SENT BY E-MAIL

DATE: August 21, 2015

TO: Federally Insured Credit Unions

FROM: Larry Fazio, Director
Office of Examination and Insurance

SUBJ: Providing Sensitive Credit Union and Member Data to NCUA

ENCL: (1) Examination Notification and Items Requested Letter
(2) Chain of Custody

Dear Chief Executive Officer:

NCUA takes protecting sensitive credit union and member data very seriously. NCUA defines sensitive data as (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.

Thus, the agency has recently updated its examination procedures to strengthen the safeguards for sensitive data received electronically from a credit union during an examination. These procedural changes are based on recommendations from NCUA's Office of the Inspector General.[1]

In order to ensure sensitive electronic credit union and member data is well protected, the data held by NCUA needs to be encrypted. The process of exchanging this data between credit unions and examiners also needs to be secure and well controlled. Thus, **effective immediately NCUA examiners may only accept sensitive data electronically as follows:**

Option 1 – Secure Electronic Transmission Or Transfer By Removable Media Includes Encryption

The preferred method is for the data file(s) to be provided on removable media (thumb drives, external hard drives, etc.) or transmitted through a secure electronic transmission. Either the data file(s) or the device or electronic transmission conveying the file(s) must be encrypted under this method. Credit unions can provide such information using their own removable media or, if permitted by the credit union's information technology security policy, media provided by

[1] See NCUA Office of the Inspector General Report #OIG-15-09 at http://www.ncua.gov/about/Leadership/CO/OIG/Documents/OIG201509MeasurestoProtectElectronicInfo.pdf

NCUA.[2] Credit unions can use various commercially available methods to electronically transmit files, such as via email or some type of secure file sharing service, provided the method incorporates encryption that meets the standards set forth below.

NCUA examiners will only accept such data files under this option if the following minimum data encryption requirements are met:[3]

- 128-bit AES encryption[4]
- 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

Under this option, when encrypted media provided by NCUA is not used, examiners will rely on the credit union's assertion that the encryption requirements above were met. Thus, NCUA examiners will have the credit union representative confirm in writing that the data file(s), removable media, or secure transmission provided to NCUA meets the minimum encryption requirements outlined above. If the transfer occurs while NCUA staff is onsite, this can be accomplished by the credit union representative signing the enclosed *Chain of Custody* document, which will be provided by the examiner. Otherwise, the credit union representative can confirm through email that the transfer met the standards above.

Option 2 – In Person Transfer by Removable Media Does Not Include Encryption[5]

If a credit union is unable or unwilling to electronically provide sensitive data in a manner that meets the requirements outlined for option 1, NCUA examiners may then only accept such data electronically if a credit union representative in person provides the data file(s) to the examiner and remains physically present while the examiner transfers the data to NCUA's encrypted equipment. NCUA examiners will immediately begin the transfer process when provided the data file(s). To complete the controlled transfer, examiners will have the credit union representative:

- Take receipt of the removable media from the examiner immediately after the data transfer is complete, and

---

[2] Eligible credit unions can apply for grants through NCUA's Office of Small Credit Union Initiatives to purchase encrypted removable media.

[3] Credit union security procedures should be followed if they require more stringent encryption and password standards than those listed.

[4] The U.S. National Institute of Standards and Technology (NIST) established the Advanced Encryption Standard (AES), a specification for the encryption of electronic data, in 2001. For more information, see "Announcing the ADVANCED ENCRYPTION STANDARD (AES)" (PDF). *Federal Information Processing Standards Publication 197*. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved July 31, 2015.

[5] Credit unions should not electronically transmit sensitive data to NCUA examiners, such as via unencrypted email, if the transmission or data file(s) does not meet the encryption standards specified in this letter. The credit union is responsible for any consequences associated with electronically transmitting or providing data to NCUA if the credit union did not follow the protocols in this letter.

- Sign the *Chain of Custody* document to acknowledge receipt of the removable media.

These new procedures are outlined in NCUA's *Examination Notification and Items Requested Letter*, which examiners use to schedule an examination. The template for the *Examination Notification and Items Requested Letter* is enclosed.

Please note NCUA examiners will not accept any sensitive data electronically if a credit union is unable to meet the requirements outlined in this letter. As part of the pre-exam planning process, NCUA examiners will coordinate with the credit union to resolve any issues that may arise with regard to this matter.

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. 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. The agency aims to have such a solution in place early in 2016. More information on the secure file transfer solution will be provided once it is ready to be deployed.

The agency will continue to work to ensure the highest standards of security for sensitive data in our possession. Please contact your regional office if you have any questions about this letter.

Sincerely,

/s/

Larry Fazio, Director
Office of Examination and Insurance

Enclosures

National Credit Union Administration

«ROName»
«ROAddress»
«ROCity», «ROState» «ROZipCode»
«ROPhone»

[Date of Letter]

[Mr. or Ms. and CEO or Manager's Name]
[Title - CEO/President or Manager etc.]
«Charternamе» [Federal Credit Union or Credit Union]
«StreetAddress»
«City», «CreditUnionState» «Zip»

Dear [Mr. or Ms. and Last Name] :

NCUA has scheduled an examination of «Charternamе» [Federal Credit Union or Credit Union] , which will include an on-site review. The exam will begin on [Month, Day and Year] ; our examination team plans to arrive on-site on [Month, Day and Year] . The effective date of the exam will be [Month, Day and Year] . **The information in this letter will help you prepare for the upcoming review. Please read this material carefully and share it with the appropriate individuals.**

Prepare for On-Site Examiners

[#] NCUA examiners will participate in the examination, and # state supervisory authority examiners will also be on-site. We have included a list of examiners including their role, arrival and departure dates as an attachment to this letter. For security purposes, examiners will provide official ID when they arrive. To prepare for on-site examiners, you should:

- Make appropriate security arrangements according to your institution's security protocols.
- Invite appropriate credit union staff to participate in an entrance meeting on [Month, Day and Year] with the exam team (meeting will take place at the credit union).
- Provide sufficient work space to accommodate examiners on the dates specified in the attachment.

Important Dates to Remember	
Exam effective date	«DateEffective»
Deadline to create indexed collection of requested items	[##/##/##]
Exam begins	[##/##/##]
Exam team arrives	[##/##/##]
Entrance meeting with exam team and credit union	[##/##/##]
On-site review concludes *(estimated)*	[##/##/##]

It is important to minimize risk to sensitive member and other credit union information provided electronically by doing so in a secure manner. NCUA defines sensitive data as (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.

In order to ensure sensitive electronic credit union and member data is well protected, the data held by NCUA needs to be encrypted. The process of exchanging this data also needs to be secure and well controlled. Thus, **NCUA examiners may only accept sensitive data electronically as follows:**

Option 1 – Secure Electronic Transmission Or Transfer By Removable Media Includes Encryption

The preferred method is for the data file(s) to be provided on removable media (thumb drives, external hard drives, etc.) or transmitted through a secure electronic transmission. Either the data file(s) or the device/transmission itself must be encrypted under this method. The credit union can provide such information using its own removable media or, if permitted by the credit union's information technology security policy, media provided by an NCUA examiner. Credit unions can use various commercially available methods to electronically transmit files, such as via email or some type of secure file sharing service, provided the method incorporates encryption that meets the standards set forth below.

NCUA examiners will only accept such data files under this option if the following minimum data encryption requirements are met:[1]

- 128-bit AES encryption[2]
- 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

Under this option when encrypted media provided by NCUA is not used, NCUA examiners will rely on the credit union's assertion that the encryption requirements above were met. Thus, NCUA examiners will have the credit union representative confirm in writing that the data file(s), removable media, or secure transmission provided to NCUA meets the minimum encryption requirements outlined above. If the transfer occurs while NCUA staff is onsite, this can be accomplished by the credit union representative signing a *Chain of Custody* document to be provided by the examiner receiving the data. Otherwise, the credit union representative can confirm through email that the transfer met the standards above.

---

[1] Credit union security procedures should be followed if they require more stringent encryption and password standards than those listed.

[2] The U.S. National Institute of Standards and Technology (NIST) established the Advanced Encryption Standard (AES), a specification for the encryption of electronic data, in 2001. For more information, see "Announcing the ADVANCED ENCRYPTION STANDARD (AES)" (PDF). *Federal Information Processing Standards Publication 197*. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved July 31, 2015.

Option 2 – In Person Transfer by Removable Media Does Not Include Encryption[1]
If the credit union is unable or unwilling to electronically provide sensitive data in a manner that meets the requirements outlined for option 1, NCUA examiners may then only accept such data electronically if a credit union representative in person provides the data file(s) to the examiner and remains physically present while the examiner transfers the data to NCUA's encrypted equipment. NCUA examiners will immediately begin the transfer process when provided the data file(s). To complete the controlled transfer, examiners will have the credit union representative:

- Take receipt of the removable media from the examiner immediately after the data transfer is complete, and
- Sign the *Chain of Custody* document to acknowledge receipt of the removable media.

NCUA examiners will not accept any sensitive data electronically if a credit union is unable to meet the requirements outlined in this letter. If you are unable to meet these expectations, please contact the examiner in charge before they arrive on-site to resolve the issue.

Collect Items and Make Information Available to Examiners

The attachment to this letter contains a list of items examiners will review during the examination. To prepare for the exam:

- Advise your Supervisory Committee or external auditor to make work papers for the last audit completed during the examination period ([Date – Date]) available to the exam team for review.
- Notify staff that examiners are authorized to access internal audits, compliance reports, and workpapers.
- Gather the information listed on the enclosed attachment and index all items before [Month, Day and Year] .

After the On-site Review

We estimate the on-site review will end by [Month, Day and Year] , at which time credit union management and officials will have the opportunity to participate in an exit meeting. Examiners will share their draft findings and conclusions at this meeting, so please schedule with staff accordingly. We will alert you of any changes in the schedule as the exam progresses.

If you have any questions about this letter or the attachments, please contact Examiner «FirstName» «LastName» at «ExaminerPhone» or at «Email». Thank you in advance for your cooperation.

Sincerely,

[1] The credit union should not electronically transmit sensitive data to NCUA examiners, such as via unencrypted email, if the transmission or data file(s) does not meet the encryption standards specified in this letter. The credit union is responsible for any consequences associated with electronically transmitting or providing data to NCUA if the credit union did not follow the protocols in this letter.

«FirstName» «LastName»
Examiner in Charge

National Credit Union Administration

Chain of Custody Tracking Form

Description of Documents/Devices					
Item #	**Quantity**	**Description of Item and Contents** (Model, Serial #)	**Sensitive Data on Device(s)** (Yes/No)	**Meets Minimum NCUA Encryption Requirements**[1] (Yes/No)	**Credit Union Representative Attesting to Device/Transmission Encryption** (Name & Signature)

Chain of Custody					
Item #	**Date/Time Released**	**Released to** (NCUA/ Credit Union)	**NCUA Representative** (Name & Signature)	**Credit Union Representative** (Name & Signature)	**Comments**

Keep an electronic copy of completed document as part of the AIRES report.

[1] Minimum 128-bit AES encryption, strong password/passphrase (minimum of 8 characters with a mixture of upper-case, lower-case, numbers, and special characters that is non-trivial and not easily guessable), password provided separately from the device or transmission.