MANAGEMENT ADVISORY REVIEW

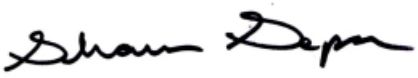
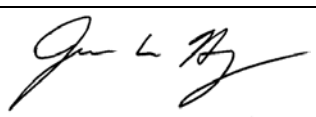
Subject:	*Type of Report*:
Notification Actions – Palm Springs Federal Credit Union	[ ] Preliminary [X] Final [ ] Supplemental

CHARACTER OF REVIEW

On December 15, 2014, the Credit Union Times reported that the National Credit Union Administration (NCUA) had confirmed that an external flash drive containing the names, addresses, social security numbers, and account numbers belonging to approximately 1,600 members of the Palm Springs Federal Credit Union (PSFCU) in California was lost during an examination. Specifically, in October 2014, PSFCU officials gave an NCUA examiner an unencrypted flash drive that the examiner subsequently lost or misplaced (the "incident"). The flash drive did not include passwords or PINS. To date, neither NCUA nor PSFCU has received an indication of any unauthorized access to members' accounts or attempts to gain improper access as a result of the incident.

The Office of Inspector General's (OIG) review focused on:

1. the use of the term "audit" in lieu of "exam," in the notification letter, dated October 30, 2014, that PSFCU sent to affected credit union members and the California Office of the Attorney General (OAG) (the "notification letter"). Here, OIG focused particularly on whether NCUA's Office of General Counsel (OGC) either proposed or influenced the use of the term "audit" in order to obfuscate the fact that an NCUA examiner was responsible for the loss of the flash drive; and
2. whether NCUA's decision not to publicly announce the incident on the agency's website was appropriate under the circumstances.

Distribution	*Case Number*: N/A	*Date of Report*: March 2, 2015
Debbie Matz, Chairman Rick Metsger, Vice Chairman J. Mark McWatters, Board Member Mark Treichel, Executive Director	*NCUA Counsel to the Inspector General/Assistant IG for Investigations* Sharon Separ 	
	NCUA Inspector General James Hagen 	

PROCEDURAL BACKGROUND

OIG requested and reviewed all documents relevant to the incident that NCUA officials received, created, and otherwise exchanged between October 24, 2014, and December 30, 2014. The documents reviewed represented internal email discussions among NCUA employees, between NCUA employees and OGC, and within OGC, respectively, as well as all draft and final documents written in response to the incident.[1] OIG also reviewed all documents pertaining to discussions between OGC and legal counsel retained by PSFCU to represent it in this matter, including draft and final versions of the notification letter. OIG further interviewed NCUA employees and OGC attorneys involved in the agency's response to the incident, as well as PSFCU legal counsel. Finally, OIG reviewed the Palm Springs Police Department (PSPD) Incident and Narrative Report, dated December 9, 2014, which OIG received from PSPD on January 28, 2015.[2]

FINDINGS

1. The Notification Letter

As required by California privacy laws and Part 748, App. B., Section III of NCUA regulations, on October 30, 2014, PSFCU issued a letter, sent via first-class mail, notifying affected members of the loss of the flash drive. The California OAG further requires publication on its website of any such notification letter that goes out to a California resident affected by a data breach. As a result, PSFCU's notification letter was posted to the OAG website and is available at: http://oag.ca.gov/ecrime/databreach/reports/sb24-47289. Prior to the issuance and posting of the notification letter, OGC engaged in discussions with PSFCU legal counsel regarding its contents and whether any additional public notification of the incident was necessary or appropriate.

OGC first learned of the incident on October 24, 2014, from PSFCU legal counsel. From the outset, PSFCU counsel conveyed a sense of urgency to OGC with regard to the timing of the notification letter's transmittal to members and the OAG. Specifically, they indicated their intent to issue the notification letter by October 30, 2014. Simultaneously, PSFCU counsel alerted OGC that it was seeking, on behalf of its client, reimbursement to include the costs of: notifying the membership; mailing related to the incident; credit monitoring services for PSFCU's 1,600 members; attorneys' fees for handling the incident; and the potential costs involved with changing plastic cards and share drafts upon the request of affected members.

As background, PSFCU legal counsel stated that when they first learned about the incident, they looked at a series of sample letters that the California OAG makes publicly available to understand what type of information and detail a breach notification letter should include. While PSFCU legal counsel wanted to ensure full compliance with California law, they also wanted to provide the minimum detail required because of the circumstances surrounding the loss of the

[1] In certain places, this report distinguishes between "NCUA employees" and "OGC" because of OGC's distinct role in working directly with PSFCU legal counsel to draft the notification letter.

[2] Despite repeated telephonic and email requests to PSPD by OGC and OIG, OIG was only able to acquire a copy of the PSPD Report when an OIG investigator traveled to Palm Springs and requested it, in person, from the reporting officer.

flash drive. That is, because it appeared that it was a question of an inadvertent loss, and not a theft by an individual who already knew or suspected what type of information the drive contained, they did not want to needlessly alert anyone who might have found or otherwise have the drive in their possession what type of information it contained.

PSFCU legal counsel, one of whom specializes in cybersecurity, pointed out to OIG that in the area of cybersecurity, when it is a question of an ongoing breach situation, such as this one, the focus is on investigating what actually occurred before going public with an announcement. At the time the parties began working on the draft notification, the PSPD had just initiated its investigation into the incident and the case was ongoing. Nevertheless, because California law required issuance and posting of a written notification letter to affected members, the credit union had to prepare some type of public announcement, in large part to ensure that members knew what had occurred. Moreover, the credit union wanted to act swiftly to put procedures in place so that if a member contacted it with inquiries, PSFCU staff was prepared to respond and advise fully and appropriately.

Consequently, taking into consideration the sample letters they reviewed and their intention to provide a succinct description of the incident, PSFCU legal counsel crafted the initial draft of the notification letter, which they forwarded to OGC on October 28, 2014, for review and comment. The initial draft referenced the term "audit" (or a variation thereof) in three instances. PSFCU counsel explained to OIG that its use of the word "audit" (and variations thereof) was intentional, based on the credit union's desire, as mentioned above, not to alert the possessor of the flash drive that, unbeknownst to him or her, it contained personally identifiable information (PII). By using the more generic term "audit," rather than "exam," the credit union and its counsel believed, as mentioned above, that they could reduce the likelihood that the notification letter might alert an unwitting possessor of the drive of the valuable information it contained, who might then use that information to attempt to gain access to member accounts or for other illegal purposes. PSFCU counsel informed OIG that after fully considering the appropriate wording, they determined that the use of the word "audit" was "adequately descriptive."

In its first mark-up of that initial draft, OGC redlined (deleted) entirely two of the three references. In the final letter, in deference to PSFCU counsel's subsequent mark-ups, a variation of the word "audit" appeared twice. Beyond the early draft of the notification letter, where OGC redlined two of the "audit" references, none of the other documentation—in particular the voluminous emails OIG collected from all parties involved in the incident—reflected a single discussion about the use of the term "audit." While both sets of counsel recalled a telephonic discussion where the use of the term "audit" rather than "examiner," was discussed, PSFCU legal counsel told OIG that it was always their position—and the credit union's—that the term "audit" should be used. OIG learned through its interviews with OGC that OGC supported the decision to use the term "audit." OGC's stated reason for agreeing with PSFCU counsel that the term "audit" should be used in the letter was based on its opinion that stating in the letter that an "examiner" was involved in the loss would be tantamount to NCUA admitting liability. OGC explained that its intent throughout the period when NCUA was deliberating its response to the incident was to shield the agency from as much potential liability as possible. In this regard, PSFCU legal counsel told OIG that its position was that NCUA did not need to expressly admit agency liability in the notification letter because it had been forthcoming in accepting responsibility for the examiner error that resulted in the loss.

That PSFCU legal counsel intentionally and originally used the term "audit" and not "examiner" is further evidenced in its initial contact with PSPD. On October 23, 2014, the PSFCU manager reported the loss of sensitive credit union information to PSPD. According to the PSPD Narrative Report, the officer assigned to the case initially spoke with PSFCU legal counsel, who related that:

> [PSFCU] had been in the middle of an annual *audit* which was conducted by the NCUA. This *audit* was being conducted . . . and one of the NCUA *auditors* . . . [was provided with] a memory stick which contained the account information of credit union members which was used to conduct the *audit.*

(Emphasis added.)

Subsequently, the reporting officer spoke with the credit union manager, who told him that PSFCU:

> was in the middle of an annual *audit* being conducted by the NCUA. She said that the *audit* . . . was scheduled to run for two weeks. [The manager] said that during the first week, a [redacted] *auditor* . . . had used the thumb drive to conduct the *audit* without any issues arising.

(Emphasis added.)

Throughout the remainder of the Narrative Report, the reporting officer consistently used the words "audit" or "auditor," but never the terms "exam" or "examiner." It is significant that both of these contacts occurred before PSFCU counsel reached out to OGC to seek input into the draft notification letter.

Consequently, OIG concluded that it was PSFCU and its legal counsel's original and ongoing intent that the notification letter should use the term "audit." This review further found that at no time did OGC attempt to influence PSFCU counsel to use the term "auditor" in lieu of "examiner." Indeed, PSFCU counsel told OIG that throughout the entire time period during which it worked with OGC on the letter, OGC never said or did anything that might have reflected an intention on its part to portray the incident with anything less than candor. OIG found further that, while OGC's intention throughout the process of drafting the letter was to shield NCUA from potential liability, it did not advance that goal at the expense of attempting to mislead affected PSFCU members, the California OAG, or the California public. Moreover, PSFCU legal counsel's statements that OGC accepted that an examiner error resulted in the loss, and its representation that NCUA intended to assume financial responsibility for the ensuing repercussions, further obviated any inference that OGC was attempting to misdirect NCUA's culpability for the incident.

2. NCUA's Decision Not to Publicly Announce the Incident

a. Designation of the Breach Notification Team

On October 28, 2014, the NCUA Acting Deputy Executive Director (DED), Office of the Executive Director (OED), informed the Executive Director (ED) about the incident. The ED sought input from the Office of Examination & Insurance (E&I) which, in turn, reviewed the internal policies addressing breach situations[3] and provided the ED with a synopsis. Paragraph 4.a. of NCUA Instruction No. 13500.08 requires that "[w]hen the NCUA becomes aware of an actual or suspected data breach, the NCUA's Breach Notification Team (BNT) will convene." Accordingly, in an email dated October 28, 2014 (5:02 p.m.), the ED appointed five individuals to the BNT: the Acting Chief Information Officer (Acting CIO), Office of the Chief Information Officer (OCIO); the Director, Office of Public and Congressional Affairs (PACA); the Regional Director (RD), Region V; the Deputy Director, E&I; and the Associate General Counsel (Enforcement and Litigation), OGC. Enlisting the assistance of the agency's (Acting) Chief Information Security Officer (Acting CISO),[4] OCIO took the lead of the BNT as the Instruction required. The BNT's composition did not conform in all respects to NCUA Instruction 13500.08 which, under ¶ 3. Definitions, defines the team as including the following: the Acting CIO, the [C]ISO, and designated representatives from PACA, OGC, Office of the Chief Financial Officer (OCFO), Office of Human Resources (OHR), E&I, and the OIG. While OED notified OIG of the incident, it did not do so until late in the day on October 29, 2014, after the BNT had already completed its assessment. Moreover, neither OHR nor OCFO were team members.

According to the Acting CISO, his role on the BNT was to: (1) assist the team in assessing the breach; (2) determine the technical causes of the breach; and (3) recommend solutions to address the issues presented and to prevent future breaches. In so doing, the Acting CISO stated that at approximately 8:00 p.m. on October 28, 2014, he notified the NCUA Senior Agency Official for Privacy (SAOP) by email of the incident. The SAOP informed OIG that, given her position's responsibilities, she should have been informed of the incident when OGC first learned of the situation, on October 24, 2014.

The Acting CISO told OIG that, relatively quickly, he surmised that the breach was a "non-technical" incident. He explained that the key point here was that there was no compromise of federal information or a federal information system, that is, information was not disclosed due to an NCUA system compromise or a failure of existing technical controls. Once OCIO understood that it was a question of a potential unauthorized disclosure of credit union member information due to a policy violation and not a technical control failure, the Acting CISO concluded that there was nothing OCIO could do except make recommendations to avoid in the future the situation that led to the loss of the thumb drive. To exemplify his point, the Acting CISO stated that this was not a situation where there was a malicious action that led to third-party access to the NCUA network such that PII was stolen. He explained that in those situations, OCIO could go in and, for example, "patch" vulnerabilities, block malicious IP addresses, remove files from

[3] Specifically, E&I consulted NCUA Instruction No. 13500.08, "Breach Notification Policy" (September 26, 2007) and NCUA Instruction No. 13500.09, "Security of External Party's Documentation" (March 25, 2008).
[4] The Acting CISO title is synonymous with the title of Senior Agency Information Security Officer, as set forth in applicable National Institute of Standards and Technology (NIST) publications.

the system, etc., in order to remedy technical control failures. He emphasized that this was not the case with the PSFCU incident, where there was no failure of federal technology or in-place technical controls. Rather, this incident was attributable to the "human component," involving a violation of an existing policy, and not a technical compromise.

Once he had determined the facts surrounding the incident, the Acting CISO consulted the following reference documents to further assess the situation and make recommendations:

- United States Computer Emergency Response Team (US-CERT) reporting guidelines;
- NIST publication 800-61 Rev2;
- NCUA Security Incident Response Procedure (SIRP), Version 1.1, dated August 1, 2014;[5] and
- Applicable Office of Management and Budget (OMB) Guidance.

Upon finalizing his assessment, the Acting CISO, on behalf of the BNT, prepared the following documents:

- A memorandum from the Acting CIO to the Acting DED dated October 29, 2014, titled "OCIO Incident Notification—Loss of Equipment/Personally Identifiable Information (PII)," presenting OCIO's findings and recommendations (OCIO memorandum); and
- A power point presentation titled "Breach Notification Requirements and Proposed Actions" (the PPP).

The Acting CISO also provided a copy of a summary of the US-CERT report, generated by that entity, which evidenced the agency's reporting of the incident to US-CERT.

b. The BNT's Assessment and Recommendations

i. The OCIO Memorandum

The OCIO memorandum characterized the loss of the unencrypted flash drive as a "Security Incident (Loss of Equipment/PII)" and provided details about what transpired leading up to—and in the immediate aftermath of—the flash drive's loss. It concluded that "while the credit union's failure to encrypt the data provided to NCUA staff was imprudent, the facts as currently known indicate that NCUA staff failed to exercise proper care over the data in their custody." The memorandum also indicated that OCIO had reported the incident to US-CERT, and had created a list of accompanying recommendations for NCUA to take immediately and long-term to address future data loss prevention. Finally, OCIO recommended that NCUA provide credit monitoring for individuals affected by the incident.

ii. The PPP

The PPP set forth specific recommendations, segregating them into: (1) Proposed Non-Technical Solutions and (2) Proposed Technical Solutions.

[5]An updated version of the SIRP (Version 1.2) was issued on December 1, 2014.

Among the Proposed Non-Technical Solutions were the following:

- NCUA should send out a memo immediately outlining information security best practices for examiners when obtaining data from credit unions. (NCUA has completed this item.)
- NCUA should roll out specialized information security training for examiners. (NCUA has begun implementing this item simultaneous with the rollout of new employee and contractor laptops.)
- NCUA senior management should continuously stress the importance of end user situational awareness and consequences of non-compliance with NCUA policies. (NCUA has initiated this item and it is currently ongoing.)
- To increase end user awareness of privacy-related issues NCUA should accelerate implementation of its Privacy Program. (NCUA has initiated this item and it is currently ongoing.)

With regard to the Proposed Technical Solutions that OCIO recommended, OIG is currently conducting an audit to determine whether NCUA has adequate controls in place to protect electronic PII and sensitive credit union examination data. Because that audit will address OCIO's Proposed Technical Solutions, this report does not include a discussion of those recommendations.

c. The Notification Decision

After reviewing the facts, the notification letter, Instruction No. 13500.08, applicable OMB guidance, and Federal Trade Commission (FTC) public information on responding to identity theft incidents, the BNT determined further that it was not necessary to post an additional notification of the incident on the NCUA website. Moreover, it concluded that such additional public notice could be detrimental. Consequently, taking into consideration the BNT's conclusions, as discussed in more detail below, and his own review of the matter, the ED made the decision not to publicly announce the incident on NCUA's website or elsewhere.[6]

The BNT and, in turn the ED, looked initially to OMB guidance, in particular the September 26, 2006, Memorandum prepared, under the aegis of OMB, by the Identity Theft Task Force,[7] titled "Identity Theft Related Data Security Breach Notification Guidance" in considering whether additional notification was necessary or appropriate. The Task Force memorandum advised that a federal agency which suffers a breach involving PII obtained from a regulated entity might wish to determine whether the source of the breach notice should be the regulated entity. (Task Force memorandum at 8.) NCUA Instruction 13500.08 reiterates this guidance, in providing that "[t]he credit union generally will provide the notice for breaches of credit union . . . member data." (Instruction at ¶ 4.c.2.) By the time the BNT was assembled on October 28, 2014, PSFCU legal counsel had already instructed NCUA that, in accordance with California law, the

[6] Instruction 13500.08 provides that "[t]he Executive Director will make the final determination of whether a data breach of personally identifiable information occurred and whether breach notification will occur. The Executive Director will approve all aspects of any breach notification." (Instruction at ¶ 4.a.)

[7] The Task Force was at that time chaired by then-Attorney General Alberto R. Gonzales and co-chaired by FTC Chairman Deborah Platt Majoras.

credit union would notify its members by letter of the incident and the letter would be posted to the California OAG website.[8]

The second consideration the BNT and the ED factored into their decision-making was the Task Force's warning that agencies should:

> [b]e aware that the public announcement of the breach could itself cause criminals engaged in fraud, under the guise of providing legitimate assistance, to use various techniques, including email or the telephone, to deceive individuals affected by the breach into disclosing . . . other sensitive personal information. One common such technique is "phishing" . . . .

(Task Force memorandum at 6.) All of the members of the BNT the OIG interviewed, as well as the ED, expressed their concern that an additional, public announcement of the incident on NCUA's website risked unnecessarily exposing the credit union members whose information was on the flash drive as potential fraud targets. They emphasized that at that point, there was no indication that anyone had yet accessed the members' data and attempted to misuse it. They opined that alerting someone in possession of the flash drive of the valuable information it contained, who might then use that information to attempt to breach member accounts or for other illegal purposes, could put the credit union members affected by the loss at even greater risk. This conclusion mirrored that of PSFCU and its legal counsel, as discussed *supra*.

The BNT further considered OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," dated May 22, 2007, which set forth questions and factors agencies should consider in determining when outside notification should be given and the nature of the notification. Among these factors, OMB warned that unnecessary notifications could have a chilling effect on the public. (M-07-16 at 12.) In this regard, OMB referenced FTC testimony which raised similar concerns about the threshold at which consumers should be notified of a breach, cautioning that too strict a standard could have several negative effects.[9] According to then-FTC Chairman Majoras, the goal of any notification requirement is to enable consumers and affected individuals to take steps to avoid the risk of identity theft. However,

> [t]he challenge is to require notices only when there is a likelihood of harm to consumers. There may be security breaches that pose little or no risk of harm, such as a stolen laptop that is quickly recovered before the thief has time to boot it up. Requiring a notice in this type of situation might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, notices may be more common than would be useful. As a result, consumers may become numb to them and fail to spot or act on those risks that are truly significant.

[8] See, http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29 and http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82

[9] Federal Trade Commission, Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft (Washington, D.C.: June 16, 2005) (Testimony).

(Testimony at 10.) Likewise, because PSFCU members affected by the incident had already been fully notified about what had occurred, the BNT concluded that a more public announcement might result in "unnecessary consumer concern and confusion" and simultaneously serve no greater purpose.

In considering further whether publicly announcing the incident on the NCUA website could have deleterious effects, the BNT gave considerable weight to the fact that California has some of the nation's strictest laws pertaining to notification and customer protections in the event of a data breach.[10] Indeed, the Acting CISO noted that there is an inclination to defer to state law requirements when they are more stringent than federal ones.[11] This, he pointed out, is the case with California laws on privacy and breach notification.

Finally, the BNT and the ED pointed out that throughout the period when both were deliberating what the agency response should be, they were aware that the PSPD investigation into the incident was ongoing. The PSPD had a subjective as well as professional interest in conducting a thorough fact-finding inquiry, because it was included in PSFCU's field of membership. Given this, the BNT and the ED were sensitive to the fact that a more expansive public announcement of the incident, beyond the notification letter and its posting on the California OAG website, might interfere with that ongoing investigation.

Based on the foregoing, the BNT advised, and the ED determined, that full compliance with California's notification rules, in addition to NCUA's commitment to reimburse PSFCU for the costs involved in providing credit monitoring to affected members, was a sufficient response on NCUA's part and that additional notification was neither warranted nor necessarily advisable.

CONCLUSION

1. OIG found no evidence to indicate that OGC attempted to either (1) obfuscate the fact that an NCUA examiner was responsible for the loss of the flash drive; or (2) otherwise unduly influence PSFCU, through its legal counsel, to use the word "auditor" in lieu of "examiner" in the notification letter.

2. OIG concluded that the ED's decision not to publicly announce the incident on NCUA's website was appropriate under the circumstances.

RECOMMENDATIONS

In response to OMB guidance issued in 2006 and 2007, respectively, NCUA first formalized internal policies documenting how it should respond in the event of a security breach incident as well as for securing documentation about or acquired from credit unions or other external parties.

[10] See, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf; http://www.uspirg.org/media/usp/national-data-theft-law-still-hard-sell; http://www.statetechmagazine.com/article/2014/10/california-strengthens-data-breach-notification-law.

[11] http://www.washingtonpost.com/blogs/the-switch/wp/2015/01/12/privacy-advocates-a-national-data-breach-notification-standard-might-actually-make-things-worse/

NCUA was fortunate, prior to the PSFCU incident, in not having to test the adequacy of those policies, because a security breach had not occurred. However, in light of lessons learned as a result of the PSFCU incident, over the past several months NCUA has revisited its internal policies and is in the process of revising them. Moreover, as mentioned above, OCIO recently recommended several non-technical solutions to address and prevent security breach incidents, which have already been fully implemented or are ongoing. Finally, to lend assistance to this effort, OIG is currently conducting an audit to determine whether NCUA has adequate controls in place to protect electronic PII and sensitive credit union examination data.

Consequently, the following recommendations recognize that this process is an ongoing one and do not at this time reflect a comprehensive overview of NCUA's current efforts in this area. They address, rather, deviations from or omissions in NCUA's existing policies that OIG noted in the course of this review.

1. Instruction 13500.08 should be revised to include the SAOP as a member of the BNT. Indeed, the SAOP should be notified of, and then involved in, all security breach incidents from beginning to end.

2. Instruction 13500.08 should be revised to omit OIG as a representative on the BNT. While OIG, like the SAOP, should be notified of and continually apprised of all security breach incidents, OIG's involvement should remain auxiliary to the BNT, so that it can simultaneously (1) fulfill its law enforcement responsibilities, if any, in response to a breach incident; and (2) independently assess NCUA's response in the aftermath of an incident, as necessary.

3. NCUA should review the complete list of designated representatives to the BNT, which Instruction 13500.08 currently lists, to determine whether all or only some of them should serve on the team. For example, in response to the PSFCU incident, the ED did not designate representatives from OCFO and OHR (in addition to OIG) to the BNT, as the Instruction currently requires. If NCUA determines that representatives from those offices should not be on the BNT, then the Instruction should be revised to reflect that.