Office of Inspector General

Office of Audits and Evaluations
Report No. AUD-15-004

The FDIC's Controls for Identifying, Securing, and Disposing of Personally Identifiable Information in Owned Real Estate Properties

March 2015

Office of Inspector General

Executive Summary

The FDIC's Controls for Identifying, Securing, and Disposing of Personally Identifiable Information in Owned Real Estate Properties

Report No. AUD-15-004
March 2015

Why We Did The Audit

As the receiver of failed FDIC-insured financial institutions, the FDIC acquires owned real estate (ORE) properties that are located throughout the United States and its territories. These properties include single-family homes, condominiums, office buildings, retail establishments, hotels, and undeveloped land (among other types of property). In some cases, ORE properties are found to contain personal property, including personally identifiable information (PII), that was left behind by the previous owners or occupants of the properties. Establishing controls to properly handle PII found at ORE properties is critical to mitigating the risk of an unauthorized disclosure that could lead to identity theft, consumer fraud, and potential legal liability or reputational damage to the Corporation. Accordingly, we conducted this audit.

The audit objective was to determine whether the FDIC has established internal controls to properly identify, secure, and dispose of PII in ORE properties. As part of our work, we reviewed the FDIC's handling of PII found at 10 non-statistically sampled ORE properties.

Background

When an insured financial institution fails, the FDIC establishes a receivership to liquidate the institution's assets. In many cases, these assets include ORE properties. Within the FDIC, the Division of Resolutions and Receiverships (DRR) has primary responsibility for liquidating assets in receivership. According to DRR records, the FDIC acquired and liquidated approximately 14,000 ORE properties between February 2007 (when the most recent financial crisis began) and December 31, 2014.

DRR typically identifies PII at ORE properties through physical site inspections. DRR has engaged two national asset management firms (referred to herein as the ORE contractors) to manage, market, and dispose of ORE properties. As part of their responsibilities, the ORE contractors are required to conduct site inspections of properties assigned to them. Site inspections address such things as the condition and appearance of the property, security risks, health and safety issues, and signage. In May 2014, DRR issued formal guidance requiring the ORE contractors to identify, report, safeguard, and destroy hard copy information and electronic equipment that may contain PII. DRR Resolutions and Receiverships Specialists (referred to herein as Account Officers) oversee the management, marketing, and sale of ORE properties. As part of their responsibilities, Account Officers review site inspection reports prepared by the ORE contractors and ensure that liability issues, including those related to PII, are identified and properly addressed. Account Officers also perform site inspections of ORE properties to ensure they are being properly maintained and marketed for sale.

When PII is identified in an ORE property, DRR's general approach is to secure the information and arrange for its immediate destruction. In doing so, DRR coordinates with other organizations within the FDIC. These principally include the Computer Security Incident Response Team (CSIRT), a group within the Chief Information Officer Organization (CIOO) that is responsible for providing technical assistance in investigating, reporting, resolving, and closing incidents; the Privacy Program staff, which reviews FDIC-prepared incident risk analyses/impact assessments and makes the final determination regarding whether an incident constitutes a breach of PII; and the Legal Division which may, on a case-by-case basis, provide advice on legal issues pertaining to PII found in ORE properties.

Audit Results

The FDIC established a number of internal controls during the course of our audit that were designed to properly identify, secure, and dispose of PII at ORE properties. Among other things, DRR held a training conference and issued formal guidance to its ORE contractors and Account Officers in May 2014 that addressed procedures for identifying, reporting, securing, and disposing of PII. DRR also modified its ORE contracts in October 2014 to specifically require that the contractors search for PII during every property site inspection. Although these control improvements are positive, they do not fully address our findings described below.

Our review of 10 non-statistically sampled ORE properties found that PII was often not identified in a timely manner and that practices for handling and disposing of the information were inconsistent in certain key respects. For example, we found that DRR contacted some, but not all, of the owners of the PII to allow them an opportunity to remove the information before it was destroyed. We also found that CSIRT was not always contacted when PII was discovered and that CSIRT did not always conduct formal investigations when PII was discovered. Further, the type of documentation that DRR retained as evidence of the destruction of PII varied considerably, and in some instances, PII that had been authorized to be destroyed was erroneously sent to an off-site storage facility.

The nature of PII found in ORE properties raises certain questions regarding the FDIC's responsibilities and obligations for handling the information. Unlike PII that DRR acquires in support of its mission (e.g., bank customer, depositor, and employee information that are considered records of failed institutions), PII acquired from ORE properties is typically left behind by businesses and individuals that may have no business relationship with the failed institution or the FDIC. We determined that a legal opinion is needed to clarify whether the PII:

- should be treated as a record of the failed institution, the personal property of the previous owner or occupant of the ORE property, or abandoned property;
- falls within the scope of federal, state, and local statutes and regulations and government-wide policy and guidance that address the handling and disposal of PII, and the extent to which the FDIC may, as a matter of policy, voluntarily comply with such criteria;
- is subject to any retention requirements; and
- should be reviewed to determine whether it is needed in connection with a criminal or civil investigation before the PII is destroyed.

Obtaining a legal opinion would reduce the risk of inconsistent handling and disposal practices, which can expose the FDIC to potential criticism. After obtaining a legal opinion, it would be prudent for the FDIC to review its existing policies, procedures, guidance, and training related to the handling and disposal of PII at ORE properties to determine whether changes are warranted. In addition, the FDIC should determine an appropriate disposition for certain PII that was identified in the ORE properties that were in our sample and sent to off-site storage.

Recommendations and Corporation Comments

Our report contains three recommendations addressed to the Director, DRR, that are intended to improve the FDIC's handling of PII found in ORE properties. In addressing the recommendations, the Director may need to coordinate with other organizations within the FDIC, such as the Legal Division and CIOO, that have responsibilities for handling PII-related risks and incidents. The Director, DRR, provided a written response, dated March 23, 2015, to a draft of this report. In the response, the Director concurred with all three of the report's recommendations and described planned and completed actions that were responsive to the recommendations.

In addition, we identified a potential control enhancement related to the FDIC's automated tools that were used to track and report information pertaining to ORE property site inspections. We are reporting this matter separately because it was not considered significant in the context of our audit results.

Contents

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, Virginia 22226

Office of Audits and Evaluations
Office of Inspector General

DATE: March 31, 2015

MEMORANDUM TO: Bret D. Edwards, Director
Division of Resolutions and Receiverships

/Signed/
FROM: Mark F. Mulholland
Assistant Inspector General for Audits

SUBJECT: *The FDIC's Controls for Identifying, Securing, and Disposing of Personally Identifiable Information in Owned Real Estate Properties* (Report No. AUD-15-004)

This report presents the results of our audit of the FDIC's controls for identifying, securing, and disposing of personally identifiable information (PII) in owned real estate (ORE) properties.[1] As the receiver of failed FDIC-insured financial institutions, the FDIC acquires ORE properties that are located throughout the United States and its territories. These properties include single-family homes, condominiums, office buildings, retail establishments, hotels, and undeveloped land (among other types of property). In some cases, ORE properties are found to contain personal property, including PII, that was left behind by the previous owner or occupant of the properties. Establishing controls to properly handle PII found in ORE properties is critical to mitigating the risk of an unauthorized disclosure that could lead to identity theft, consumer fraud, and potential legal liability or reputational damage to the Corporation.

The audit objective was to determine whether the FDIC has established internal controls to properly identify, secure, and dispose of PII at ORE properties. To address the objective, we reviewed federal statutes and regulations, government-wide policy and guidance, and FDIC policies, procedures, and guidance that relate to identifying and safeguarding PII, responding to potential or known breaches, establishing time periods for records retention, and disposing of PII. We also interviewed officials in the FDIC's Division of Resolutions and Receiverships (DRR), Division of Administration (DOA), Legal Division, and Chief Information Officer Organization (CIOO) who were involved in identifying, securing, and/or disposing of PII in ORE properties. In addition, we reviewed the FDIC's handling of PII found in 10 non-statistically sampled ORE properties.[2]

[1] Certain terms that are underlined when first used in this report are defined in Appendix 2, *Glossary of Key Terms*.

[2] A non-statistical sample is judgmental and cannot be projected to the population. See Appendix 1 for details regarding our sampling methodology.

We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix 1 of this report includes additional details about our objective, scope, and methodology; Appendix 2 contains a glossary of key terms; Appendix 3 contains a list of abbreviations and acronyms; Appendix 4 contains the Corporation's comments on this report; and Appendix 5 contains a summary of the Corporation's corrective actions.

BACKGROUND

When an insured financial institution fails, the FDIC establishes a receivership to (among other things) liquidate the institution's assets. In many cases, these assets include ORE properties. The FDIC may initially acquire an ORE property because it is on the books and records of a failed financial institution and, as such, becomes an asset of the receivership. The FDIC may also acquire an ORE property during the term of a receivership through the foreclosure process after a borrower of a failed financial institution defaults on a loan secured by real estate.[3] Within the FDIC, DRR has primary responsibility for liquidating assets in receivership. According to DRR records, the FDIC acquired and liquidated approximately 14,000 ORE properties between February 2007 (when the most recent financial crisis began) and December 31, 2014.

DRR's Approach to Handling PII in ORE Properties

DRR typically identifies PII in ORE properties through physical site inspections. DRR has engaged two national asset management firms—Prescient, Inc., and Quantum/G&A Joint Venture (collectively referred to in this report as the ORE contractors)—to manage, market, and dispose of ORE properties. As part of their responsibilities, the ORE contractors are required to conduct initial site inspections of properties assigned to them and to re-inspect properties every 30 days thereafter. Site inspections address such things as the condition and appearance of the property, security risks, health and safety issues, and signage. In May 2014, DRR issued a Guidance Memorandum, entitled *ORE Property Inspections, Property Maintenance, and Signage* (referred to in this report as the Guidance Memorandum), that required the ORE contractors to identify, report, safeguard, and destroy hard copy information and electronic equipment (such as computers, printers, fax machines, USB flash drives, and CD/DVDs) that may contain PII.

DRR assigns a Resolutions and Receiverships Specialist (referred to in this report as an Account Officer) to oversee the management, marketing, and sale of each ORE property. As part of their responsibilities, Account Officers must review site inspection reports prepared by the ORE contractors and ensure that liability issues, including those related to PII, are identified and properly addressed. Account Officers are also responsible for

[3] The FDIC may acquire ORE properties through other means. For example, a property may be "discovered" after an investor or taxing jurisdiction contacts the FDIC about a property. In addition, the FDIC may enter into a compromise, settlement, or deed-in-lieu-of foreclosure that results in the acquisition of an ORE property.

performing initial site inspections of ORE properties within 60 days of assignment, and annually thereafter, to ensure the properties are being properly maintained and marketed for sale.

When PII is identified in an ORE property, DRR's general approach is to secure the information (e.g., ensure that it is in a locked building, room, or cabinet) and arrange for its immediate destruction. DRR's May 2014 Guidance Memorandum states that the ORE contractors must notify FDIC officials, including Oversight Managers and Account Officers, whenever PII is found in an ORE property. In addition, the Guidance Memorandum states that ORE contractors and Account Officers must follow FDIC Circular 1360.9, *Protecting Sensitive Information*, which states that if PII is suspected or known to be lost or otherwise compromised, immediate notification must be made to the FDIC Help Desk/Computer Security Incident Response Team (collectively referred to in this report as CSIRT) and to the appropriate supervisor/Oversight Manager and division or office Information Security Manager (ISM) at the earliest available opportunity. The Circular also requires that the FDIC's *Data Breach Handling Guide* be followed for any loss, misuse, or unauthorized access of PII in order to reduce the potential harm or embarrassment to individuals and the Corporation.

The role of CSIRT is to provide technical assistance in investigating, reporting, resolving, and closing computer security and data loss incidents. When CSIRT is notified of an incident involving PII, CSIRT reviews and forwards the reported incident information to appropriate senior FDIC managers, the division or office ISM, Privacy Program staff, and the United States Computer Emergency Readiness Team (US-CERT) within the Department of Homeland Security. The ISM is responsible for following the *Data Breach Handling Guide*, to include completing an incident risk analysis/impact assessment (referred to this report as an impact assessment) that, among other things, considers the nature of the PII; the possibility of misuse; the likelihood that the incident may lead to harm; the ability to mitigate the risk of harm; the risk that the incident involved a breach; and the need for a mitigation strategy. The Privacy Program staff reviews the impact assessment and makes the final determination regarding whether an incident constitutes a breach of PII. After all incident-related activities have been completed and documented, the Privacy Program staff submits official incident closure information to CSIRT.

On a case-by-case basis, the DRR ISM and CSIRT consult with the Privacy Program staff and/or the Legal Division on privacy and legal issues, respectively. In addition, DRR's Internal Review staff may review PII-related incidents to determine their underlying causes and identify possible policy violations and internal control weaknesses that may have contributed to the incidents.

Statutes, Regulations, Policies, and Guidance

Congress has enacted a number of statutes, and federal agencies have issued numerous regulations, policies, and guidance aimed at safeguarding PII from unauthorized disclosure, responding to potential or known breaches, establishing timeframes for records retention, and disposing of such information. Relevant federal statutes include,

but are not limited to, the Privacy Act of 1974, the Federal Information Security Management Act (as amended in December 2014), the Health Insurance Portability and Accountability Act of 1996, and the Federal Deposit Insurance Act; relevant regulations include, for example, Parts 314 and 682 of title 16 of the Code of Federal Regulations (CFR), entitled *Standards for Safeguarding Customer Information* and *Disposal of Consumer Report Information and Records*, respectively; and relevant policy and guidance include Office of Management and Budget (OMB) memoranda and National Institute of Standards and Technology (NIST) security standards and guidelines. In addition, most states and territories have enacted statutes governing the handling of PII within their jurisdictions. Not all of these criteria are binding on the FDIC. However, we considered them in the performance of our audit because they define prudent business concepts and practices.[4]

The nature of PII found in ORE properties raises certain questions regarding the FDIC's responsibilities and obligations for handling the information. Unlike PII that DRR acquires in support of its mission (e.g., bank customer, depositor, and employee information that are considered records of a failed financial institution), PII acquired from ORE properties is typically left behind by businesses and individuals that may have no business relationship with the failed institution or the FDIC. Such PII can include a wide variety of information, such as personal tax returns, consumer credit applications, copies of drivers' licenses, and medical records. As a result, uncertainty exists regarding whether such information should be treated as a record of the failed institution, the personal property of the previous property owner or occupant, or abandoned property. It is also unclear whether PII found in ORE properties falls within the scope of federal, state, and local statutes and regulations and government-wide policy and guidance that impose various requirements, such as notifications when potential or known breaches occur and records retention periods. As discussed later, the answers to these questions can affect the FDIC's approach to handling PII in ORE properties.

Review of PII Found in ORE Properties

DRR identified PII in 10 ORE properties during the period February 20, 2014 through August 31, 2014. Seven of these properties were initially acquired and managed by the former East Coast Temporary Satellite Office (ECTSO) in Jacksonville, Florida, before they were transferred to the Dallas Regional Office between December 2013 and February 2014. The remaining three properties were initially acquired and managed by the Dallas Regional Office. Table 1 describes key information pertaining to the 10 ORE properties, including the dates that the properties were acquired, the dates that the PII was discovered, and the type of PII that was discovered. We reviewed the FDIC's handing of PII at each of these properties to determine the actions that were taken to identify, secure, and dispose of the information. The results of our review are described later in this report.

[4] Appendix 1 contains additional information about the criteria we considered during the audit.

Table 1: Ten ORE Properties Where PII Was Identified

Type of ORE Property	Date Acquired by the FDIC	Date Transferred to the Dallas Regional Office	Date PII Was Identified	Type of PII Identified
1. Warehouse	8/23/2013	12/11/2013	2/20/2014	Employee Records, Personal and Business Bank Statements, Unused Checks
2. Hotel	8/23/2013	12/11/2013	2/24/2014	Employee Records
3. Office Building	8/23/2013	2/27/2014	5/12/2014	Employee Records, Cancelled Checks, Title Records, Attorney Records, Diskettes
4. Restaurant/Bar	1/30/2014	N/A	5/16/2014	Insurance and Payroll Records, Bank Statements, Tax Records, Mortgage Statements
5. Gas Station and Shopping Center	8/23/2013	12/11/2013	2/28/2014	Employment Records, Paystubs with Social Security Numbers, Copies of Drivers' Licenses
6. Automobile Dealership	8/23/2013	12/23/2013	3/6/2014	Employee Records, Credit Applications
7. Residence	8/23/2013	12/11/2013	6/11/2014	Personal Checkbook
8. Residence and Out Buildings	5/31/2014	N/A	8/25/2014	Social Security Numbers, Names, Addresses, Death Certificates
9. Restaurant	5/16/2014	N/A	5/22/2014	Social Security Numbers, Credit Card Information, Business Records, Computers
10. Health Care Facility	8/23/2013	12/11/2013	4/3/2014	Personal Medical Information, such as Computerized Tomography (CT) Scans

Source: Office of Inspector General (OIG) analysis of FDIC records.

Audit Results

The FDIC established a number of internal controls during the course of our audit that were designed to properly identify, secure, and dispose of PII at ORE properties. Among other things, the FDIC held a training conference and issued formal guidance in May 2014 to its Account Officers and ORE contractors that addressed procedures for identifying, reporting, securing, and disposing of PII. The FDIC also modified its ORE contracts in October 2014 to specifically require that the contractors search for PII during every property site inspection. Although these control improvements are positive, they do not fully address our findings described below.

Our review of 10 non-statistically sampled ORE properties found that PII was often not identified in a timely manner and that practices for handling and disposing of the information were not consistent in certain key respects. The inconsistent practices we identified can be attributed, in part, to the need for a legal opinion that clarifies the FDIC's responsibilities and obligations for handling PII found in ORE properties. Inconsistent treatment of PII can expose the FDIC to potential criticism.

Based on the results of a legal opinion, it would be prudent for the FDIC to review its existing policies, procedures, guidance, and training related to the handling and disposal of PII at ORE properties to determine whether changes are warranted. Ensuring the adequacy of these controls is critical to mitigating the risk of an unauthorized disclosure of PII that could lead to identity theft, consumer fraud, and potential legal liability or reputational damage to the Corporation. In addition, the FDIC should determine an appropriate disposition for certain PII that was identified in the ORE properties that were in our sample and sent to off-site storage.

Finally, we identified a potential control enhancement related to the FDIC's automated tools that were used to track and report information pertaining to ORE property site inspections. We are reporting this matter separately because it was not considered significant within the context of our audit results.

The FDIC's Practices for Identifying, Securing, and Disposing of PII in ORE Properties

We reviewed the FDIC's handling of PII at 10 non-statistically sampled ORE properties and found that the Corporation's practices for identifying, securing, and disposing of the information were not consistent in the following key respects.

Identifying PII. The amount of time that elapsed between the date that the FDIC acquired the ORE property and the date that the PII was discovered ranged from 1 week to 6 months. Notably, seven of the properties that involved the longest period of time to identify PII were transferred from the former ECTSO to the Dallas Regional Office during the period December 2013 through February 2014. In all seven cases, the PII was identified through site inspections conducted by the Dallas Regional Office about 60 days after the properties were transferred from the ECTSO.

Securing PII. Although not required by policy or guidance, the Account Officer contacted the owner of the PII for 3 of the 10 ORE properties to allow the owner an opportunity to remove the PII before it was destroyed. In two of these instances, the owner chose to remove the PII from the property. In addition, although not required by policy or guidance, the Account Officer conducted an inventory of the PII at 1 of the 10 ORE properties before it was destroyed.

Account Officers contacted the CSIRT for all but 1 of the 10 ORE properties.[5] CSIRT opened an incident and conducted an investigation for six of the nine properties about which it was contacted. CSIRT did not open an incident or conduct an investigation for the remaining three properties because CSIRT personnel believed that doing so was not necessary.[6]

Disposing of PII. The FDIC obtained contractor invoices to evidence the destruction of PII at all six of the ORE properties where PII was destroyed. The FDIC also obtained a certificate of destruction for three of these same six properties. In general, the contractor invoices contained much less information about the PII that was destroyed, where it was destroyed, and how it was destroyed than the certificates of destruction. We also noted that for one of these six properties, neither the contractor invoice nor the certificate of destruction referenced the shredding of hard copy PII that took place. Further, we noted three instances in which an FDIC official had authorized the destruction of electronic PII by Cascade Asset Management, LLC (Cascade)—the FDIC's national contractor for data and electronic equipment disposition services—but the PII was erroneously sent to an off-site storage facility. Table 2 summarizes our analysis of evidence supporting the destruction of PII for the 10 ORE properties in our sample.

Table 2: Evidence Confirming the Destruction of PII

ORE Property	Format of PII	Certificate of Destruction Obtained	Invoice Retained	Electronic PII Sent to Off-site Storage
1. Warehouse	Hard Copy and Electronic	For Hard Copy Only	For Hard Copy and Electronic	
2. Hotel	Hard Copy and Electronic		For Hard Copy Only	✓
3. Office Building	Hard Copy and Electronic	For Hard Copy and Electronic	For Hard Copy and Electronic	
4. Restaurant/Bar	Hard Copy		Hard Copy	
5. Gas Station and Shopping Center	Hard Copy and Electronic			✓
6. Automobile Dealership	Hard Copy and Electronic		For Hard Copy and Electronic	
7. Residence*	Hard Copy			
8. Residence and Out Buildings	Hard Copy and Electronic	For Hard Copy and Electronic	For Hard Copy and Electronic	
9. Restaurant*	Hard Copy			
10. Health Care Facility	Electronic			✓

Source: OIG analysis of FDIC records.
* The FDIC contacted the owner of the PII who removed it before it was destroyed.
✓ The PII was erroneously sent to off-site storage.

[5] The Account Officer determined that contacting CSIRT for the remaining ORE property would not be beneficial because the building containing the PII was secured and a breach appeared unlikely.
[6] We did not independently assess the appropriateness of CSIRT's decisions about whether to open an incident and conduct an investigation because a review of CSIRT's internal controls was not within the scope of this audit.

In addition, DRR did not always maintain a chain of custody over the PII by obtaining a receipt when the PII was turned over to a contractor for destruction or ensuring that an FDIC employee was present during the destruction process.

Factors Impacting the FDIC's Handling of PII at ORE Properties

The inconsistent practices described above were caused primarily by: (a) weaknesses in the property site inspection process, (b) guidance to Account Officers and ORE Contractors that did not fully address how to handle and dispose of PII at ORE properties, and (c) a lack of a comprehensive legal opinion that clarifies the FDIC's responsibilities and obligations pertaining to PII at ORE properties. A description of these causes follows.

Site Inspection Process

In early 2014, DRR determined that its site inspections of ORE properties were generally not effective in identifying and addressing liability issues, including the presence of PII. This concern was highlighted when several ORE properties that were transferred from the former ECTSO to the Dallas Regional Office were subsequently found to contain PII. In each case, the inspections of the properties by the ECTSO either did not identify the PII or ensure that the liability risks associated with PII discoveries were addressed. A review of the circumstances pertaining to these properties by DRR's Internal Review staff in early 2014 concluded that internal controls over the property site inspection process, including controls for identifying and addressing PII, were not adequate. Among other things, Internal Review staff concluded that guidance for performing site inspections did not adequately address PII; Account Officers did not always conduct timely site inspections; and inspectors did not always enter properties during site inspections.

To address the weaknesses described above, DRR held a training conference and issued its Guidance Memorandum to the ORE Contractors and Account Offices in May 2014. The Guidance Memorandum established detailed procedures for identifying PII at ORE properties. DRR also modified its property site inspection checklists to specifically address PII and issued a Quick Reference Guide that described a "zero tolerance" policy for PII, meaning that property inspectors should always presume that electronic equipment contains PII and that any doubts about hard copy documents should always result in a determination that the information contains PII. In addition, DRR modified its ORE contracts in October 2014 to require the contractors to search for PII during site inspections. The contract modifications also accelerated the amount of time that the ORE contractors have to perform their initial site inspections for certain higher-risk properties that are more likely to contain PII from 21 to 7 days. Collectively, these control improvements significantly improved the FDIC's ability to properly identify PII at ORE properties.

Guidance for Handling and Disposing of PII

Prior to the spring of 2014, DRR had issued limited guidance to its Account Officers and ORE Contractors that addressed their responsibilities for handling and disposing of PII at ORE properties. DRR guidance focused primarily on the handling and disposal of PII in bank owned and leased premises.[7] In March 2014, DRR updated its Job Aid, entitled *How to Manage and Market Real Estate*, to require that Account Officers check for hard copy PII at ORE properties. In addition, the Guidance Memorandum and Quick Reference Guide issued in May 2014 defined procedures for alerting FDIC officials to PII discoveries, securing PII when it is found, and shredding hard copy PII.

While the guidance issued in March and May 2014 was positive, existing guidance does not address certain aspects of handling and disposing of PII at ORE properties. For example, existing guidance does not address the circumstances under which the owner of the PII should be contacted and afforded an opportunity to remove the PII before it is destroyed. Existing guidance also does not address when it is appropriate to prepare an inventory of the PII, nor does it address the type of documentation that should be retained as evidence of the destruction of PII. Further, existing guidance does not indicate when it would be appropriate to engage Cascade to destroy electronic PII.

Policies, procedures, and guidance are an important internal control for ensuring that processes are repeatable, consistent, and disciplined and for reducing operational risk associated with changes in staff. This concept is consistent with the Government Accountability Office's *Standards for Internal Control in the Federal Government* and FDIC Circular 4010.3, *FDIC Enterprise Risk Management System*.

Legal Opinion

As described in the Background section of this report, the nature of PII found in ORE properties raises questions about the FDIC's responsibilities and obligations for handling the information. Such questions include:

- Should the PII be treated as a record of the failed institution, the personal property of the previous owner or occupant of the ORE property, or abandoned property?

- Does the PII fall within the scope of federal, state, and local statutes and regulations and government-wide policy and guidance related to safeguarding PII, responding to known or potential breaches, and disposing of the information? To what extent may the FDIC, as a matter of policy, voluntarily comply with such criteria?

- What retention requirements (if any) apply to the PII?

[7] Such guidance is reflected in the *Failed Financial Institution Closing Manual*, dated October 2012; the *DRR Asset Resolution Manual*, dated May 9, 2011; and the DRR Job Aid, entitled *How to Manage and Market Real Estate*, dated November 11, 2011.

- Should research be performed to determine whether the PII may be needed in connection with a criminal or civil investigation before the information is destroyed?

DRR officials informed us that they have, on a case-by-case basis, obtained informal advice from the Legal Division on issues involving PII in ORE properties. In some cases, for example, attorneys in the Legal Division have orally advised DRR officials to contact the owners of the PII and request that they remove the information before it is destroyed.

Obtaining an opinion from the Legal Division that addresses the questions described above would be a prudent business practice. Among other things, it would provide a legal basis for the FDIC's approach to handling and disposing of PII at ORE properties and promote a consistent understanding among corporate officials regarding the FDIC's responsibilities and obligations for handling the information. A legal opinion would also help to inform DRR about whether changes in existing internal controls for identifying, securing, and disposing of PII are warranted, such as whether US-CERT should continue to be notified of breaches and whether an impact assessment should continue to be conducted when PII has already been destroyed. In this regard, DRR may need to coordinate with other organizations within the FDIC, such as the CIOO, that have responsibilities for handling PII at ORE properties. Absent a legal opinion, there is an increased risk that PII will not be handled in a consistent manner, exposing the FDIC to potential criticism.

Recommendations

We recommend that the Director, DRR:

1. Obtain an opinion from the FDIC Legal Division that clarifies the FDIC's responsibilities and obligations for handling PII at ORE properties. At a minimum, the opinion should clarify whether the PII:

    a. should be treated as a record of the failed institution, the personal property of the previous owner or occupant of the ORE property, or abandoned property;
    b. falls within the scope of federal, state, and local statutes and regulations and government-wide policy and guidance addressing PII and the extent to which the FDIC may, as a matter of policy, voluntarily comply with such criteria;
    c. is subject to any retention requirements; and
    d. should be researched to determine whether it may be needed in connection with a criminal or civil investigation before the information is destroyed.

2. Review and update, as appropriate, existing policies, procedures, guidance, and training related to identifying, securing, and disposing of PII at ORE properties.

3. Determine the appropriate disposition of the PII that was identified at three of the ORE properties reviewed during the audit and that is currently in off-site storage.

Corporation Comments and OIG Evaluation

The Director, DRR, provided a written response, dated March 24, 2015, to a draft of this report. The response is presented in its entirety in Appendix 4. In the response, the Director concurred with all three of the report's recommendations. Subsequent to the response, a DRR official informed us that action to address Recommendation 3 was completed on March 25, 2015. The official provided us with documentation evidencing the actions taken. A summary of the Corporation's corrective actions is presented in Appendix 5. The planned and completed actions are responsive to the recommendations and the recommendations are resolved.

Objective, Scope, and Methodology

Objective

The audit objective was to determine whether the FDIC has established internal controls to properly identify, secure, and dispose of PII in ORE properties.

We conducted this performance audit from April through December 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Scope and Methodology

To address the audit objective, we reviewed federal laws and regulations, government-wide policy and guidance, and FDIC policies, procedures, and guidance that relate to identifying and safeguarding PII, responding to potential or known breaches, establishing time periods for records retention, and disposing of such information. A list of the salient criteria that we reviewed is reflected below. Not all of these criteria are binding on the FDIC. As a result, we did not assess the FDIC for compliance with the criteria. However, we did consider these criteria in the performance of our audit because they define prudent business practices and concepts.

Federal Statutes and Regulations

- The Privacy Act of 1974, as amended
- The Health Insurance Portability and Accountability Act of 1996, as amended
- The Federal Deposit Insurance Act, as amended
- The Records Management Act, as amended
- The Federal Information Security Management Act, as amended in December 2014
- Parts 314 and 682 of title 16 of the CFR, entitled *Standards for Safeguarding Customer Information* and *Disposal of Consumer Report Information and Records*, respectively
- Part 360 of title 12 of the CFR, entitled *Records of Failed Insured Depository Institutions*

Government-wide Policies and Guidance

- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost of Security in Agency Information Technology Investments*[8]
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*
- NIST security standards and guidelines

FDIC Policies, Procedures, and Guidance

- Circular 1360.9, *Protecting Sensitive Information*, dated April 30, 2007
- Circular 1360.12, *Reporting Computer Security Incidents*, dated June 26, 2003
- Circular 1360.20, *FDIC Privacy Program*, dated March 12, 2013
- Circular 1210.1, *FDIC Records and Information Management (RIM) Policy Manual*, dated July 2, 2012
- DRR Circular 7100.2, *Maintenance and Protection of Bank Employee and Customer Personally Identifiable Information*, dated June 13, 2007
- *FDIC Data Breach Handling Guide*, Version 1.0, dated December 18, 2013
- *FDIC DIT Privacy Program Strategic Framework*, dated August 2012
- *DRR Failed Financial Institution Closing Manual*, dated April 22, 2010
- *DRR Asset Resolution Manual*, dated May 9, 2011
- DRR ORE/OOA FF&E Section Procedures, dated June 11, 2014
- DRR Job Aid, *How to Manage and Market ORE Assets*, dated November 18, 2011 and updated March 26, 2014
- DRR's Guidance Memorandum, *ORE Property Inspections, Property Maintenance, and Signage,* and *FDIC PII/SI Quick Reference Guide* issued in May 2014
- DRR's *Assuming Institution Procedures for Bank Premises, ATMs, Leased Data Management Equipment, Receivers Deeds* (undated)
- DRR's *Guidelines for ORE Contractor Access to Bank Premises Prior to Issuance of PII Certificate*, dated January 17, 2011
- Draft *DRR ORETracker User Guide*, as of December 19, 2014
- DRR draft manual, *Owned Real Estate,* as of May 5, 2014

To obtain an understanding of the internal controls that the FDIC had established to identify, secure, and dispose of PII at ORE properties, we:

- reviewed relevant FDIC policies, procedures, guidance, job aids, training materials, and provisions of ORE contracts;

[8] This OMB memorandum and the preceding memorandum were subsequently updated by OMB Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*.

- interviewed DRR, CIOO, DOA, and Legal Division officials who had responsibility for designing, implementing, and reviewing controls for identifying, securing, and disposing of PII at ORE properties; and

- attended DRR's national training conference for ORE Contractors and Account Officers held on May 14, 2014.

In addition, we reviewed the FDIC's handling of PII found in 10 non-statistically sampled ORE properties to determine the actions that were taken to identify, secure, and dispose of the information. A non-statistical sample is judgmental and cannot be projected to the population. The 10 ORE properties represented all properties where DRR had identified PII during the period February 20, 2014 through August 31, 2014. DRR identified one additional ORE property where potential PII had initially been identified. However, it was later determined that the property did not contain PII, and as a result, we did not include the property in our sample. Further, seven of the 10 ORE properties were initially acquired and managed by the former ECTSO before they were transferred to the Dallas Regional Office between December 2013 and February 2014. Because the ECTSO closed in April 2014, we were not able to speak with the original Account Officers to discuss their oversight and management of the properties. In addition, information about these properties in ORETracker was limited.[9]

For each sampled ORE property, we interviewed key officials, including the DRR ISM and Account Officer, about the actions they took to identify, report, secure, and dispose of the PII; reviewed relevant documents, such as site inspection reports prepared by ORE contractors and Account Officers, impact assessments prepared by the DRR ISM, investigative materials and communications involving CSIRT, and records evidencing the destruction of PII. A review of CSIRT's internal controls was not within the scope of this audit. Our review of CSIRT activities was generally limited to determining whether CSIRT had been notified of the discovery of PII for our sample ORE properties and determining whether CSIRT decided to open an incident and conduct an investigation. We did not independently assess the appropriateness of CSIRT's decisions about whether to open incidents and conduct investigations. We also analyzed relevant information, such as property acquisition, assignment, and site inspection dates and results, in ORETracker and DRR's *Summary of Property Inspections*.[10]

With respect to information systems, we relied on certain data in ORETracker to identify property-specific information, such as location, date of acquisition, and site inspection

[9] ORETracker is an automated application that maintains asset management information pertaining to properties assigned to ORE contractors. Among other things, the application tracks the date that the property was assigned to the ORE contractor, the date of the most recent site inspection, and general comments about the condition of the property.

[10] The *Summary of Property Inspections* is an automated management reporting tool that maintains information pertaining to site inspections performed by DRR Account Officers. The tool includes such information as inspection dates and general comments about ORE properties, including whether liability issues (such as the presence of PII) exist.

status. Where the data were significant to our audit results, we corroborated the data to the extent possible with information from other sources, such as documentation and testimonial evidence. We determined that some of the information in ORETracker was not current, accurate, and complete. However, the data reliability issues we found did not affect our ability to address the audit objective or support our findings and conclusions. In this regard, we identified a potential control enhancement related to ORETracker and the *Summary of Property Inspections* that were used to track and report information about site inspections of ORE properties. We are reporting this matter separately because it was not considered significant in the context of our audit results. In addition, we assessed the risk of fraud and abuse related to our audit objective in the course of evaluating the audit evidence.

Finally, we followed up on recommendations related to our audit objective that were contained in a prior FDIC OIG audit report, entitled *DRR's Controls for Managing, Marketing, and Disposing of Owned Real Estate Assets* (Report No. AUD-13-001), dated October 5, 2012. We performed our audit work at the FDIC's offices in Dallas, Texas, and Arlington, Virginia.

Glossary of Key Terms

Term	Definition
Abandoned Property	Personal property left by an owner who intentionally relinquishes all rights to its control. Real property may not be abandoned. Many jurisdictions have statutes that modify the common law's treatment of abandoned property.
Breach	An incident in which sensitive information, such as PII, has been lost, compromised, acquired, disclosed, or accessed without authorization, or any similar incident where persons other than authorized users and for other than authorized purposes have access or potential access to sensitive information.
Certificate of Destruction	A document confirming that something (in the context of this audit, hard copy and electronic information) has been ruined, annihilated, or put out of existence.
Computer Security Incident Response Team	A team of computer security professionals established by the FDIC to provide centralized technical assistance to effectively investigate, resolve, and close computer security vulnerabilities and incidents.
Data Breach Handling Guide	A document describing how the FDIC addresses data breaches and incidents involving sensitive information, including PII. The guide includes the key definitions, roles and responsibilities, and step-by-step procedures.
Incident	An adverse event or situation that poses a threat to the confidentiality, integrity, or availability of the FDIC's information systems, network, or data.
Information Security Managers	Individuals designated by FDIC division directors to serve as the primary liaison to support the FDIC Privacy Program and work with security staff in the CIOO. ISMs are divisional points of contact for matters involving the investigation of reported breaches involving PII.
National Institute of Standards and Technology	A non-regulatory federal agency within the Department of Commerce. As part of its responsibilities, NIST develops and publishes technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive, but unclassified, information in federal computer systems.
Owned Real Estate	Real property owned by a lender—typically a financial institution, government agency, or government loan insurer.
Personally Identifiable Information	Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records (e.g., fingerprint or voice print), alone, or when combined with other personal information which is linked or linkable to a specific individual,

Glossary of Key Terms

	such as date and place of birth or mother's maiden name.
Privacy Program Staff	Staff that implement and manage, on behalf of the FDIC Chief Privacy Officer, a comprehensive set of privacy and data protection policies and procedures designed to promote robust and effective privacy protection throughout the Corporation.
Records of a Failed Financial Institution	When acting as the receiver of a failed insured financial institution, the FDIC succeeds to the books and records of the institution. The FDIC's regulation at 12 CFR 360, *Records of Failed Insured Depository Institutions*, defines the term record as any reasonably accessible document, book, paper, map, photograph, microfiche, microfilm, computer or electronically-created record generated or maintained by an insured institution in the course of and necessary to its transaction of business. This regulation states that the FDIC in its discretion will consider certain factors defined in the regulation when determining whether particular documentary material obtained from a failed institution is a record for purposes of the Federal Deposit Insurance Act.
United States Computer Emergency Readiness Team	Housed within the U.S. Department of Homeland Security, US-CERT strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world. The Federal Information Security Management Act, as amended in December 2014, requires agencies to report security incidents to US-CERT. Within the FDIC, CSIRT is responsible for notifying US-CERT of incidents, as appropriate, within OMB-mandated and US-CERT established timeframes.

Abbreviations and Acronyms

Abbreviation/Acronym	Explanation
CFR	Code of Federal Regulations
CIOO	Chief Information Officer Organization
CT	Computerized Tomography
CSIRT	Computer Security Incident Response Team
DOA	Division of Administration
DRR	Division of Resolutions and Receiverships
ECTSO	East Coast Temporary Satellite Office
FDIC	Federal Deposit Insurance Corporation
ISM	Information Security Manager
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
ORE	Owned Real Estate
PII	Personally Identifiable Information
RIM	Record Information Management
US-CERT	United States Computer Emergency Readiness Team

Corporation Comments

550 17th Street NW, Washington D.C. 20429-9990 Division of Resolutions and Receiverships

March 24, 2015

TO: Mark F. Mulholland
Assistant Inspector General for Audits
Office of Inspector General

FROM: Bret D. Edwards, Director /**Signed**/
Division of Resolutions and Receiverships

SUBJECT: Management Response to Draft Audit Report Entitled, *The FDIC's Controls for Identifying, Securing, and Disposing of Personally Identifiable Information in Owned Real Estate Properties* (Assignment No. 2014-033)

The Federal Deposit Insurance Corporation (FDIC) has completed its review of the Office of Inspector General's (OIG) draft audit report entitled *The FDIC's Controls for Identifying, Securing, and Disposing of Personally Identifiable Information in Owned Real Estate Properties* (Assignment No. 2014-003) dated February 27, 2015. We appreciate the OIG's observations and recommendations to enhance the controls around the management and disposition of personally identifiable information (PII) that is discovered in owned real estate (ORE) properties acquired as a result of resolution and receivership activities.

In its report, the OIG indicates that the Division of Resolutions and Receiverships (DRR) strengthened its existing controls during the course of the audit that are designed to properly identify, secure, and dispose of PII discovered in ORE properties. We agree with the OIG about the need to address certain issues identified during the course of the audit, especially and including procuring legal guidance regarding the appropriate handling of discovered PII in such properties. As we work closely with the Legal Division over the next several months, we will modify our current procedures on an interim basis where appropriate.

Below is a description of the FDIC's specific corrective actions for each OIG recommendation.

Recommendation 1: Obtain an opinion from the FDIC Legal Division that clarifies the FDIC's responsibilities and obligations for handling PII at ORE properties. At a minimum, the opinion should clarify whether the PII:

a. should be treated as a record of the failed institution, the personal property of the previous owner or occupant of the ORE property, or abandoned property;
b. falls within the scope of federal, state, and local statutes and regulations and government-wide policy and guidance addressing PII and the extent to which the FDIC may, as a matter of policy, voluntarily comply with such criteria;
c. is subject to any retention requirements; and
d. should be researched to determine whether it may be needed in connection with a criminal or civil investigation before the information is destroyed.

Corporation Comments

Management Response: DRR concurs with the recommendation.

Corrective Action: The Legal Division is preparing an opinion that addresses this recommendation.

Completion Date: July 31, 2015.

Recommendation 2: Review and update, as appropriate, existing policies, procedures, guidance, and training related to identifying, securing and disposing of PII at ORE properties.

Management Response: DRR concurs with the recommendation.

Corrective Action: After we receive the legal opinion, all related policies, procedures, training, and guidance will be revised accordingly. Additionally, we plan to consult with the FDIC's Chief Privacy Officer to determine whether additional changes to existing internal controls for identifying, securing, and disposing of PII at ORE properties are warranted and whether we should continue to conduct a formal impact assessment in instances where the PII discovered in ORE has already been destroyed.

Completion Date: January 31, 2016.

Recommendation 3: Determine the appropriate disposition of the PII that was identified at three of the ORE properties reviewed during the audit and that is currently in off-site storage.

Management Response: DRR concurs with the recommendation.

Corrective Action: We will research the subject PII, determine the appropriate method of disposition, and execute accordingly.

Completion Date: May 22, 2015.

2

Summary of the Corporation's Corrective Actions

This table presents corrective actions taken or planned by the Corporation in response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

Rec. No.	Corrective Action: Taken or Planned	Actual/ Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	DRR will obtain a written opinion from the Legal Division that addresses the recommendation.	7/31/15	$0	Yes	Open
2	After receiving the legal opinion referenced in Recommendation 1, DRR will revise its policies, procedures, training, and guidance accordingly. Additionally, DRR will consult with the Chief Privacy Officer to determine whether additional changes to existing internal controls are warranted and whether DRR should continue to conduct a formal impact assessment in instances where PII discovered in ORE properties has already been destroyed.	1/31/16	$0	Yes	Open
3	DRR researched the subject PII and determined that it should be destroyed. DRR provided a certificate of destruction to evidence that the PII had been destroyed.	3/25/15	$0	Yes	Closed

[a] Resolved –(1) Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when (a) Corporate Management Control notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, when the OIG confirms that corrective actions have been completed and are responsive.