Phase 1 Report: Document and Review of Program Controls

California Clean Fuel Reward Program

August 23, 2021

CohnReznick
ADVISORY • ASSURANCE • TAX

To: California Clean Fuel Reward Program Steering Committee

From: CohnReznick LLP

Subject: Results of Phase 1: Document and Review of California Clean Fuel Reward Program Controls

Date: August 23, 2021

I. Executive Summary

The California Clean Fuel Reward program (CCFR) is funded through revenues generated through the California Air Resource Board (CARB) Low Carbon Fuel Standard (LCFS) program. The CCFR is administered by Southern California Edison (SCE). CohnReznick LLP was engaged to serve as the independent program auditor for the CCFR program.

This report provides high level information on the overall objectives, scope and approach of the audit activities related to the CCFR Program and the results of the Phase 1 "Document and Review Program Controls" effort (or Phase 1 CCFR Program Assessment).

The objective of this first phase effort was to assess and provide feedback on the documentation, processes and controls initially established by the program implementer (Maritz) and SCE to support the program and manage inherent risks.

This Phase 1 CCFR Program Assessment commenced in late August of 2020 and covered the processes and controls in place at the time of the program launch November 17th, 2020.

Throughout this assessment phase CohnReznick interacted heavily with and provided ongoing real time feedback to both SCE and Maritz while various processes and control mechanisms were being developed and put in place to support the CCFR program.

Ongoing discussions were held during the program's pre-launch development period and post program launch. Several recommendations and suggestions were implemented prior to the program launch and others were implemented during this year. Our report primarily highlights controls that were in place during our review and remediation recommendations that were implemented prior to the program launch.

Interviews were conducted with personnel from both SCE and Maritz and process walkthroughs were performed Additionally, our assessment included reviewing several iterations of process documentation to evaluate the design of established controls. Our report highlights the issues noted at the conclusion of our review.

Any remediation activities reflected in management's responses to the issues noted in this report were not reviewed during the interim audit.

Engagement Objectives

Assess the adequacy of the control activities put in place or being developed to support the CFR Program by reviewing:

- Various processes, procedures, controls, and program documentation available
- The roles and responsibilities of various process owners and the adequacy of the segregation of duties and authority/approval controls in place
- The monitoring activities and enforcement of the reward reimbursement processes and policies, including, but not limited to monitoring the performance of the selected Financial Institution and implementer (Maritz)
- The design of current state data privacy and cyber security controls in place to protect the program such as segregation of duties and system access controls, monitoring and incident response
- The monitoring and enforcement of the dealer enrollment process

Engagement Approach and Scope

1. During the Phase 1 CCFR Program Assessment CohnReznick provided on-going feedback to SCE and Maritz as they were developing their processes and controls.

2. Processes and controls in place related to the following areas were documented and/or reviewed:

i. CCFR Dealer Enrollment

ii. CCFR Vendor Set up

iii. CCFR Retailer Claims

iv. CCFR Vendor Payment

v. Privacy

vi. Cyber-security

3. Walkthroughs were performed for the controls identified to validate their design.

4. Segregation of duties and system access controls for Maritz's CCFR system (including the Okta identity management component) and SCE's SAP system.

5. Control deficiencies or areas of improvement identified were documented along with remediation recommendations and discussed with those responsible for the setup and development of the CCFR control structure and operating model.

Results:

The results of this Phase 1 CCFR Program Assessment identified the following issues:

1. A secondary review of dealer enrollments and rebates processed by Maritz is not performed.

2. There was no evidence to support that a completeness and accuracy review of new dealer set ups and claims processed was performed by Maritz.

3. Access rights and approval controls related to the CCFR Aquia site should be enhanced.

4. Southern California Edison along with other power utility companies are considered to be national critical infrastructure organizations. As such SCE is hesitant to provide specific details related to the privacy and security control mechanisms in place that protect the company from data breaches and cyber security threats. Therefore, CohnReznick was unable to verify, test or validate the design of security and privacy controls in place for the CCFR program. *Note: Privacy and security controls at Maritz were reviewed with no issues noted.*

Please refer to Section II for detailed Findings and Recommendations and Section III for Process Improvements.

Lastly, as stated above, we worked with SCE and Maritz to provide ongoing feedback while SCE and Maritz were developing the processes and controls to support the program. As such, there were multiple areas of improvement noted during the course of the review. These issues were corrected and incorporated into the controls that were reviewed by CohnReznick. While these issues are not detailed in Section II, we have included a summary outlining these matters in Section IV -Remediated Issues Not Identified in Report.

II. Findings/Recommendations

1. A secondary review of dealer enrollments and rebates processed by the Maritz call center associates is not performed.

Risk:
Multiple data attributes are manually reviewed by the Call Center Associate which increases the risk of human errors and the potential of fraudulent additions.

Recommendation:
A secondary review of all dealer enrollments and rebate requests should be established. Additionally, a review of all previously made reward payments should be performed to ensure that they were valid and properly paid.

<u>Maritz response - *Dealer Enrollments:*</u>

While a secondary review of enrollments was not part of the original scope, Maritz began performing a second validation of all enrolled dealers' banking information in June 2021. In addition, this data will be validated every six months. There are several fields validated to ensure the vendor and banking information provided is correct. This review checks for accuracy as well as for updated information.

Before the secondary review was in place, validations were performed to ensure the enrollment information provided by the vendor was correct. The Maritz Call Center uses an Enrollment Validation Checklist which is included in the Standard Operating Procedures documentation (SOP) and available upon request.

<u>Maritz response - *Reward Payments:*</u>

The original process included elements of #1 and #2 below and based on early feedback and learnings from the program, AI was developed and quickly implemented as another data-driven approach to review the documents. #3 Post-Sale Validation is dependent on collecting data from both the program and third-party sources and implemented in May 2021.

Going forward, the validation approach performed by stages is as follows:

1. Claim Form – a claim is checked against applicable verification services through automated methods and the retailer is notified of the claim receipt via email. Then, the claim is analyzed by the system Application Programming Interface (API) and Line Item Digital Audit (LIDA/AI) engine to generate assessments for the claim approval process.

2. Call Center Validation - Call Center verifies all required claim information is present and correct. If there are contradictions between the auditor's assessment and the Ai assessment, the 2-Auditor Workflow is triggered, requiring a second auditor to validate the claim before it can be sent for payment.

3. Post-Sale Validation - Vehicle Identification Number (VIN) validation process provides an additional validation measure that the claim contains valid data. Vehicle registration validation is an additional validation that the claim contains valid data. Both validations are performed for claims data back to the inception of the program.

***Additional CohnReznick Note*:** *The Artificial Intelligence and other automated verification tools were not fully implemented until 6/10/2021. Maritz should perform verifications of dealer enrollments and claims processed prior to 6/10/2021. CohnReznick did not test the newly implemented controls as part of this review.*

2. **There was no evidence to support that a completeness and accuracy review of files received from SCE for new dealer set up and claims processed was performed by Maritz.**

Once Maritz completes processing new dealers and new claim submissions, Maritz sends an Excel file generated by the CCFR system to SCE for processing. SCE uploads the new vendor and claim payment information to SAP for processing. Upon completion, SCE sends back an Excel file generated by SAP to Maritz. The written SOPs provided by Maritz indicated that Maritz did not do a detailed verification. In addition, during the walkthrough Maritz did not provide evidence that that verification was being performed. Maritz later indicated that the detailed verifications were in fact being performed and that the SOP document was not correct. Evidence of these verifications were not documented; hence CR could not validate that these verifications were performed.

Risk:
Lack of validation of vendor information and claim payment information sent by SCE back to Maritz could lead to errors and fraudulent payments, as the file sent back by Maritz are manually created and can be manipulated.

Recommendation:
Management should ensure that the CCFR system validates the specific details for new vendors and claims information sent back by SCE to Maritz to ensure that the new vendors set up and claims paid by SCE agree to the information provided by Maritz and maintain documentation to support the validations performed.

Maritz Response: *- New Dealer Enrollments*:

Standard Operating Procedure (SOP) provided earlier was not the final version and language was misleading and interpreted that no validation was being performed on the return files from SCE to Maritz. This has been corrected in the SOP.

An automated process for transferring enrollment information to SCE and receiving it from SCE was implemented in late March 2021. The automated process eliminated the manual intervention needed previously to upload the enrollment data, thus minimizing the risk of inaccurate data being processed. The automated process does a match of what is provided back from SCE to what is in the CCFR system. Any mismatch will trigger an alert sent to an email address which is monitored by Maritz team members. When an alert is received, an investigation is initiated with SCE. SCE uploads a corrected file via the website and the CCFR system will automatically process the file.

During the manual process timeframe, if return files did not match the fields being validated, an alert was sent to the Maritz CCFR project members. When an alert was received, an investigation was initiated with SCE. SCE uploaded the corrected file to SharePoint and Maritz followed the standard process for processing it.

Fields validated in both the automated and the manual process ensured the claim information matched.

To ensure data was not manipulated during the Manual process time period (Dec 2020 - late March 2021), Maritz will compare the information within the CCFR database to what is in the SCE/SAP database.

<u>Maritz Response:</u> - ***Submitted Claims***

Standard Operating Procedure (SOP) provided earlier was not the final version and language was misleading and interpreted that no validation was being performed on the return files from SCE to Maritz. This has been corrected in the SOP.

An automated process for validating claims submission from SCE to Maritz was implemented in late March 2021. The automated process eliminated the manual intervention needed previously to upload the claims data, thus minimizing the risk of inaccurate data being processed. The automated process does a match of what is provided back from SCE to what is in the CCFR system. Any mismatch will trigger an alert sent to an email address which is monitored by Maritz CCFR project members. When an alert is received, an investigation is initiated with SCE. SCE uploads a corrected file via the website and the CCFR system will automatically process the file.

During the manual process timeframe, if return files did not match the fields being validated an alert was sent to the Maritz CCFR project members. When an alert was received, an investigation was initiated with SCE. SCE uploaded the corrected file to SharePoint and Maritz followed the standard process for processing it.

Fields validated in both the automated and the manual process ensured the claim information matched.

To ensure data was not manipulated during the Manual process time period (Dec 2020 - late March 2021), Maritz will compare the information within the CCFR database to what is in the SCE/SAP database.

Note: *CohnR*eznick did not test the design of the newly implemented controls as part of this audit.

3. **Access rights and approval controls related to the CCFR Aquia site should be enhanced.**

The following issues related to system access and approval controls were noted:

a. The standard operating procedures (SOP) provided by Maritz indicated that Maritz Administrators and Call Center associates had the ability to delete user data in the CCFR Aquia site, including dealer information.

Note: Updated SOP's provided as of April 13, 2021 indicated that the rights were no longer available to Administrators and Call Center Associates. Additionally, Maritz management stated that the ability to delete user data in the system was never activated. Although CohnReznick was unable to independently verify this assertion we were able to verify that the delete capability is currently unavailable.

b. An excessive number of individuals (31) had System Administrative access to the CCFR Aquia site prior to April 11, 2021.

- o Two individuals were developers with a generic email that was not assigned to a specific person. (***Members of Proficient, the consulting firm used by for the CCFR implementation)***

c. Controls surrounding system access are not clearly defined as to responsibility for reviewing and approving access, the appropriateness of the access being granted or the frequency in which an access review should be performed. ***(As of the date of this review, an access review had not yet been performed.)***

Risk:

Excessive system access can result in inappropriate access to data and increases the risk of fraud.

Recommendations:

- Changes made by the Developers should be verified by Maritz to validate that the change made was proper.
- A review should be performed to determine the appropriateness of information deleted prior to April 11th.
- Management should perform access reviews on a quarterly basis. Okta reviews should also be included in the access reviews.

Maritz Response (3a-b):

- Call Center Associates never had the ability to delete user data. The SOP provided earlier was not the final version and was incorrectly documented. This has been corrected in the SOP.
- The DELETE permissions shown in earlier versions of the SOP for Maritz users (Admins and Call Center users) existed in error as the original intention was to create CRUD style permissions (Create/Update/Delete) for several user roles. However, during development, it was determined that the user permissions for all Maritz users should not be developed in this manner, instead only allowing View and Update permissions for Retailer-generated submissions (enrollments and claims). Thus, no DELETE permissions have ever existed for Maritz users in relation to customer or retailer data.

  This can currently be demonstrated by viewing the allowed actions within the Maritz Admin system for both Maritz Admin and Maritz Call Center users.

Maritz response (3 c):

- Every six months, the Maritz Project Manager will review system access for all roles. As needed, the User Removal & Termination Process will be followed to remove inappropriate permissions.
- The Granting User Access process is followed by individuals who need to request access to the CCFR system. The Maritz Project Manager monitors

the process and grants or denies user permission requests. A report can be pulled from Okta listing individual's permissions.

- The Maritz team reviews and validates the development by Perficient individuals by engaging in User Acceptance Testing before any development work is deployed to production. The Perficient permissions and Maritz' involvement in UAT, mitigate the risk of unauthorized access of data and fraud.

4. **Southern California Edison along with other power utility companies are considered to be national critical infrastructure organizations. As such SCE is hesitant to provide specific details related to the privacy and security control mechanisms in place that protect the company from data breaches and cyber security threats. Therefore, CohnReznick was unable to verify, test or validate the design of security and privacy controls in place for the CCFR program. Note:** *There were no privacy and security issues noted at Maritz.*

   CohnReznick met with SCE's Principal Manager Cybersecurity & Intelligence Operations and the Information Governance, Advisor to discuss controls in this area at a high level and we were informed at a high level of the following:

   a. SCE uses the NIST Cybersecurity Framework which provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyberattacks.

   b. The Cybersecurity Framework in place at SCE also extends to the CCFR program.

   c. SCE's Privacy compliance program implements controls and practices consistent with the Fair Information Protection Practices framework.

   d. SCE has a multi-layered defense system that monitors and protects against cyberthreats 24 hours a day, every day. Partnerships and information sharing among peer electric companies, government agencies and other trusted organizations committed to protecting the energy grid are equally important to helping block millions of malicious emails, domains and websites. As cyberthreats grow and become more sophisticated, we remain committed to protecting the energy grid and to strengthening our defenses.

Recommendation:

As mentioned above, CohnReznick was unable to verify, test or validate the security and privacy controls in place for the CCFR program at SCE. The program steering committee may want to consider a close door session with both organizations on this topic to gain greater comfort on the design and effectiveness of controls in place that are protecting the program.

SCE Response:

SCE's tactical support of the CCFR program leverages existing SOC documented operational procedures as well as enterprise security and privacy protections. The scope of SCE's CCFR work is focused on general program management and processing payments to vendors/retailers.

SCE requires all suppliers to adhere to our policy on information security, cyber security and privacy, which can be supplied upon request.

III. Process Improvement Recommendations

Dealer return information is aggregated with the dealer's submitted claims for monetary reimbursement. However, there is no separate reporting of monetary reimbursements, which includes car returns. As such, monetary reimbursements cannot be identified unless each dealer's submissions are reviewed in detail.

Recommendation:
Management should consider creating a more efficient process to capture dealer's returns separate from the dealer's claims.

Management Response:
Maritz has return data stored and will be developing a plan to review/analyze it. This is a future process to be developed.

IV. Remediated Issues Not Identified as Findings in the Report

As previously discussed CohnReznick the CCFR program was a build out. CohnReznick worked collaboratively with both Maritz and SCE to provide independent feedback on the internal control structure of the CCFR program. The following issues noted were all addressed and remediated during the period of our fieldwork and as such were not noted as Findings to be included in Section II above.

a. During the course of this review, CohnReznick noted protected information (such as participant PII, developer credentials, secure tokens) stored in plain text. To mitigate issues related to the exposure of secure data we recommended that steps be taken to obfuscate sensitive data as well as disallow the storage and/or auto-fill of privileged credentials by the development team.

b. CohnReznick noted that a Privacy and Participant Policy was not developed and recommended that a Privacy Policy and Participant Consent be developed prior to enrollment.

c. Documentation detailing the validation or reconciliation steps being performed by the Maritz or SCE teams did not exist. For instance, there was no documentation as to how SCE was validating the information provided by Maritz nor was there any documentation as to how Maritz was validating the information that was provided by SCE in return.

CohnReznick recommended that the narratives detail what specifically is done to perform and review the validation steps and ensure that there are appropriate controls added.

d. CohnReznick noted that there was no formal checklist of the various audit tasks being performed by the Maritz Call Center Associate. Furthermore, there was no documentation over the manual reviews being performed by the Call Center team or the level of review itself. CR recommended that a detailed checklist be utilized to ensure all the necessary reviews have been completed and documented.

e. CohnReznick noted that there was no documentation as to how rejections performed by Maritz of new dealer enrollments were being communicated to the dealer. CohnReznick recommended that the communication process include an email from Maritz to the dealer and that the email be retained.

f. There was inadequate documentation outlining how changes to the dealer information are processed and reviewed for completeness and accuracy. CohnReznick recommended that the process narrative include the process of changing dealer information and that the review performed by the Maritz Call Center team is documented

g. The verification of the rebate amount to the battery size, new vehicle, etc. was not documented. CohnReznick recommended that the narrative include all the verifications performed for the rebates.