cost of credit;
- Giving members the right to cancel certain credit transactions within three days if the borrowers principal residence is used as collateral;
- Regulating credit card practices and providing for timely resolution of credit billing disputes; **and**
- Imposing limitations on certain home equity transactions.

The Act applies to credit offered or extended to a consumer primarily for personal, family or household purposes. It also applies to all creditors who regularly extend credit that is either subject to a finance charge or is payable in more than four (4) installments. The Act divides consumer loans into two categories: open-

bluntly: "Companies fall out of compliance almost instantly upon achieving it."

**Mind the Basics.** Even as the payments industry pushes the addition of EMV and tokenization technology, many companies are still failing to cover the basics, Visa's risk chief Ellen Richey says. For example, many professionals are not changing the default passwords on sensitive systems, she warns.

**Physical Security for Digital Systems.** Just because a system is digital doesn't mean that firewalls and encryption are the best tools to defend it. "You could have the most secure bank in the world with locked doors, three-foot thick fences and gates that come down at night, but they still have an alarm inside of it," said Javelin analyst Al Pascual. There are software-based alarm systems that can alert a company when a cyber-intruder inevitably gets through its defenses.

**Consumers Can Help....** With mobile banking apps, consumers can manage any aspect of their accounts on the go. They can limit their card's spending to certain merchant categories or temporarily shut the card off entirely if it gets misplaced. If a bank wanted to, it could even use these tools to place the liability for fraud on the consumer — thus giving the consumer an incentive to use these anti-fraud tools proactively.

**...But Don't Count on Them.** Even with consumers holding new anti-fraud capabilities in their hands, they won't have the expertise of a security professional. Consumers make bad assumptions about their security, which is why phishing scams still work.

*Source: Payments Source*

## Advocacy Highlight

### 2016 CUNA GAC – The Biggest CU Advocacy Event of the Year

February 21-25, 2016 • Washington, D.C.

CUNA Governmental Affairs Conference is the largest gathering of credit union advocates rallying on behalf of America's more than 103 million credit union members.

Join thousands of credit union leaders to leverage the power of our united system and share credit unions' positive impact with lawmakers from all 50 states.

Click [here](#) to register and get more information.

### Major Cybersecurity Bill Clears Senate

The Senate approved a key cybersecurity bill after several days of debate on the chamber floor — and several years of lobbying by business groups, including bankers.

The Cybersecurity Information Sharing Act would make it easier for the private sector and government to share cyber threat information. The bipartisan legislation failed to advance on the floor several times earlier this year before this latest effort, which kicked off last week. The legislation is a victory for the banking industry and other firms, in part because it provides certain liability protections for companies passing along data about potential attacks. The bill passed the Senate 74-21.

The House passed similar information sharing legislation this past spring.

end credit which typically includes personal lines of credit, credit card accounts, and home equity lines of credit and closed-end credit such as most automobile loans and mortgage loans.

Regulation Z rules do **not** apply to the following:

- Business, commercial, agricultural or organizational credit; or
- Credit over \$54,600 for 2015 (adjusted each January based on the Consumer Price Index for Wage Earners and Clerical Workers) **unless**, the extension of credit is secured by real property or personal property used or expected to be used as the principal dwelling of the member or a **private** education loan (i.e., those that are **not** made, insured, or guaranteed pursuant to a program authorized by title IV of the Higher Education Act of 1965).

In this summary, the word "member" is substituted for the word "consumer" as used by Regulation Z; and "credit union" is substituted in most cases for "creditor."

[InfoSight \(AZ, CO, WY\)](#)



## Compliance Calendar

### October 23

- ♦ 5300 Call Report Due to NCUA

### November 11

- ♦ Veterans Day - Federal Holiday

### November 26

- ♦ Thanksgiving Day – Federal Holiday

### December 25

- ♦ Christmas Day – Federal Holiday

### December 31

- ♦ Foreign Account Tax Compliance Act Effective Date

## Effective Dates New and Revised Rules

### December 31, 2015~IRS

["Foreign Account Tax Compliance Act" \(FATCA\) Rule](#)

## CUNA Comment Calls – Due Dates on Proposed Rules

The two chambers are now expected to try and hash out a number of sticky details in a bicameral conference, including which agency should oversee the information sharing process. Observers have suggested it's unlikely the House will take up the Senate legislation as it stands.

Industry groups praised the Senate's passage of the bill, but said they are hoping to make changes when the legislation goes to conference.

"Importantly, while we are supportive of the process moving forward to a conference, SIFMA does have serious concerns with language adopted during the Senate process which would give an outsize and inappropriate role to the Department of Homeland Security in making information sharing determinations and could lead to burdensome regulation that would undermine the voluntary nature of CISA, which is at its core," said Ken Bentsen, the president and CEO of SIFMA. "We strongly urge the Conference Committee to strike this provision."

*Source: Payments Source*



The [CUNA Regulatory Advocacy Report](#) 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.

## CUNA Schools and Webinars

### November 19

Webinar: [Identify Interest Rate and Market Risk](#)

### December 17

Webinar: [Managing Credit Risk](#)

### October 19, 2015~CFPB

[Request to Develop Survey on POS/ATM Overdraft Disclosure](#)

### November 19, 2015~NCUA

[Investment & Deposit Activities – Bank Notes](#)



## [Training & Events Calendar](#)

### November 9

Webinar: [Preparing for the Impact of Same Day ACH](#)

### November 12

Webinar: [Regulatory Requirements for the Board & Senior Management](#)

### November 24

Webinar: [Top 10 Mistakes in Deposit Compliance Exams](#)

### December 3

Webinar: [Advanced ACH Specialist Series: Reg E Error Resolution Rules vs NACHA Operating Rules – Obligations, Consumer Disputes & Case Studies](#)

### December 9

Webinar: [BSA Special Risks: Policy, Law Enforcement & Regulator Issues](#)

### December 14

Webinar: [Revised TRID Mortgage Exam Procedures: Reviewing September 15, 2015 Changes](#)

### December 15

Webinar: [Robbery Prevention, Apprehension & Recovery](#)

Please respond to [Mark Robey](#) with any questions or concerns regarding content of this newsletter.

Sign up to receive Regulatory Compliance News by sending an email to [Donna Gibbs](#).

Archived Regulatory Compliance Newsletters can be accessed [here](#) or on our website [www.mwcua.com](http://www.mwcua.com) – Compliance News.

If you're having trouble viewing content, please check your viewer's settings.