TILA-RESPA Integrated Disclosure Rule

With one of the most sweeping regulatory changes for credit unions in decades less than one month away, MWCUA is dedicated to helping you prepare. Each week we will present a topic, question, or idea taking you one step closer to successful implementation.

29

Days until
October 3, 2015

Does your training include consumer complaint tracking, processing, correcting, and responding?

Regulatory Compliance News

MOUNTAIN WEST
Credit Union Association

September 4, 2015

Compliance News

Court Affirms FTC Authority on Cybersecurity Issues

(8/26/15) A Third Circuit U.S. Court of Appeals panel of judges ruled Aug. 24 that the FTC could proceed with its lawsuit against hotel chain Wyndham Worldwide Corp. The suit claims the company violated the FTC Act's unfair business practice provisions when it took inadequate security measures to protect consumer data. As a result, the FTC claims, Wyndham had data breaches that between 2008 and 2009 exposed more than 619,000 payment cards and other consumer information.

Legal experts say the court's decision essentially affirms the FTC's right to oversee and fine U.S. companies for cybersecurity missteps that result in the compromise of personal information and payment.
Based on the court's decision, "it is even clearer that the FTC is the leading agency in the U.S. for data breach matters," says cybersecurity attorney Chris Pierson, who serves as chief security officer of payments provider Viewpost. "Challenging the FTC's authority to regulate unfair/deceptive acts and practices is unlikely to be fruitful in court. The Wyndham case is a seminal case for the FTC for the proposition that the FTC has the power and ability to oversee cybersecurity breach issues as the nation's default regulator."

In a research note, threat-intelligence firm iSight Partners says the ruling reinforces the FTC's authority to punish organizations that fail to take adequate steps to ensure user security. "This creates additional financial risk for enterprises that elect not to make cybersecurity a priority, theoretically pushing organizations to enact effective security policies," according to the research note. "The FTC has provided some resources and guidelines for cybersecurity, and may seek to establish a structure or system for issuing fines in the future."

Other FTC Actions

In addition to its ongoing case against Wyndham, a final FTC ruling is pending in its longstanding breach-related cybersecurity case against medical testing

Compliance Team

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.

company LabMD. And in July, the FTC charged ID theft protection firm LifeLock with deception, claiming the company violated a 2010 settlement with the commission and 35 state attorneys general by continuing to make deceptive claims about its ID theft protection services and failing to take steps to protect users' data.

Privacy attorney Kirk Nahra of the law firm Wiley Rein says the Wyndham ruling could hurt LabMD's case, because the court has now made it clear that the FTC does have the authority to regulate cybersecurity. LabMD has argued, in part, that the FTC does not have jurisdiction.

What the Wyndham case does not make clear, however, is whether the FTC can fine and sue breached businesses that are regulated by other agencies, Nahra adds. "The Wyndham case doesn't address that issue at all, and I can't even try to guess how a court would [rule] based on the Wyndham decision," he says.

Attorney Adam Greene, a partner at law firm Davis Wright and Tremaine in Washington, says the Wyndham ruling leaves many questions about how the FTC will regulate cybersecurity going forward. "The ruling means that entities will need to read the FTC tea leaves to best discern what is 'reasonable' security, as the court did not hold that the FTC has to set forth more specific standards," he says.

And Matt Franko, a senior management consultant at forensics and security assessment firm SecureState, contends that giving more government agencies authority to oversee corporate cybersecurity, as the Wyndham ruling does, won't be good for business.

"The government seems to be allowing all industries to govern themselves, until they prove they cannot get their own houses in order," Franko says. "Now they're stepping in, with the courts' help, and levying fines and lawsuits in attempt to rectify the situation." For additional information, please see this article.

Source: CU Info Security

12 Red Flags for "Funnel Accounts" Used to Launder Money

Regulatory and law enforcement agencies are cautioning financial institutions about an increased use of illegal funnel accounts to launder proceeds from human smuggling, human trafficking and drug trafficking crimes. In light of the recent attention on this money laundering trend, I thought it would be useful to provide a brief overview of funnel accounts and how they are used to launder criminal proceeds.

What is a "funnel account"?

A funnel account (sometimes referred to as an interstate funnel account) is a method used to launder money that exploits branch networks of financial institutions. It involves illegal funds deposited into an account at one geographic location that gives criminals immediate access to the money via withdrawals in a different geographic location. The transaction amounts are kept under the AML reporting requirements in an attempt to avoid detection.

How Criminal Enterprises Use Funnel Accounts

Funnel accounts are opened by criminal organizations in the geographic area where the funds will be withdrawn, often locations along the southwest border of the U.S. The criminal organization provides the account number to co-conspirators around the U.S. who make cash deposits into the account from various geographic locations. The illicit funds are then immediately available for withdrawal by the criminal organization in the state in which the account was opened.

InfoSight Highlight

NCUA Advertising Signage Requirements

The credit union will follow the NCUA advertising rules in all its advertisements. All credit union advertisements or promotions will include either the NCUA's official advertisement sign or an abbreviated statement.

NCUA Advertising Statement

The credit union can choose either of the following options to comply with this Regulation:

- *Statement:* "**This Credit Union is federally-insured by the National Credit Union Administration.**"
- *Short Statement (no longer requires accompanying "official sign"):* "**Federally Insured by NCUA**"; or
- *The Official Sign:* (note: if the NCUA official sign in the advertisement is so small that the NCUA's sign and the two lines of small type become indistinct, the credit union should use the NCUA official advertising statement, or the short statement instead.)

InfoSight (AZ, CO, WY)

CU Compliance Connection – Promoting a Culture of Compliance

In this video for Compliance Connection, Compliance Consultant Amy Wargo details how to set up a culture of compliance at your credit union. View the CUBE TV video here.

Advocacy Highlight

The Federal Trade Commission has extended the deadline for public comment on the proposed verifiable parental consent method that Riyo, Inc., has submitted for Commission approval under the agency's Children's Online Privacy Protection Rule.

Alien smuggling organizations (ASOs) often use funnel accounts to receive illicit proceeds from U.S. based family members of foreign nationals living in Mexico and Central America who pay "coyotes" to smuggle their relatives into the United States across the southwest border. Deposits into funnel accounts can occur anywhere in the U.S. since individuals making payments to smuggling organizations can live in any part of the country.

Red Flags Indicators for Funnel Accounts

U.S. Immigration and Customs Enforcement (ICE) recently featured the topic of funnel accounts in their publication *Cornerstone Report* and provided the red flags listed below as potential indicators of this type of money laundering scheme.

- Account(s) with multiple deposits which are shortly transferred to other accounts
- Accounts with high aggregate dollar deposit activity but with low account balances
- Accounts with deposits from multiple, different individuals or companies
- Accounts with multiple deposits from multiple locations outside the banking area
- Accounts with multiple deposits from multiple sources (e.g., cash, ATM deposits, checks, wire transfers, etc.)
- Accounts opened in the U.S., by individuals temporarily within the U.S. who are bearing immigration identity documents (such as border crossing cards), then used to wire transfer funds back to Mexico
- Deposits are immediately (or within 1 to 2 days) withdrawn or wired from the account
- Accounts with an unusually high number of charge-backs
- Financial activity not commensurate with stated business or occupation of the depositing individual
- Anonymous cash deposits made in destination states [interior states] followed by rapid cash withdrawals made in source states [border states]
- Abrupt change in account activity
- Branch-shopping at various financial institutions to disguise nexus of the deposited funds with movements across the U.S. international borders.

Financial institutions would be well advised to incorporate these red flag indicators into their suspicious activity detection initiatives.

Source: Verifin

FTC Consumer Privacy Conference Announced

The Federal Trade Commission has announced it will host PrivacyCon, a conference examining cutting-edge research and trends in protecting consumer privacy and security, in Washington, DC on January 14, 2016. The event is the first of its kind and will bring together leading stakeholders, including whitehat researchers, academics, industry representatives, federal policymakers, consumer advocates and others. A PrivacyCon website has been established and more information will be posted at a later date.

Source: FTC

Register for OFAC Symposium

OFAC has opened the registration for its 2015 Fall Symposium to be held September 22 from 8 a.m. to 4 p.m. ET in Washington, D.C. Note that online registration does not automatically confirm attendance. A separate email will be sent containing registration status. Travel arrangements should not be made until a confirmation email is received.

Source: OFAC

Providing Sensitive Credit Union and Member Data to NCUA

ALEXANDRIA, Va. (8/27/15)--Recently updated examination procedures from the National Credit Union Administration are intended to strengthen safeguards for data received electronically during an examination.

The changes, detailed in a letter sent to credit union CEOs last week, are based

The deadline for comments has been extended from the original date of Sept. 3 to Sept. 14, 2015. Information for submitted comments is found in the Federal Register notice at the link below.

From the original notification on July 31, 2015: The Federal Trade Commission is seeking public comment on a proposed verifiable parental consent method that Riyo has submitted for Commission approval under the agency's Children's Online Privacy Protection Rule.

Under the rule, online sites and services directed at children must obtain permission from a child's parents before collecting personal information from that child. The rule lays out a number of acceptable methods for gaining parental consent, but also includes a provision allowing interested parties to submit new verifiable parental consent methods to the Commission for approval.

In a Federal Register notice to be published shortly, the FTC is seeking public comment about the proposed Riyo verifiable parental consent method including whether the proposed method is already covered by existing methods under the rule and whether it meets the rule's requirement that it be reasonably calculated to ensure that the person providing the consent is actually the child's parent. The Commission also seeks comment on whether the program poses a risk to consumers' information and whether that risk is outweighed by the benefits of the program.

Source: FTC

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
Credit Union National Association

Compliance Calendar

September 7

- Labor Day – Federal Holiday

September 18

- NACHA's Return Rate Levels & Reinstated Transactions Rule

October 3

- CFPB: Know Before You Owe Disclosure - Effective Date

October 3

- CFPB: Integrated Mortgage Disclosures - Effective Date

on recommendations the NCUA's Office of the Inspector General made in June.

The NCUA defines "sensitive data" as: information which by itself, or in combination with other information, could be used to cause harm to a credit union, credit union member or any other party external to the NCUA; and any information concerning a person or their account which is not public information, including any non-public personally identifiable information.

"In order to ensure sensitive electronic credit union and member data is well protected, the data held by NCUA needs to be encrypted," reads the letter, signed by Larry Fazio, director of the NCUA's Office of Examination and Insurance. "The process of exchanging this data between credit unions and examiners also needs to be secure and well controlled."

Effective immediately, NCUA examiners may only accept sensitive data electronically through:

- Secure electronic transmission or transfer by removable media, including encryption. The data files or the electronic transmission conveying the files must be encrypted. Encryption must have 128-bit encryption and the use of a strong password (minimum eight characters, mixture of upper- and lowercase letters, numerals and special characters). The password must be provided separately from the device or transmission; and

- In-person transfer by removable media not including encryption. If a credit union is unable or unwilling to provide data as mandated in the previous option, it may accept data if a credit union representative provides the data files to the examiner and remains physically present while the examiner transfers the data to the NCUA's encrypted equipment.

"The above protocols reflect the initial steps NCUA is taking to strengthen the safeguards for sensitive data received electronically from a credit union during an examination," the letter reads. "NCUA is in the process of acquiring a secure file transfer solution (such as an online portal) to facilitate examiner staff and credit unions securely and efficiently exchanging information."

Fazio added that agency aims to have such a solution in place early in 2016.

MOUNTAIN WEST Credit Union Association

Training & Events Calendar

Regulatory Compliance & BSA School

Be sure to mark your calendars for the Regulatory Compliance & BSA School. And, if you are tight on funds, professional development scholarships are available through Mountain West Credit Union Foundation. Click here to view the Scholarship Application.

September 9-10: Denver, CO
October 20-21: Phoenix, AZ

September 10

Webinar: Loan Concentration Management: Evaluation, Risk Tolerance & Regulatory Guidance

September 15

Webinar: Loan Underwriting Basics: Interviewing, Credit Reports, Debt Ratios & Regulation B

October 27

Webinar: Adverse Action Consumer & Mortgage Loan Best Practices

---

October 12

- Columbus Day – Federal Holiday

October 23

- 5300 Call Report Due to NCUA

November 1

- Daylight Savings Time Ends

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

CUNA Comment Calls – Due Dates on Proposed Rules

August 24, 2015~NCUA

Member Business Lending Rule

August 27, 2015~DOL

Department of Labor Proposal to Update Rules Concerning Overtime Pay

September 8, 2015~NCUA

NCUA's Economic Growth and Regulatory Paperwork Reduction Act (EGRPRA) Regulatory Review: No. 3

Effective Dates New and Revised Rules

October 1, 2015~DOD *(Compliance Mandatory 10/3/2016)*

Military Lending Act Rule

October 3, 2015~CFPB

TILA-RESPA Integrated Disclosure Rule

December 31, 2015~IRS

"Foreign Account Tax Compliance Act" (FATCA) Rule

CUNA Schools and Webinars

September 8 – October 7

CUNA Lending Compliance eSchool

September 10

Webinar: Custom Construction Lending – Technical Stuff, Best Practices and Red Flags

September 14

Webinar: Changes to the Military Lending Act

October 8

Compliance Networking Council –Registration is Open

Plan to attend the next Compliance Networking Council on Thursday, October 8, 2015. The Compliance Council brings together compliance professionals to discuss the challenges inherent in keeping credit unions compliant with the regulations that govern them. The council provides opportunities to meet with your counterparts from other credit unions, discuss upcoming regulatory changes, as well as strategies to minimize their impact. This council will take place in Denver, CO, Phoenix, AZ and Rock Springs, WY. For more information or to register, please e-mail: training@mwcua.com.

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