**From:** Andrea D'Alessandro
**Sent:** Friday, May 10, 2024 2:30 PM
**To:** Richard Parkinson; Hema Widhani
**Cc:** Lilly Raymond; David Hamlett; April Virhuez; Kalli Chapman; Gregg Klein; Maximilian Stefani; Jim Flors; Lydia Barlow; Carrie Bonis; Ashley Bryson; Rockell Metcalf; Allison Korman; Suzanne Manganiello; Suzanne Sainato; Kaitlin Betancourt; Philip Ramey; Laura Weiss; Ketan Bhanushali; Lalitha Kavutharapu; Allison Shilling; Sonia Singh; Ken Nevola; Ian Cornell; Al Limone; Amanda Turner; Cecilia Orchard; Jerry Roman; John Koskoski; Lily White; Philip Barreca; Bryan Aguila; Andrea D'Alessandro
**Subject:** Internal Audit Report: Partially Satisfactory - Control Condition Assessment - 2024 - Marketing - Social Media Listening and Customer Look-a-like Process
**Attachments:** Marketing - Social Media Listening and Customer Look-a-like Process CCA Issues.pdf

# Internal Audit Department

Internal Audit has assessed the control condition of key controls within the ABC Company Marketing function for the period December 1, 2022 to November 30, 2023. A control condition audit is designed to provide reasonable assurance as to the design and effectiveness of the system of internal controls implemented by management.

Internal Audit's testing resulted in the identification of 2 medium risk issues, the summary of which are presented below. Additionally, 1 low risk issue was identified. The details of the issues identified and management's action plans can be reviewed in the attached PDF.

| Issue Rating | Repeat Issue | Issue Summary | Issue Owner | Due Date | Issue ID |
|---|---|---|---|---|---|
| Medium | No | Minimum third-party and privacy standards were not executed resulting in inadequate information security controls to prevent inappropriate access to customer information by internal or external parties. The root cause can be attributed to both various VEM and organizational changes occurring over the past few years, which over time has impacted clarity regarding the applicable ongoing monitoring standards. Also, during the vendor onboarding process (2018) appropriate SaaS configuration was not performed. Management remediation date: October 31, 2024 | David Hamlett | October 31, 2024 | IS-002722 |
| Medium | No | Controls over the transmission to and disposal of customer data in LiveRamp requires improvement. The root cause is primarily attributed to the lack of effective Vendor Engagement Manager's monitoring process and management's awareness of the expected standards, associated controls including the approved data transmission methods. Management remediation date: August 30, 2024 | Maximilian Stefani | August 30, 2024 | IS-002723 |

**Control Condition:** Partially Satisfactory

**Control Environment:** Unrated

**Rating Rationale:** Based on the results of the work performed, Internal Audit has concluded that certain elements of the system of internal controls related to social and paid media operations are not adequately designed or operating as intended to mitigate key business risks. The issues identified highlight the need to improve key components of the governance framework over key processes to ensure vendor activities and applications are appropriately monitored, secured, and customer data protected in accordance with Company standards. The issues have a meaningful impact on management's ability to mitigate the risks that can lead to regulatory damages, customer dissatisfaction and reputational harm. However, controls related to marketing material review and approval are effectively designed and operating as intended. As a result, Control Condition has been rated Partially Satisfactory.

**Scope:** The scope included an assessment of the design and effectiveness of the key controls related to social and paid media operations, including the Social Media Listening and Customer Look-a-like processes. The audit focused on certain key risks including:

- Product, Operations, and Trading – Customer Service/Escalation
- Regulatory Compliance – Misleading Communications and Marketing Materials
- People and Governance – Governance and Risk Management
- Information Security – Unauthorized Data Access & Inadvertent Data Exposure

Testing focused on controls in certain key processes including:

- Governance and Risk Management
- Sprinklr Customer Service/Escalation and Monitoring
- Misleading Communications and Marketing Materials
- Access to Key Systems
- Data Transfer

The following processes were excluded from the scope of the review:

- Social Media programs and processes for Assurance IQ, PGIM, and International businesses are managed locally and would be subject to separate risk-based audit coverage.

Any questions regarding this report should be directed to the Group Vice President or Vice President responsible for the audit, Lily White and Andrea D'Alessandro, respectively.

# Internal Audit Department

**Issue ID: IS-0002722**

**Issue Name:** Minimum third-party and privacy standards were not executed resulting in inadequate information security controls to prevent inappropriate access to customer information by internal or external parties.

Issue Description: Sprinklr is a Software as a Service (SaaS) social media management platform used to implement social media strategy and support the tracking and triage of comments received from consumers (e.g., service requests, customer complaints). The ABC Company Social Media Listening Program uses Sprinklr to monitor social media content involving ABC Company across various public platforms (e.g., Facebook, LinkedIn). The Social Media team began collecting Personal Information (PI) to provide further customer assistance since 2018.

Based on testing performed, Internal Audit noted the following:

- Vendor Engagement Manager (VEM) didn't update the Inherent Risk Rating (IRR) for Sprinklr to reflect the collection of PI, therefore the required enhanced monitoring and due diligence per Third-Party Risk Management Program and Standards wasn't performed. Similarly, a Privacy Impact Assessment (PIA) was not completed for Sprinklr. There were 173 (out of 11,160) cases during the scope period where PI was requested from the customer. Management has since completed the PIA as of February 2024.
- Sprinklr can be accessed from outside of the ABC Company network using personal devices through established credentials (username and password), therefore bypassing Enterprise authentication and information security controls, including data loss prevention. Additionally, multifactor authentication (MFA) as required by Enterprise standards was not in place at the time of the audit.
- While access to Sprinklr can be provisioned directly by certain users within the Social Media Operations team, a recertification has not been implemented; however, access at the application level was deemed appropriate.
- Access to ABC Company's specific social media account handles (public usernames) managed within the platform is not reviewed periodically to ensure appropriateness of user access and permissions. IA and management were unable to confirm the appropriateness of access at the time of the audit.

Root Cause Explanation: The root cause can be attributed to both various VEM and organizational changes occurring over the past few years, which over time has impacted clarity regarding the applicable ongoing monitoring standards. Also, during the vendor onboarding process (2018) appropriate SaaS configuration was not performed.

Rating Rationale: Without the appropriate vendor onboarding and oversight controls to ensure compliance with Company standards, key vendor, privacy, and information security risks may not be assessed and appropriately addressed which can result in privacy breaches or complaints. The misclassification of a vendor application and the resulting absence of information security controls increases the likelihood of unauthorized access and data breaches. ABC Company manages 59 social media accounts with combined followers totaling over 1.4 million, which increases the potential of significant reputational impact if an unauthorized user gains access to the application through either incorrect access provisioning or inadvertent exposure from access to the ABC Company network. Additionally, the collection and sharing of PI without adequate protection increases the risk of regulatory fines and litigation. These risks are partially reduced as there is a limited number of user licenses (24) available to provision access for the Sprinklr application. Further, based on management's re-assessment of the vendor IRR, it was estimated that the potential number of records containing PI within the engagement is currently limited to between 500 and 10k records, within a moderate risk range based on threshold established by the Privacy standards. As a result, the issue is rated "Medium" risk.

Audit Risk Taxonomy Level 1: 8. Information Security

Issue Rating: Medium
Status: Open

Repeat Issue: No
Issue Target Date: October 31, 2024

Operating Division: US Businesses
Business Group: Marketing
Reportable Segment: USBC – Global Brand

**Action Plan ID: AC-003536**
**Action Plan Description:** Complete a Privacy Impact Assessment and reclassify the application to Restricted.

| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
|---|---|---|
| April Virhuez | June 30, 2024 | Closed |

**Action Plan ID: AC-003537**
**Action Plan Description:** Complete the vendor assessment based on current usage of Sprinklr.

| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
|---|---|---|
| April Virhuez | June 30, 2024 | Closed |

**Action Plan ID: AC-003538**
**Action Plan Description:** Implement access provisioning controls and recertification process through Central Security Service.

| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
|---|---|---|
| April Virhuez | June 30, 2024 | Open |

**Action Plan ID: AC-003539**
**Action Plan Description:** Oversee a comprehensive assessment of current CMO SaaS vendors to confirm that the following controls are in place where applicable:

1. A Privacy Impact Assessment has been completed.
2. The vendor IRRT has been refreshed in accordance with current VGO standards.

| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
|---|---|---|
| Carrie Bonis | June 30, 2024 | Open |

| **Action Plan ID: AC-003533**<br>**Action Plan Description**: Implement single sign on (SSO) authentication for users when accessing Sprinklr through both web and mobile. | | |
|---|---|---|
| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
| Ketan Bhanushali | July 31, 2024 | Open |

| **Action Plan ID: AC-003534**<br>**Action Plan Description:** Explore solutions to implement multifactor authentication (MFA) for Sprinklr access. | | |
|---|---|---|
| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
| Ketan Bhanushali | July 31, 2024 | Open |

| **Action Plan ID: AC-003535**<br>**Action Plan Description:** Assess enterprise standards for data loss protection and determine whether controls can be configured by the vendor to meet requirements. Implement identified solutions and monitor adherence, as appropriate. | | |
|---|---|---|
| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
| Ketan Bhanushali | July 31, 2024 | Open |

| **Action Plan ID: AC-003610**<br>**Action Plan Description:** Assess the active SaaS applications within the Marketing organization and determine whether they adhere to relevant Enterprise Information Security Control Standards. Develop a tracking document that lists all SaaS applications and their level of adherence to standards with variables that impact implementation of required configurations. Additionally, document a plan to remediate identified gaps supported by risk and criticality assessments. | | |
|---|---|---|
| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
| Ketan Bhanushali | September 30, 2024 | Open |

# Internal Audit Department

**Issue ID: IS-0002723**

**Issue Name:** Controls over the transmission to and disposal of customer data in LiveRamp requires improvement.

Issue Description: LiveRamp, a third-party provider that offers a cloud-based onboarding application designed to collect, organize, and connect customer data to marketing and social media platforms. The ABC Company Paid Media team provides LiveRamp with customers' personal information (e.g., names, address, phone numbers), to be hashed and anonymized prior to sharing with additional third-party social media platforms for the purposes of creating curated groups of prospective customers.

Based on testing performed by Internal Audit, the following was identified:

- A records disposition plan was created between ABC Company and LiveRamp that defines the record retention schedule as 30 days to dispose of data files; however, the plan is incomplete to account for the various file types being transmitted.
- Vendor monitoring controls are not in place to ensure that records are being deleted in accordance with the existing agreement (i.e., monthly attestations from LiveRamp). During the audit's scope period, ABC Company transmitted data files containing approximately 9.3 million customer records to LiveRamp.
- The method for uploading data to LiveRamp through an online portal was outside of the process approved by ABC Company's Enterprise Architecture Review Board (EARB). Management is relying on a manual upload of the customer data. and there are currently 23 active users across the broader marketing organization with the capability to upload data through the unapproved online portal.

Root Cause Explanation: The root cause is primarily attributed to the lack of effective Vendor Engagement Manager's monitoring process and management's awareness of the expected standards, associated controls including the approved data transmission methods.

Rating Rationale: Failure to reduce the exposure of customer data, as well as using an unapproved process to transmit customer data to a vendor, could result in data breaches, as well as reputational and regulatory damages. The risk is elevated due to the high frequency and large volume of data transmitted to LiveRamp, and the potential of ABC Company customer data being subject to a data breach at the vendor. Additionally, not following the EARB-approved process could expose customer data to unauthorized users and attempts to intercept unsecured transmissions. Further, allowing the transmission of data by all LiveRamp users increases the likelihood of inaccurate and/or incomplete data being utilized for the basis of targeted marketing campaigns. These risks are partially reduced because both the approved and unapproved data transmission processes use the same vendor infrastructure to transmit data securely through Secure File Transfer Protocol (SFTP). As a result, the issue is rated "Medium" risk.

Audit Risk Taxonomy Level 1: 8. Information Security

Issue Rating: Medium
Status: Open
Operating Division: US Businesses
Business Group: Marketing

Repeat Issue: No
Issue Target Date: August 30, 2024

Reportable Segment: USBC – Digital and Marketing

| **Action Plan ID: AC-003540**<br>**Action Plan Description**: Revise records disposition plan and contractual agreement with LiveRamp to clearly define data deletion requirements. | | |
|---|---|---|
| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
| Maximilian Stefani | June 30, 2024 | Open |

| **Action Plan ID: AC-003542**<br>**Action Plan Description:** Ensure training/communication of EARB approved process for all Social Media team members. | | |
|---|---|---|
| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
| Gregory Aronne | June 30, 2024 | Open |

| **Action Plan ID: AC-003543**<br>**Action Plan Description:** Explore methods to disable direct uploads through LiveRamp or assign restricted user permissions with the application. | | |
|---|---|---|
| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
| Ketan Bhanushali | July 31, 2024 | Open |

**Issue ID: IS-0002724**

**Issue Name:** Controls to ensure timely response and escalation of customer service-related comments require enhancement.

Issue Description: As part of the ABC Company Social Media Listening Program, the Social Media Operations team utilizes the Sprinklr platform as the primary tool to support the tracking and triage of comments received involving ABC Company and its social media accounts across various public platforms (e.g., Facebook, LinkedIn). If customer comments received are specific to service requests or customer complaints, a case is created within Sprinklr and assigned to a member of the Social Media team to ensure timely escalation takes place with the appropriate internal parties for tracking and resolution.

Internal Audit (IA) verified that appropriate procedures were followed, and timely response and escalation occurred by the Social Media Operations team for a sample of 25 cases generated within the scope period. There were 2 cases reviewed where IA could not obtain evidence of response prior to closure of the case within Sprinklr. Upon further investigation with management, it was determined that the Sprinklr feed has not been capturing automatic responses sent to consumers directly within the Facebook direct message platform, a recent process enhancement implemented by the team. Additionally, process discrepancies were identified within the Standard Operating Procedures (SOP) regarding the auto response process change implemented.

Root Cause Explanation: The root cause is primarily attributable to a lack of change management discipline and oversight to ensure process enhancements are implemented appropriately and working as intended prior to being operationalized.

Rating Rationale: A lack of controls to ensure Sprinklr cases related to consumer service requests or complaints are identified and escalated to the appropriate internal parties for tracking and resolution in a timely manner increases the likelihood of cases going unaddressed. Unresponsiveness to customer inquiries, coupled with ambiguity in SOPs may result in a negative customer experience, poor quality of service, and operational inefficiencies. While there is the potential for customer dissatisfaction and reputational harm risks, the overall impact is limited to auto response cases which are deemed lower risk. Further, except for the cases identified above, IA determined that the resolution of the remaining cases was appropriate. Therefore, Internal Audit deems this issue to be “Low” risk.

Audit Risk Taxonomy Level 1: 12. Product, Operations, and Trading

Issue Rating: Low
Repeat Issue: No
Status: Open
Issue Target Date: July 31, 2024

Operating Division: US Businesses
Business Group: Marketing
Reportable Segment: USBC – Global Brand

| **Action Plan ID: AC-003544**<br>**Action Plan Description**: Update procedures to reflect the use of the Meta direct messaging platform as part of the case review and closure process. Implement a management oversight procedure to identify and test process changes prior to the operational go-live date. | | |
|---|---|---|
| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
| April Virhuez | June 30, 2024 | Open |

| **Action Plan ID: AC-003545**<br>**Action Plan Description:** Explore solutions to the current gap preventing automated responses from feeding directly to Sprinklr to alleviate the need of manual reconciliation. | | |
|---|---|---|
| Action Plan Owner: | Action Plan Closure Target Date: | Action Plan Status: |
| April Virhuez | June 30, 2024 | Closed |