



VIRGINIA ALCOHOLIC BEVERAGE CONTROL AUTHORITY

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2021

Auditor of Public Accounts
Staci A. Henshaw, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

Our audit of the Virginia Alcoholic Beverage Control Authority (Authority) for the year ended June 30, 2021, found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- instances of noncompliance or other matters required to be reported under Government Auditing Standards.

We have audited the basic financial statements of the Authority as of and for the year ended June 30, 2021, and issued our report thereon, dated December 2, 2021. Our report is included in the Authority's Annual Report that it anticipates releasing in December 2021.

–TABLE OF CONTENTS–

Pages

AUDIT SUMMARY

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

1-5

INDEPENDENT AUDITOR’S REPORT ON INTERNAL CONTROL OVER
FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

6-8

AUTHORITY RESPONSE

9-11

AUTHORITY OFFICIALS

12

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Continue Improving Database Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Partial (first issued in fiscal year 2019)

Prior Title: Improve Database Security

The Virginia Alcoholic Beverage Control Authority (Authority) continues to improve security for the database that supports its human resource system in accordance with the National Institute of Standards and Technology Standard, 800-53 (NIST Standard), and industry best practices. Since the prior year, the Authority has resolved three of the eight weaknesses and has made some progress for the remaining five weaknesses.

We communicated the control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The NIST Standard and industry best practices require the implementation of certain controls to reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information. The Authority continued to prioritize the migration from the Virginia Information Technologies Agency above other organizational priorities, causing limited resources to focus on improving the controls and processes affecting the database.

The Authority should dedicate the necessary resources to ensure database configurations, controls and processes align with the requirements in its policies, the NIST Standard, and industry best practices. This will help maintain the confidentiality, integrity, and availability of mission critical data.

Improve Security Awareness Training Program

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in fiscal year 2019)

The Authority does not effectively and consistently manage its information security awareness and training program to ensure all users complete required training related to the Authority's policies for accessing its information systems and controls that protect the confidentiality, integrity, and availability of sensitive data. The Authority uses two systems to provide training to its central office and retail employees and contractors. Additionally, since the Authority's warehouse employees do not have access to information systems, the Authority provides them with in-person physical security training. For the in-person training, the Authority uses a signed roster to track completion. Our audit identified the following weaknesses within the Authority's training program:

- The Authority's Security Awareness and Training Policy and Security Awareness Training Standard do not outline requirements identifying which trainings each user group must complete. As a result, the Authority does not formally document nor consistently assign employees the required security awareness trainings.

- The Authority does not effectively monitor nor have an enforcement measure to ensure users complete the assigned training by the required deadline. The Authority designates the Human Resources Department (Human Resources) to coordinate, monitor, and track completion of security awareness training. Human Resources sends email reminder notifications to employees that have not completed the assigned training, as well as periodic notifications to the employee's manager. However, the Authority does not use an enforcement measure, such as disabling a user's account, that forces the users to complete training and comply with the Authority's policy. As a result of the lack of consistency and enforcement measures, we identified the following:
 - Sixty-two out of 147 (42%) warehouse employees did not complete the *Physical Security* training for the 2020 calendar year.
 - Nine out of 72 (12.5%) central office employees did not acknowledge the Authority's Acceptable Use Agreement when first hired between January and April of 2021.
 - Thirty-seven out of 1,253 users (3%) did not complete the *Access Control and Password* training for the 2020 calendar year.
 - Twenty out of 4,983 users (0.4%) did not complete the *Cyber Threat* training for the 2020 calendar year.
 - Sixty-five out of 4,375 users (1.5%) did not complete the *Retail Protection and Card Reader* training for the 2020 calendar year.

The Authority's Security Awareness and Training Policy, which aligns with the NIST Standard, requires all Authority users to complete security awareness training within 30 days of the Authority granting the user access to Authority resources. Additionally, the policy requires users to annually attend security awareness refresher training and sign an acknowledgement stating they have read and understood the Authority's acceptable use policy (*NIST Standard, Sections AT-2 Security Awareness; PL-4 Rules of Behavior*).

Without a consistent process to monitor and enforce users to acknowledge acceptance of the Authority's acceptable use policy, the Authority cannot ensure users understand the Authority's behavior requirements and responsibilities for information and system usage, security, and privacy. Also, by not having a consistent process to monitor and enforce users to complete security awareness training within the required timeframe, the Authority increases the risk that users will be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering.

The absence of details within the Authority's policy that outlines the Authority's requirements and process for assigning training modules to specific employee groups and monitoring to ensure users complete training by the required deadline contributes to the Authority inconsistently assigning

training modules to its employees and not ensuring users complete the required trainings by the deadlines. The Authority should improve its policy and procedures to clearly document its requirements and process for assigning and monitoring training. Additionally, the Authority should implement an enforcement measure to ensure all users complete the required trainings by the assigned deadlines.

Improve Oversight of Third-Party Service Providers

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: Yes (first issued in 2020)

The Authority does not maintain a formal and consistent process to oversee and manage its third-party service providers in accordance with the NIST Standard. The Authority currently uses 37 service providers for information technology business operations. Our review identified the following weaknesses:

- The Authority's Third-Party Provider Information Security policy states that Information Security shall use methods during preacquisition that most appropriately balances resources, risk, and the needs of the business to assess third-party cyber risk. Additionally, the Third-Party Information Security policy states that the Authority should use third-party audits to establish trust with a service provider. However, the Authority's policy makes the controls optional by stating that the Authority assesses providers' cybersecurity risk and evaluates providers' security controls as needed. To determine the level of assurance needed over third-party service providers, the Authority must complete risk assessments for all providers.
- The Authority has not conducted a formal risk assessment for each of its third-party service providers. Out of the 37-information technology third-party service providers the Authority utilizes, the Authority has not completed a risk assessment for 19 (51%) of the providers and has not finalized the risk assessments for an additional nine (24%) service providers. Without completing risk assessments and sensitivity classifications, the Authority is unable to determine the level of assurance needed over the third-party service providers' controls and operations.
- The Authority does not consistently monitor security control compliance by the providers on an ongoing basis. Additionally, the Authority does not document its reviews and determination of possible compensating controls of deficiencies found in third-party service provider assurance reports. The Authority obtained independent assurance for two of its 37 (5.4%) service providers prior to fiscal year 2021; however, the Authority has not obtained independent assurance for any of its 37 information technology service providers for fiscal year 2021.

The NIST Standard requires the Authority to employ methods to monitor security control compliance by the provider on an ongoing basis. Without gaining assurance that its service providers'

implement information security controls and that they operate effectively, the Authority cannot guarantee its data is secure in accordance with its policies and the NIST Standard (*NIST Standard Section: SA-9 External System Services*). Due to the Authority's insufficient policy and procedures, and the Authority not documenting the level of assurance needed from each service provider, the Authority did not formally and consistently document risk assessments document its evaluation of the providers' cybersecurity risks and compliance and effectiveness of security controls.

The Authority should revise its policy and procedures to include minimum requirements that enforce a consistent process for the ongoing monitoring of third-party service providers. Additionally, the Authority should consistently enforce its process to document formal risk assessments and maintain continued oversight over its service providers. This will ensure the service providers adhere to the same security controls that govern the Authority's internal information technology systems and confirm overall compliance with the requirements outlined in the NIST Standard.

Improve Internal Controls over Employment Eligibility Process

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

Human Resources does not complete Employment Eligibility Verification (I-9) forms timely, in accordance with guidance issued by the U.S. Citizenship and Immigration Services of the U.S. Department of Homeland Security. Our sample of 25 employees hired by the Authority during fiscal year 2021 found:

- Human Resources staff did not complete Section 2 of the I-9 form timely for one of 25 employees (4%);
- For one of 25 (4%) employees, Human Resources did not document in Section Two the issuing authority for documents provided; and
- Human Resources staff did not create a case in the e-verify system within three days of the first day of employment for five of 25 employees (20%).

Failure to complete I-9 forms timely can result in penalties. Additionally, use of the e-verify system is required by the Code of Virginia § 40.1-11.2. The issues listed above occurred because Human Resource employees have not received proper training in this area and because the Authority's policy does not adequately address the timing of e-verify. The Human Resources Director should inform and adequately train Human Resources staff on the U.S. Department of Homeland Security's guidelines and use of the e-verify system. Internal policies should clearly address use of the e-verify system and the Human Resources Director should ensure that staff follow those guidelines.

Improve Internal Controls over Processing Payments

Type: Internal Control

Severity: Significant Deficiency

Repeat: No

The Authority is not processing payments received from external vendors in compliance with their internal Signature Authority & Procurement Responsibility policy. In our sample of 30 vouchers for which prompt payment requirements were applicable, we identified six instances (20%) in which the Authority did not process payment within the required 30 days. Our review of vouchers for prompt payment excluded merchandise for resale. The Authority initiates payments to these vendors based on shipments from the Authority's warehouse to the retail stores, rather than receipt of invoice from the vendor. The Authority pays these invoices on a net-30 basis from the last date of the cycle. As such, these payments pose a lower risk due to the internal invoicing process.

Per the Authority's policy, Accounts Payable establishes the required payment due date based on the terms of the contract; or if a contract is not in existence, thirty calendar days after the receipt of a proper invoice, or thirty days after the receipt of goods or services, whichever is later. By not ensuring timely payments, the Authority may harm their reputation as a buyer, damage relationships with vendors, and could incur late fees.

For fiscal year 2021, the Authority made payments by the required due date for 95% of all payments. As mentioned above, we focused our review on vendor-initiated invoices, which comprise approximately 23% of the Authority's payments. Late payment was primarily a result of departments responsible for receiving goods or services not performing their duties timely. Accounts Payable requires a three-way match before processing payment, thus Accounts Payable cannot process payment for the respective vendor charges until departments record the receipt of goods or services in the Commonwealth's procurement system. The Authority should ensure that departments approve and submit required documentation in a timely manner to Accounts Payable to ensure the Authority can process all payments within the 30-day period.



Staci A. Henshaw, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 2, 2021

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Kenneth R. Plum
Chairman, Joint Legislative Audit
and Review Commission

Alcoholic Beverage Control Board
Virginia Alcoholic Beverage Control Authority

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the **Virginia Alcoholic Beverage Control Authority** (Authority) as of and for the year ended June 30, 2021, and the related notes to the financial statements, which collectively comprise the Authority's basic financial statements, and have issued our report thereon dated December 2, 2021.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the Authority's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled “Continue Improving Database Security,” “Improve Security Awareness Training Program,” “Improve Oversight of Third-Party Service Providers,” “Improve Internal Controls over Employment Eligibility Process” and “Improve Internal Controls over Processing Payments,” which are described in the section titled “Internal Control and Compliance Findings and Recommendations” that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Authority’s financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that is required to be reported under Government Auditing Standards and which is described in the section titled “Internal Control and Compliance Findings and Recommendations” in the findings titled “Continue Improving Database Security,” “Improve Security Awareness Training Program,” “Improve Oversight of Third-Party Service Providers” and “Improve Internal Controls over Employment Eligibility.”

Authority’s Response to Findings

We discussed this report with management at an exit conference held on November 23, 2021. The Authority’s response to the findings identified in our audit is described in the accompanying section titled “Authority Response.” The Authority’s response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Findings

The Authority has not taken adequate corrective action with respect to the previously reported findings “Continue Improving Database Security,” “Improve Security Awareness Training Program” and “Improve Oversight of Third-Party Service Providers.” Accordingly, we included these findings in the section entitled “Internal Control and Compliance Findings and Recommendations.” The Authority has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Audit Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

JMR/clj

Virginia Alcoholic Beverage Control Authority

Chief Executive Officer

Travis G. Hill



Chair

Maria J. K. Everett

Vice Chair

Beth G. Hungate-Noland

Board of Directors

William D. Euille

Gregory F. Holland

Mark E. Rubin

December 8, 2021

Ms. Staci A. Henshaw, CPA
Auditor of Public Accounts
101 N. 14th Street
Richmond, VA 23219

Dear Ms. Henshaw,

Attached are the Virginia Alcohol Beverage Control Authority ("VA ABC", the "Authority") responses to the audit for fiscal year ended June 30, 2021. Virginia ABC appreciates the opportunity to respond to the findings noted and to strengthen our controls based on the recommendations. Our responses to the findings in the Report on Internal Controls follow.

Continue Improving Database Security

The Authority agrees that it will dedicate the necessary resources to ensure database configurations, controls, and processes align with the requirements in its policies, the NIST Standard, and industry best practices. VA ABC continues to make progress in this area and as VA ABC retires legacy systems, we will continue to make improvements and progress.

Improve Security Awareness Training Program

VA ABC agrees that its security awareness training program is still in the process of being refined. During the last two calendar years we have developed our own training modules, including role-based training, and are refining our process for deployment and monitoring of the training modules. VA ABC



www.abc.virginia.gov | 7450 Freight Way Mechanicsville, VA 23116 | 804.213.4400

does monitor and does have an enforcement measure to ensure users complete the assigned training by the required deadline. VA ABC would agree that the current manual monitoring process is not ideal, although it does exist.

VA ABC is currently implementing changes to our security awareness training program. VA ABC does agree that it should improve its security awareness training procedure to document our process more clearly for assigning and monitoring training and is currently in the process of drafting that document. VA ABC's policy does allow for enforcement measures to ensure users complete required training, although VA ABC uses these as a last resort.

Improve Oversight of Third-Party Service Providers

VA ABC agrees that it needs a more defined, repeatable third-party vendor management process with easily accessible and well catalogued artifacts. We would also like to stress that we have not made control evaluation optional, but rather provided flexibility for the ways in which we assess those controls. VA ABC also agrees that the pre-existing third-party vendor applications procured while VA ABC was part of the VITA partnership should be risk assessed. While we do have a process for assessing new procurements, VA ABC does not methodically catalog those artifacts in an easily accessible repository. VA ABC is also in the process of documenting a formal third-party monitoring procedure. VA ABC will document the requirements that trigger monitoring, the responsible party for monitoring, the frequency of the monitoring, and the artifacts that must be retained and catalogued as evidence of the monitoring process.

Improve Internal Controls over Employment Eligibility Process

VA ABC concurs with the exceptions noted by Auditor of Public Accounts (APA). The Division of Human Resources (HR) will enhance controls over proper and timely completion and review of Employment Eligibility Verification (I-9) forms, to be in accordance with guidance issued by the U.S. Citizenship and Immigration Services of the U.S. Department of Homeland Security. HR will implement creation of a daily I-9 control checklist report that would include all the required and appropriate information to assist in determining if an employee's I-9 is completed in accordance with Federal regulations. HR will also cross-train an additional team member as a back-up to the process to ensure increased compliance. HR will provide additional training for our Retail Hiring managers on the accurate completion and timely submission of the I-9 documents. Lastly, we will review all policies and divisional standard operating procedures to ensure they clearly address the use of the e-verify system. We will re-educate the HR team on compliance obligations related to the U.S. Department of Homeland Security's



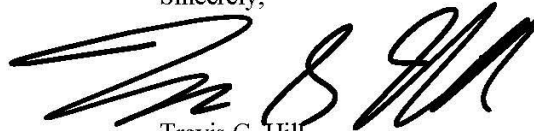
www.abc.virginia.gov | 7450 Freight Way Mechanicsville, VA 23116 | 804.213.4400

guidelines and use of the e-verify system. Virginia ABC will complete all corrections associated with this recommendation in fiscal year 2022.

Improve Internal Controls Over Processing Payments

VA ABC concurs that the Authority did not process payments on the exceptions noted by APA, on vendor-initiated invoices within the required 30 days. The Division of Financial Management Services' Accounts Payable department will continue to reinforce, amongst the Authority's designated department receivers, the importance of confirming and approving receipt of goods and services in a timely manner to ensure that the Authority can make all payments within the 30-day period. Accounts Payable's Assistant Manager will continue to monitor and report payment delays by sending out weekly reminders to Receivers, with a copy of the reminder to their respective supervisors on the third notification. In fiscal year 2022, expenses that are not approved and submitted by Receivers in the Commonwealth's Procurement System by the third reminder, will be further escalated to Assistant Controller and Director of Finance. This will provide further oversight to ensure expenses are received timely and will improve accountability. Lastly, VA ABC will retrain department Receivers to effectively and efficiently review and address issues that may arise and prevent them from timely approving receipt of goods and services.

Sincerely,

A handwritten signature in black ink, appearing to read 'Travis G. Hill', is written over a light blue horizontal line.

Travis G. Hill
Chief Executive Officer



www.abc.virginia.gov | 7450 Freight Way Mechanicsville, VA 23116 | 804.213.4400

ALCOHOLIC BEVERAGE CONTROL AUTHORITY

As of June 30, 2021

BOARD OF DIRECTORS

Maria J. K. Everett
Chair

Beth Hungate-Noland
Vice Chair

Gregory F. Holland
Member

Mark Rubin
Member

William “Bill” Euille
Member

OFFICIALS

Travis Hill
Chief Executive Officer

Elizabeth Chu
Chief Transformation Officer

John Daniel
Government Affairs Officer

Mark Dunham
Chief Retail Operations Officer

Jerome Fowlkes
Chief Administrative Officer

Thomas Kirby
Chief Law Enforcement Officer

Paul Williams
Chief Information Officer

Eddie Wirt
Chief Communications and Research Officer