Citywide
Federal Red Flags Rule Compliance
(Identity Theft Protection Programs)
May 18, 2020

Report Highlights

Governance
The City established the Privacy Oversight Council and defined policy to address federal compliance. Compliance can be strengthened through ongoing monitoring, and coordination of periodic assessments.

Departmental Programs
Three of the four impacted departments had appropriately updated their compliance programs, and monitored for incidents of identity theft. The fourth department had a compliant program the previous fiscal year, and can update its program for current-year compliance.

City Auditor Department
140 N 3rd Avenue Phoenix, AZ 85003
602-262-6641 (TTY use 7-1-1)
Executive Summary

Purpose

Our purpose was to evaluate compliance with the Federal Red Flags Rule (Rule) for all departments that extend credit (provide a service without receiving immediate payment) and have accounts for individuals.

Background

The Federal Trade Commission (FTC) issued regulations requiring certain organizations to implement identity theft prevention programs under the Fair and Accurate Transaction Act of 2003. This act is also referred to as the Red Flags Rule (16 CFR Part 681). The Rule requires businesses and organizations to implement a written Identity Theft Prevention Program (Program). We last evaluated City compliance with the Rule in 2014 and found that the City needed to improve overall governance (Red Flags, #1140094). We also found that most departments still needed to formally develop and regularly maintain their Programs.

Results in Brief

The City should strengthen ongoing monitoring of Citywide compliance and coordination of periodic assessments.

The City established the Privacy Oversight Council and defined policy to address compliance. The Chief Privacy Officer oversees City compliance with the Rule and the ongoing monitoring and coordination of periodic assessments. Periodic assessments have been incorporated into the annual privacy information management plan process where departments identify sensitive and confidential information they store, process, or maintain. However, the information management plan process does not incorporate elements of the Rule to properly assess and evaluate departments on a continual basis.

Not all impacted departments had updated their Rule Program; therefore, the City was not compliant with the Rule.

Three of the four impacted departments submitted updated Rule Programs, with the exception of the Aviation Department. In lieu of an updated Program, we reviewed Aviation’s documentation for the previous year. Overall, the Programs contained the required elements required by the Rule.
## Department Responses to Recommendations

### Rec. #1.1: ISPO – implement a process to periodically review what departments or functions are subject to the Red Flags Rule. As the Privacy Oversight Council determines a department is newly subject to or is no longer subject to the Rule, maintain documentation justifying the change.

**Response:** Per A.R. 1.95 – Privacy Program, the Law Department is responsible to “Review applicable laws with which the City must comply.” Determining which departments are subject to Red Flags Rules requires an interpretation of the most recent Red Flags Act - the Red Flags Program Clarification Act of 2010 (RFPCA). By May 29, 2020, ITS will develop and make a request to the Law Department to review the RFPCA in relation to requirements for City Departments. Further action will be dependent on the results of the analysis.

**Target Date:** May 29, 2020

**Explanation, Target Date > 90 Days:** N/A

### Rec. #1.2: ISPO – update the annual information management plan process to specifically identify utility accounts, mortgage loans, or other types of accounts typically subject to the Red Flags Rule. Include the qualifying questions outlined by the Federal Trade Commission to assist departments in determining Rule compliance.

**Response:** The ISPO will update the information management plans according to the applicable RFPCA requirements, such as account type and qualifying questions, as determined by the Law Department. The target date is contingent on Law having completed their review of the RFPCA (per #1.1) within 60 days.

**Target Date:** August 10, 2020

**Explanation, Target Date > 90 Days:** N/A

### Rec. #1.3: Law Department – appoint a designated subject matter expert to assess departments on an annual basis for Rule compliance and to document assessments.

**Response:** The Law Department is assigning three positions to annually assess Rule compliance as a committee, and to create continuity in the position. The Chief Counsel, Assistant Chief Counsel of the Finance and Public Services Section and an attorney either assigned to the Water or IT departments. Currently the committee will be Julie Kriegh and Stephen Wetherell. The people may change as the assignments in law change and new people are hired or moved. This is the reason for assigning specific positions rather than people.

**Target Date:** Completed

**Explanation, Target Date > 90 Days:** N/A
**Rec. #2.1:** Aviation Department – submit an updated Rule Program and documentation that supports compliance with the Rule.

**Response:** FMD will work with Law Department and the Privacy Oversight Council (POC) to determine if Aviation is subject to Red Flag Rule Compliance. If Aviation is subject to compliance, then Aviation will submit an updated program and associated documentation. If Aviation does not need to comply with the Rule, then Aviation will provide the POC’s decision.

<table>
<thead>
<tr>
<th><strong>Response</strong></th>
<th><strong>Target Date:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>FMD will work with Law Department and the Privacy Oversight Council (POC) to determine if Aviation is subject to Red Flag Rule Compliance. If Aviation is subject to compliance, then Aviation will submit an updated program and associated documentation. If Aviation does not need to comply with the Rule, then Aviation will provide the POC’s decision.</td>
<td>March 19, 2021</td>
</tr>
</tbody>
</table>

**Explanation, Target Date > 90 Days:** Additional time is needed to schedule this item on the POC agenda. This could take one year. Recently, the POC has only met annually.
1 – Red Flags Rule Compliance – Governance

Background

In order to be compliant with the Rule, entities must complete several general steps based on the size, complexity, and nature of their operations. The FTC has issued guidelines to assist entities in developing their Program. The guidelines were designed to provide flexibility to individual organizations in adopting their Programs.

Entities should conduct an initial risk assessment to determine the level of risk for identity theft. The risk assessment identifies the types of covered accounts, methods used to open and access the accounts, and any previous experience of identity theft. Every creditor is expected to conduct a periodic risk assessment to identify covered accounts. Once the risk has been determined, a Program must be developed.

The Rule contains specific requirements about the administration of an organization’s Program, including:

- Approval of the Program(s) by executive management
- Designation of accountability for oversight (person at senior management level)
- Mandatory staff training
- Supervision of third-party providers (where applicable)
- Periodic reassessment and updates to the Program(s)

The Program must include a policy that addresses the warning signs of identity theft or “red flags.” The policy must include the following steps:

- Identify relevant red flags (risks that may occur at the organization)
- Detect red flags (procedures to detect the red flags that have been identified)
- Respond to red flags (procedures to respond if the red flags are detected)
- Mitigate red flags (procedures to minimize the occurrence of identity theft)

The City established the Privacy Oversight Council to set direction for privacy and identity theft protection strategies and initiatives. The roles and responsibilities of the Council and the City’s Privacy Program are outlined in Administrative Regulation 1.95 – Privacy Program. In addition, City IT Standard b1.9 – Red Flags Rule defines the key elements of a Rule Program and provides guidance to comply with the City’s Rule requirements.
Results

The City established a governance body, the Privacy Oversight Council; however, a subject matter expert needs to be identified within the Law Department to provide guidance to departments.

The Privacy Oversight Council governs privacy and identity theft protection strategies and initiatives. The Privacy Oversight Council is composed of personnel from the City Clerk Department, Human Resources Department, Law Department, Public Information Office, and the Information Security and Privacy Office (ISPO). In addition to serving on the Privacy Oversight Council, the Law Department is responsible for reviewing applicable laws with which the City must comply. In a previous audit, we noted that attorneys from the Law Department had been working on interpretation of the Rule but had not designated a “subject matter expert” (SME) regarding the Rule. As a result, the Law Department designated a SME to provide guidance. However, this individual recently departed the City and a successor has yet to be determined. As a result, departments and their attorneys may interpret the Rule differently. Implementing a central point of contact would minimize the risk of inconsistent Rule interpretation and streamline communication between the Law Department and other departments.

Controls to appropriately identify departments subject to the Rule require strengthening.

Entities must perform periodic risk assessments to determine whether they should comply with the Rule. To assess risk, ISPO relies on the information obtained through the annual Information Management Plan (IMP) process. The IMP process requires departments to identify sensitive and confidential information it stores, processes, or maintains and to document controls in place to safeguard information.

Although the IMP process does require departments to identify financial accounts, such as credit/debit cards, checking/savings accounts, and/or retirement account numbers; it does not specifically call out other accounts that may be applicable to the Rule, such as utility accounts or mortgage loans. In addition, the IMP process does not include qualifying questions, to help determine if a department is subject to the Rule. The resulting risk is that each department may not be assessed accurately to determine whether it must comply with the Rule.

Controls to reevaluate departments for Rule compliance require strengthening.

The Rule also requires periodic identification of covered accounts to determine whether an entity offers or maintains covered accounts. To assess covered accounts and further determine who must comply with the Rule, City departments work with the Law Department. However, this does not occur on a continual basis as evaluations are inconsistent. The Housing Department last worked with the Law Department in 2014, where it was determined that the department did not meet the criteria of a “creditor,” nor did it have any “covered accounts” as defined under the Rule. As a result, the Housing Department has used this evaluation to support its exemption from the Rule. Inconsistent identification may not consider changes to business processes or reflect changes in risks to customers as required by the Rule.
In addition, the Aviation Department has been subject to the Rule based on deferred payments for general Aviation customers. However, both the Aviation Department and its Law Department representative were unable to determine if this criterion still applied. The resulting risk is the Aviation Department may go through the cost of compliance when it is not required and may not offer any benefit.

Recommendations

1.1 ISPO – implement a process to periodically review what departments or functions are subject to the Red Flags Rule. As the Privacy Oversight Council determines a department is newly subject to or is no longer subject to the Rule, maintain documentation justifying the change.

1.2 ISPO – update the annual information management plan process to specifically identify utility accounts, mortgage loans, or other types of accounts typically subject to the Red Flags Rule. Include the qualifying questions outlined by the Federal Trade Commission to assist departments in determining Rule compliance.

1.3 Law Department – appoint a designated subject matter expert to assess departments on an annual basis for Rule compliance and to document assessments.
2 – Red Flags Rules Compliance – Individual Departments

Background

At the time of our prior audit (February 13, 2014), eight departments/ functions were identified as having to comply with the Rule:

- Aviation
- Community & Economic Development – Expand (CEDD-Expand)
- Community & Economic Development – PCDIC (CEDD-PCDIC)
- Housing
- Neighborhood Services
- Public Transit
- Public Works
- Water Services

Since 2014, the CEDD-Expand function was incorporated into Neighborhood Services, the CEDD-PCDIC function was outsourced to a third party, and the Law Department deemed that both Housing and Public Works were no longer subject to the Rule. No City functions were added to the compliance list. As such, we validated Rule compliance in the Aviation, Neighborhood Services, Public Transit, and Water Services departments.

Results

*Not all impacted departments had updated their Rule Program; therefore, the City was not compliant with the Rule regulations.*

We evaluated the Rule Programs and supporting documentation from Aviation, Neighborhood Services, Public Transit, and Water Services against the federal requirements of the Rule. All departments, with the exception of Aviation, had submitted the required updated documentation for FY 19/20. Due to staffing changes within Aviation and the transition of responsibilities to other staff, program documentation was not completed for FY19/20, therefore we evaluated documentation submitted for FY 18/19 by Aviation. For FY 19/20, Water Services reported three incidents of identity theft, no other department reported incidents. Water Services appropriately handled the incidents according to their policy.
### Impacted Departments

<table>
<thead>
<tr>
<th>Department</th>
<th>Program Developed</th>
<th>Training Provided to Staff</th>
<th>Plan Reviewed Annually</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aviation</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Neighborhood Services</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Public Transit</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Water</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Three out of four impacted departments submitted updated Rule Programs.*

Overall, the Programs met the requirements of the Rule and we noted no exceptions. Although Aviation did not provide an updated Program, ISPO advised that it was working with the department to obtain documentation that supports compliance with the Rule.

### Recommendation

2.1 Aviation Department – submit an updated Rule Program and documentation that supports compliance with the Rule.
Scope, Methods, and Standards

Scope

We reviewed Red Flags Rule Programs and supporting documentation for Neighborhood Services, Public Transit, and Water Services submitted for FY 19/20. We also reviewed the Rule Program and supporting documentation for Aviation submitted for FY 18/19. All Programs and documents were tested against the current Rule.

The internal control components and underlying principles that are significant to the audit objectives are:

- Control Environment
  - Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity’s objectives.

- Control Activities
  - Management should design control activities to achieve objectives and respond to risks.

- Monitoring Activities
  - Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
  - Management should remediate identified internal control deficiencies on a timely basis.

Methods

We used the following methods to complete this audit:

- Reviewed the prior audit recommendations to ensure that the responses were effectively implemented.

- Interviewed department staff identified as having to comply with the Red Flags Rule.

- Obtained the departments' Rule Programs and supporting documentation to determine if the Programs complied with Federal regulations.

Unless otherwise stated in the report, all sampling in this audit was conducted using a judgmental methodology to maximize efficiency based on auditor knowledge of the population being tested. As such, sample results cannot be extrapolated to the entire population and are limited to a discussion of only those items reviewed.
Standards

We conducted this performance audit 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Any deficiencies in internal controls deemed to be insignificant to the audit objectives but that warranted the attention of those charged with governance were delivered in a separate memo. We are independent per the generally accepted government auditing requirements for internal auditors.