Issue 11 | October 2015

Network Compliance Teacher

Compliance News and Tips from Credit Union Compliance Officers
sponsored by CU*Answers AuditLink

In this Issue...

Editor's Corner

It is hard to believe that it is October already and with that brings many things. It's the beginning of a new fiscal year here at CU*Answers; summer comes to an end and brings us the beautiful fall season; and in many of our worlds, it's also audit season. Time to get those annual audits in before the year end. I know I will be busy on the road for the next couple months conducting a few of those audits, but before I do, it's time to get another Network Compliance Teacher published.

This edition has some great articles regarding Identity theft protection, the new credit card offsets under the Truth in Lending Act, loan participation and also a lesson on encrypting. Thank you to all that participated in this edition.

Marsha Sapino, AAP
AuditLink Associate
CU*Answers

Get Involved with the Network Compliance Teacher!

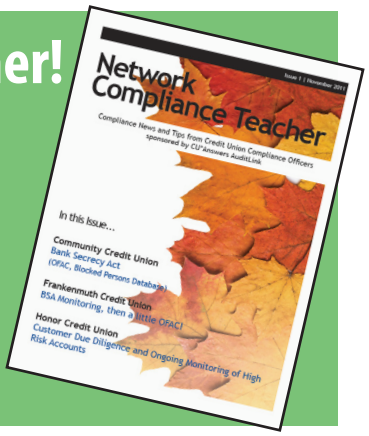
Have something to contribute?

Want to write an article for a future Network Compliance Teacher Issue?

Have a topic to suggest for a future issue?

We're looking for compliance officers like you to contribute!

Contact AuditLink at auditlink.cuanswers.com



The Network Compliance Teacher is a collaboration of compliance minded Credit Union Professionals like you from throughout the cuasterisk.com network.

Current and previous issues of The Network Compliance Teacher are available for download from the AuditLink website at http://auditlink.cuanswers.com.

AuditLink
CU*ANSWERS Management Services
6000 28th Street SE
Grand Rapids, MI 49525
(800) 327-3478
auditlink.cuanswers.com

Proud Member of the cuasterisk.com Network

Meeting NCUA Requirements for Encrypting Office and PDF Documents

Patrick Sickels
CU*Answers
Internal Auditor

On August 21, 2015, the NCUA sent a letter to credit unions Providing Sensitive Credit Union and Member Data to NCUA. This letter states that, unless protected, the NCUA will no longer accept sensitive from credit unions that is:

> "(1) any 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 NCUA, and (2) any information concerning a person or their account which is not public information, including any non-public personally identifiable information."

The information that could cause "harm to a credit union" might be disclosure of weak CAMEL ratings, for example. Other sensitive information would of course be member sensitive information, such as member account numbers and so forth.

The NCUA will only accept this information if it is transmitted securely, such as through Zix™ or other email encryption, or if the files are protected through data encryption that meets these minimum standards:

- "128-bit AES encryption
- Strong password (a minimum of eight characters; mixture of upper- and lower-case, numbers, and special characters; not easily guessable, etc.)
- Password must be provided separately from the device or transmission"

The credit union will need to confirm in writing that its transfer meets these requirements. Credit unions may also do in-person transfers in so required.

The good news is that most Microsoft Office™ products and Adobe™ products provide ways to encrypt documents on the fly at the level required by the NCUA. Here are the methods of encryption for the more commonly used suite of word processing, spreadsheet, and PDF products.

Office 2013 and Office 2010

1. Click File.
2. From the Info tab, select Protect Document > Encrypt with Password.
3. The Encrypt Document dialog window appears. Type in a strong password (a minimum of eight characters; mixture of upper- and lower-case, numbers, and special characters; not easily guessable, etc.) and then select OK.
4. Re-enter your desired password in the Confirm Password window and click OK.
5. The Info window shows the new required permissions.

While it does not say so explicitly anywhere in the Office products themselves, this Microsoft Technet article describes the encryption as AES 128-bit, and thus compatible with the NCUA requirements:

> "Although there are Office 2013 settings to change how encryption is performed, when you encrypt Open XML Format files (.docx, .xslx, .pptx, and so on) the default values — AES (Advanced Encryption Standard), 128-bit key length, SHA1, and CBC (cipher block chaining) — provide strong encryption and should be fine for most organizations. AES encryption is the strongest industry-standard algorithm that is available and was selected by the National Security Agency (NSA) to be used as the standard for the United States Government. AES encryption is supported on Windows XP SP2, Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012."
>
> https://technet.microsoft.com/en-us/library/cc179125.aspx

Note: You may need to save your information in the Open XML formats (.docx, .xslx, etc.) for the encryption to work.

Office 2007

1. Click the Office button, then Save As.
2. Click Tools, and then click General Options.
3. Type a password in the Password to Open field.
4. Click OK when completed and click the Save button.

Office 2007 also uses 128-bit AES encryption so long as the document is saved in the Open XML format and there have been no changes to the default Office settings by your network administrator.

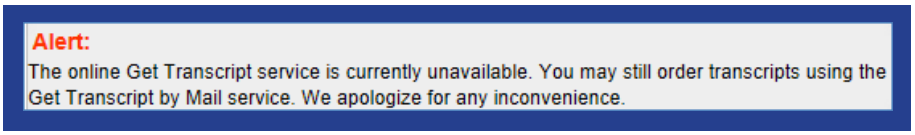
continued on page 5

Identity Theft Prevention - The New Normal

Brian W. Vitale, CAMS-Audit, NCCO
Chief Risk and Compliance Officer
Notre Dame Federal Credit Union

In August 2015 the Internal Revenue Service (IRS) confirmed more than 330,000 U.S. taxpayers' sensitive personally identifiable and tax information fell victim to identity thieves. How could this happen you ask? The IRS provided an online service called "Get Transcript" allowing anyone with a social security number and corresponding date of birth to order an online transcript of their last filed federal tax return. Take a moment to think about that. What personally identifiable information is on your tax return? To name a few: Your name, address, social security number, occupation and wages, salaries, tips, etc. from your W-2. Further, how many of you have dependents? My wife and I have four daughters, each of their names and social security numbers are listed on our tax return. So, of the 330,000 U.S. taxpayers identified by the IRS as potential victims, are they counting all six members of my family or only one head of household?

Following the IRS announcement, the online "Get Transcript" feature on their website was deactivated (www.irs.gov/Individuals/Get-Transcript).



Not a week goes by we don't read about the latest breach impacting millions of Americans. Some of the more infamous breaches in the past two years include Target, Home Depot, Anthem Blue Cross Blue Shield, JP Morgan Chase Bank and the Office of Personnel Management. Important to note, the IRS was not breached. The fraudsters utilized the online "Get Transcript" resource made available by the IRS. Are you one of the 330,000 U.S. taxpayers impacted by this "Get Transcript" scam?

The next appropriate question any reasonable person will ask: How did the fraudster obtain the personally identifiable information (name, social security number and date of birth) needed to take a very important step in stealing an identity? The short answer: Countless ways. Sophisticated social engineering techniques including phishing emails, vishing (telephone calls) and surfing your online presence via Facebook and Twitter, for example, are some of the ways fraudsters obtain your information. And, don't forget good old dumpster diving – a very effective non-technological technique used to obtain your personally identifiable information.

Do you have an expectation that those with whom you do business have an obligation to protect your sensitive, personally identifiable and transactional information from those intent on stealing your money and/or identity? Notre Dame FCU agrees with you. We take seriously our fiduciary responsibility to each and every member of the credit union. To that end, we continue to evolve member authentication and validation methods and techniques to ensure we maintain our commitment as gatekeepers of our member information.

One way we accomplish this is by ensuring we authenticate every member prior to executing a request. In the past, when our members called into our Shamrock Call Center or came into one of our branches, our employees validated our member's identity by asking standard authenticating questions such as member number, social security number, date of birth and/or mother's maiden name. Authenticating our members via traditional and previously accepted best-practice methodologies is no longer our process. However, this wasn't always the case.

A March 2015 Case Study
Financial Institution: Notre Dame FCU
Call Center Reps: Billy, Bobby, Suzy, Sally, Jesse and Johnny
Month: March 2015
Member: Member Smith
Fraudster: Fraudster

[Day #1: 8:35am] Notre Dame FCU's Shamrock Call Center received an after-hours voicemail from our member (herein referred to as Member Smith). Member Smith contacted Notre Dame FCU to advise he believed his account may have been hacked due to recent email updates he received post changes to his account profile. Billy, one of our call center service agents, attempted to return Member Smith's call via the phone number we have listed within the core – a best-practice security measure. A voicemail was left for Member Smith.

[Day #1: 10:06am] Member Smith contacted the Shamrock Call Center and spoke with Suzy. Member Smith advised Suzy someone had hacked into his accounts and filed a fraudulent tax return in his name. Suzy reviewed Member Smith's account history and advised she saw no suspicious activity in any of his accounts. No further action was taken at that time.

continued on page 6

Loan Participation and Indirect

Brian Lauer
Messick & Lauer P.C.
211 N. Olive Street
Media, PA 19063

On August 10, 2015, the National Credit Union Administration issued a legal opinion letter regarding loan participations in indirect loans. The issue that required clarification, may not appear on the surface to be a very hard question, but like many legal clarifications the analysis of an issue can have far reaching implications. Essentially, the loan participation rule, Part 701.22 of the NCUA regulations, very clearly states that a federally insured credit union can only purchase a loan participation from the "originating lender," and that such lender is the party with which the borrower contracts. In the context of indirect lending, the merchant is the party with which the borrower contracts and then the financing instrument is assigned to the credit union. This meant that credit unions could not sell participations in indirect loans to other credit unions because the selling credit union was not the originating lender. Not anymore. This legal opinion letter clarifies that, although the merchant is technically the party with which the borrower initially contracts, indirect lending programs are truly meant to allow the credit union to originate more loans at the point of sale. In this context, the credit union is really the originating lender.

There are many practitioners in the industry that just assumed this was the case and in fact there were some old legal opinion letters from the NCUA that hinted at this approach. So, while it is a great thing that this letter was issued and clears up a potentially big issue for the industry, the really interesting part of this letter are the implications it has on indirect lending.

In order for the NCUA to get to the final position of the letter, it needed to address and define "indirect lending." Indirect lending is not truly part of the NCUA regulations. The only reference to it is in Part 701.23 in relation to the sale of loans and the exclusion of indirect loans from the cap on loan purchases. Part 701.23 states that indirect loans are those where the credit union makes the final lending decision and the loan is assigned to the credit union very soon after the loan is closed.

This legal opinion letter now further explains indirect lending. The most enlightening section of this letter relates to the legal interpretation of the phrase "very soon after" taken from the language in Part 701.23. The NCUA explains the period of time between the closing of a loan or sales financing arrangement and the assignment of that instrument to a credit union will depend on the type of loan and industry standards for closing and assigning such loans. So, what is the number of days? No one knows and apparently NCUA does not plan to tell anyone.

This could affect your indirect lending programs if you are not careful about how the program is constructed. This letter will now highlight for examiners these issues that for many may not have been on the radar. Credit unions should review their indirect programs and assess whether there is proper justification for the time it takes to assign an indirect loan to the credit union. Is it fast enough? Is the speed typical under industry standards? For instance, different auto dealerships may move at different speeds when processing sales and assigning loans. It is unclear if one would meet the very soon after parameters if it is significantly slower.

Again, this letter is very important for the use of loan participations to manage a credit union's lending portfolio, but will it create more problems now that this rock has been turned over.

NCT

Credit Card Offsets under the Truth in Lending Act

Steven Van Beek
Attorney and Counselor
Howard and Howard

On August 18, 2015, a United States District Court in Massachusetts ruled (the "Order") that a credit union's deduction of funds from a member's account was the equivalent of an offset, which is prohibited by the Truth in Lending Act (TILA).

General Prohibition of Offsets

Section 169 of TILA includes a general prohibition on offsets for credit card accounts; however, it also states in subsection (b) that "this section does not alter or affect the right under State law of a card issuer to attach or otherwise levy upon funds of a cardholder held on deposit with the card issuer if that remedy is constitutionally available to creditors generally." Regulation Z, in 12 C.F.R. § 1026.12(d)(2), further clarifies this exception by stating that card issuers can obtain a consensual security interest in funds without violating the general prohibition of offsets.

Importantly, the Official Staff Commentary (OSC) states that the security interest "must not be the functional equivalent of a right of offset; as a result, routinely including in agreements contract language indicating that consumers are giving a security interest in any deposit accounts maintained with the issuer does not result in a security interest that falls within the exception of § 1026.12(d)(2)."

Awareness, Intent and Affirmative Agreement

The OSC outlines the specific conditions that credit unions must follow to obtain a valid consensual security interest. Specifically, in order to qualify for the exception "a security interest must be affirmatively agreed to by the consumer[.]" Additionally, the "consumer must be aware that granting a security interest is a condition for the credit card account (or for more favorable account terms) and must specifically intent to grant a security interest in a deposit account."

The Order focused closely on the fact that the credit union's credit card agreement was the only document that mentioned a security interest and that the member was not provided the credit card agreement until the credit card had been approved and delivered. The Court noted that the timing of the disclosures made to the member is significant and provides context for addressing the member's awareness and intent.

Indicia of the Member's Awareness and Intent

The OSC states that credit unions must obtain indicia of the consumer's awareness and intent – including at least one of the following (or a substantially similar procedure that evidences the consumer's awareness and intent):

1. Separate signature or initials on the agreement indicating that a security interest is being given.
2. Placement of the security interest on a separate page, or otherwise separating the security interest provisions from other contract and disclosure provisions.
3. Reference to a specific amount of deposited funds or to a specific deposit account number.

Many credit unions have the security interest provision of their credit card agreements bolded (and perhaps within a separate box) in an attempt to otherwise separate the security interest provisions from other contract and disclosure provisions. In the Order, the Court stated that "the bold text and boxing around the security interest agreement is minimally sufficient to make out that this language was separated from the other text of the Agreement."

Importantly, the indicia of intent must demonstrate that the member was aware that the security interest was a condition of receiving the credit card account. In the Order, the Court found the credit union's approach was insufficient to create a consensual security interest and, thus, the deduction of funds from the member's account was a prohibited offset.

Review Existing Procedures

The Order highlights the risks related to using the funds in a member's account to pay toward a credit card obligation without obtaining a prior consensual security interest. Credit unions must review their existing procedures – for obtaining a security interest and for offsetting funds – to determine their risks. If a credit union's current procedures are insufficient, the credit union should identify ways to update its procedures for new accounts as well as the options available to obtain a consensual security interest from existing cardholders.

Conclusion

In response to the Order, all credit unions issuing credit cards should review their procedures to determine whether they are obtaining a valid, enforceable consensual security interest. If a credit union's procedures are insufficient, the deduction of money from a member's account to pay an outstanding balance could be deemed a prohibited offset and significantly increase the credit union's regulatory and legal risks – including the potential for a class action lawsuit or an UDAAP claim.

NCT

continued from page 1

Office 2003 and Earlier

Support for Office 2003 has ended, and these programs can no longer be used to reliably encrypt documents. Documents created under these programs must either be saved under Office 2007 or later, converted to an encrypted PDF, sent through secure (encrypted) email, or transferred in person.

Adobe Acrobat DC

1. Open the PDF and choose Tools > Protect > Encrypt > Encrypt with Password.
2. If you receive a prompt, click Yes to change the security.
3. Select Require A Password To Open The Document, then type the password in the corresponding field. For each keystroke, the password strength meter evaluates your password and indicates the password strength.
4. Password Security - Settings let you set a password to open a PDF. The Compatibility option you choose determines the type of encryption used. It is important to choose a version compatible with the recipient's version of Acrobat or Reader. For example, Acrobat 7 cannot open a PDF encrypted for Acrobat X and later.

   Acrobat 7.0 And Later (PDF 1.6) encrypts the document using the AES encryption algorithm with a 128-bit key size.

   Acrobat X And Later (PDF 1.7) encrypts the document using 256-bit AES. To apply 256-bit AES encryption to documents created in Acrobat 8 and 9, select Acrobat X And Later.

   Note: Acrobat 6.0 And Later (PDF 1.5) encrypts the document using 128-bit RC4, which does not meet NCUA standards and cannot be used to reliably protect the information..

5. Select an encryption option:

   Encrypt All Document Contents
   Encrypts the document and the document metadata. If this option is selected, search engines cannot access the document metadata.

   Encrypt All Document Contents Except Metadata
   Encrypts the contents of a document but still allows search engines access to the document metadata.

   Encrypt Only File Attachments
   Requires a password to open file attachments. Users can open the document without a password. Use this option to create security envelopes.

6. Click OK. At the prompt to confirm the password, retype the appropriate password in the box and click OK.

Adobe Acrobat X and Later

1. In a single PDF or component PDF in a PDF Portfolio, open the PDF and choose Tools > Protection > Encrypt > Encrypt with Password. (You can also choose File > Properties and select the Security tab.) If you receive a prompt, click Yes to change the security.
2. Select a compatibility level. This option sets the encryption level and key size. Note: You may not select anything lower than Acrobat 7.0, or your PDF will not meet NCUA requirements.
3. Select the type of password to add, and then type the password in the corresponding field. For each keystroke, the password strength meter evaluates your password and indicates the password strength using color patterns. If you are setting a permissions password, determine the level of access.
4. To allow recipients to copy PDF content to another document, select Enable Copying Of Text, Images, And Other Content.
5. Click OK. At the prompt to confirm each password, retype the appropriate password in the box and click OK.

Adobe Acrobat 7.0

1. Select Document Security option from File menu.
2. Open Security Options drop down menu and select the option Acrobat Standard Security.
3. Checkmark the box Password Required to Open Document.
4. Enter password.

Adobe Acrobat 6.0 and Earlier

Adobe Acrobat 6.0 uses 128-bit RC4 encryption, which does not meet NCUA standards. These PDFs must be saved as a Microsoft Office 2007 or later document, sent through secure (encrypted) email, or transferred in person. Earlier versions of Adobe Acrobat cannot be relied upon to provide sufficient encryption to meet NCUA standards.

NCT

continued from page 2

[Day #2: 4:22pm] Shamrock Call Center service agent Bobby received a call from a person claiming to be Member Smith; post-mortem identified as the Fraudster. The Fraudster claimed he had just spoken to another call center service agent and forgot to update his phone number and email address. The Fraudster authenticated with Member Smith's full social security number, date of birth and joint owners name. He failed to correctly provide Member Smith's mother's maiden name. However, Bobby continued to make the changes as requested by the Fraudster. Bobby provided the Fraudster Member Smith's member number and changed his email to an email address equivalent to brianvitale@yahoo.com (Member Smith's first and last name were not listed in the email).

[Day #2: 4:25pm] Shamrock Call Center service agent Sally received a call from the Fraudster claiming to be Member Smith. Fraudster advised Sally he ordered a replacement credit card a few weeks ago, yet has not received it. The Fraudster authenticated with Member Smith's full social security number, address and joint owners name. A replacement credit card was issued and sent via UPS two-day delivery to the address of file. Sally continued to advise the Fraudster the credit limit on the card was $25,000.

[Day #3: 9:27am] Shamrock Call Center service agent Jesse received a call from the Fraudster claiming to be Member Smith. Fraudster was asked no authentication questions. Fraudster was provided the UPS tracking number from the previous day UPS shipment.

[Day #4: 12:22pm] Shamrock Call Center service agent Suzy received a call from the Fraudster claiming to be Member Smith. Fraudster claimed he had just called the call center to reset the PIN on the credit card, yet the PIN was not working. The Fraudster was authenticated with Member Smith's address, joint owners name and email address. Fraudster failed to correctly provide Member Smith's email address as Bobby never updated the email address per the Fraudster's request [Day #2: 4:22pm]. Nevertheless, Suzy changed the email address to the equivalent of brianvitale@yahoo.com and reset the credit card PIN to last four of Member Smith's social security number. Suzy ended the call reminding the Fraudster the credit limit on the card was $25,000.

[Day #4: 12:33pm] Shamrock Call Center service agent Suzy received a call from the Fraudster claiming to be Member Smith. Fraudster claimed the credit card PIN reset the day before was not working. The Fraudster authenticated with Member Smith's full social security number, date of birth and joint owners name. He failed to correctly provide Member Smith's mother's maiden name. Suzy changed Member Smith's mother's maiden name and reset the PIN per the Fraudster's request.

[Day #4: 2:45pm] Shamrock Call Center service agent Bobby received a call from the Fraudster claiming to be Member Smith. Fraudster advised Bobby his credit card was declined at an ATM. The Fraudster authenticated with Member Smith's address, telephone number and joint owners name. Bobby advised the Fraudster the credit card was not blocked and instead should attempt to make purchases instead of cash advances.

[Day #4: 4:37pm] Shamrock Call Center service agent Johnny received a call from the Fraudster claiming to be Member Smith. Fraudster advised Johnny he continued to have problems using the credit card. Johnny noticed a sum total of twenty-six (26) ATM withdrawals over a period of twenty-four (24) hours on the credit card. The Fraudster was then shutdown.

How many Red Flags can you find in the above sequence of actual events? Notre Dame FCU took a loss of $21,000 in fraudulent credit card ATM and purchase transactions. The Fraudster continues to call our Shamrock Call Center.

Increased member authentication and validation methods and techniques are the new normal here at Notre Dame FCU. What are your protocols at your credit union? How confident are you in the authentication and validation framework set-up at your credit union? Can a fraudster redirect your UPS or FedEx packages? If you don't know, please make it a top priority to find out.

If you have any questions about Identity Theft Prevention or general inquiries about social engineering pitfalls, please do not hesitate to contact me via email at bvitale@notredamefcu.com or directly at (574) 400-4971.

Written by:
Brian W. Vitale, CAMS-Audit, NCCO
Chief Risk and Compliance Officer
Notre Dame FCU

NCT

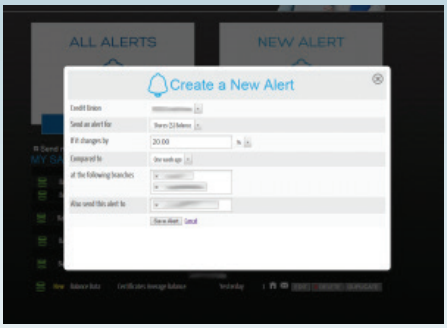
MY CU TODAY

Username: Password: Login

Learn more about My CU Today! It's the first external data warehouse with alerts and trends for every credit union stakeholder!

Watch a demo at
mycutoday.com/demo/

$100/month value!



Keep Your Finger on the Pulse

- A new external data warehouse
- Mobile access anytime, anywhere
- Daily alerts, before your morning coffee
- Credit Union data trend graphs
- Email alerts to all credit union stakeholders

www.mycutoday.com • 800.327.3478

CU*ANSWERS
A Credit Union Service Organization