



Bank-A-Count Corp.
Rudolph, Wisconsin

System and Organization Controls Report
Relevant to Print Services System

SOC 3[®] Report

November 1, 2021 to April 30, 2022



WIPFLI

SOC 3[®] is a registered trademark of the American Institute of Certified Public Accountants.

The report, including the title page, table of contents, and sections, constitutes the entire report and should be referred to only in its entirety and not by its component parts. The report contains proprietary information and is considered confidential.

Bank-A-Count Corp.

SOC 3 Report

November 1, 2021 to April 30, 2022

Table of Contents

Section 1 Bank-A-Count Corp.’s Assertion 2

Section 2 Independent Service Auditor’s Report 4

Attachment A – Description of the Boundaries of Bank-A-Count Corp.’s Print Services Systems 7

 Company Overview 8

 Services Provided 8

 Risk Management 8

 Organizational Structure 8

 General Computer Controls 9

 Complementary User Entity Control Considerations 12

 Complementary Subservice Organization Controls 13

Attachment B – Service Commitments and System Requirements of Bank-A-Count Corp.’s Print Services System 14

Section 1

Bank-A-Count Corp.'s Assertion

Bank-A-Count Corp.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Bank-A-Count Corp.'s ("Bank-A-Count") Print Services System (the "system") throughout the period November 1, 2021 to April 30, 2022, to provide reasonable assurance that Bank-A-Count's service commitments and system requirements relevant to security, processing integrity, and confidentiality, were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2021 to April 30, 2022, to provide reasonable assurance that Bank-A-Count's service commitments and system requirements were achieved based on the trust services criteria relevant to security, processing integrity, and confidentiality (the "applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Bank-A-Count's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2021 to April 30, 2022, to provide reasonable assurance that Bank-A-Count's service commitments and system requirements were achieved based on the applicable trust services criteria.

Section 2

Independent Service Auditor's Report

Independent Service Auditor's Report

Management of Bank-A-Count Corp.
Rudolph, Wisconsin

Scope

We have examined Bank-A-Count Corp.'s (Bank-A-Count) accompanying assertion titled "Bank-A-Count Corp.'s Assertion" (the "assertion") that the controls within Bank-A-Count's Print Services System (the "system") were effective throughout the period November 1, 2021 to April 30, 2022, to provide reasonable assurance that Bank-A-Count's service commitments and system requirements were achieved based on the trust services criteria relevant to security, processing integrity, and confidentiality (the "applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Bank-A-Count is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Bank-A-Count's service commitments and system requirements were achieved. Bank-A-Count has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Bank-A-Count is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Bank-A-Count's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Bank-A-Count's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independent Service Auditor's Report (Continued)

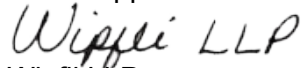
Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Bank-A-Count's Print Services System were effective throughout the period November 1, 2021 to April 30, 2022, to provide reasonable assurance that Bank-A-Count's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.


Wipfli LLP

Minneapolis, Minnesota
June 17, 2022

Attachment A – Description of the Boundaries of Bank-A-Count Corp.'s Print Services Systems

Attachment A – Description of the Boundaries of Bank-A-Count Corp.’s Print Services System

Company Overview

Bank-A-Count Corp. (“Bank-A-Count”) serves as a printer and mailer of documents containing variable data commonly used in financial services, property management, and markets with similar needs.

The main products of Bank-A-Count include personal and business checks, payment coupons, variably printed letters or announcements, monthly statements, and related products.

Privately owned, Bank-A-Count serves companies across the United States and has a customer base of over a thousand customers that place ongoing repeat orders.

Bank-A-Count maintains two separate manufacturing and servicing facilities in Rudolph, Wisconsin, and an administrative support office in nearby Wisconsin Rapids, Wisconsin.

Services Provided

Bank-A-Count is a data processing, imaging, and delivery services provider, delivering responsive service and fast turnaround time on orders of any size. Core business services focus on offering full-service document solutions directly to customers or to distributor-based customer clientele, which in turn sell Bank-A-Count products to their clientele as an outsourced solution offering.

Risk Management

Employees of Bank-A-Count, from line staff to senior management, have a responsibility for maintaining an effective internal control environment. Bank-A-Count’s risk management policies provide guidelines for an enterprise-wide risk management program, including mission, strategic objectives, and corporate governance structure, as well as key program components and initiatives. Bank-A-Count has established principles and policies for identifying, assessing, monitoring, and controlling risk across the organization. Risk management efforts include provisions for compliance, operations, data integrity, reputation risk, and privacy and security. Common risk scenarios are tracked and graded based on their overall risk to the Company, as well as individual risk factors. Risk escalation and assessment procedures are structured to provide employees with the tools necessary for mitigating risk and identifying process improvement opportunities.

Organizational Structure

Bank-A-Count is organized into segments including Customer Service, Operations, Information Technology, Human Resources, Marketing, and the Management Team. These segments work together to achieve one common goal: providing customers with flexible service solutions supported by reliable systems and a responsive staff.

Attachment A – Description of the Boundaries of Bank-A-Count Corp.’s Print Services System

Organizational Structure (Continued)

The Board of Directors, made up of senior management and independent directors, sets strategic goals and the corporate vision and periodically reviews policies and procedures developed by the Management Team. The Management Team works with department supervisors to develop policies, procedures, and reporting mechanisms for day-to-day operations. Supervisors and production staff implement the policies and procedures to facilitate the corporate vision.

Policies

Bank-A-Count has numerous policies in place to address the varying intricacies of its business. Policy statements exist for select enterprise functions and range from covering risk management programs to covering policies that guide personnel decisions. More specifically, policies are in place to address appropriateness with regard to infrastructure, software, people, procedures, and data.

Bank-A-Count’s policies are designed to protect the confidentiality, processing integrity, and security of its system and operations and to safeguard its business information and that of its customers and user organizations.

Policies defined as important to the organization are communicated to personnel with regular frequency. Existing employees periodically receive ongoing training on companywide policies. These policies are addressed with new hires at the time of an initial orientation and during appropriate follow-up sessions. New hires are informed of other policies that pertain directly to their work during on-the-job training within their department. Bank-A-Count’s Employee Handbook is posted on the internal intranet site and available for employees’ review of pertinent policies.

Bank-A-Count’s policies are periodically reviewed, as necessary, with updates approved by the Chief Executive Officer (CEO) and President. Changes to the Company’s policies are communicated to staff as soon as feasible. New policies are established, or updates to existing ones are considered to comply with environmental, regulatory, or technological changes that may impact business. Likewise, competitive situations or other outside influence, regulatory compliance, or internal considerations may also drive attention to policy statements. Policies are subject to ongoing monitoring by management.

Employees aware of policy infringements or those who have concerns related to policy terms are instructed to report the issue immediately to supervisory personnel within their department or facility or to a member of the Management Team.

General Computer Controls

General computer controls establish the control environment in which computer application systems are developed and operated.

The following significant areas of the data processing environment and general controls for Bank-A-Count are discussed in this section.

Attachment A – Description of the Boundaries of Bank-A-Count Corp.’s Print Services System

General Computer Controls (Continued)

Overview of Processing Environment

Bank-A-Count uses a dedicated department and dedicated personnel to support the document processing functions. Bank-A-Count incorporates various general computer controls to support and maintain software packages that are relevant to Bank-A-Count’s document solutions product line. The systems are physically located in two Rudolph, Wisconsin, production facilities; an administrative and marketing support location in Wisconsin Rapids, Wisconsin; and a third-party colocation facility in Port Edwards, Wisconsin.

Production Processing

Bank-A-Count employees perform and monitor the preprocessing of production data for checks, variable print mailings, and coupon books in various print formats. Bank-A-Count uses software to assist in the monitoring of required process controls and tasks to help ensure the proper outcome of the process. Bank-A-Count uses a third-party-provided postal processing software package and applies postal system updates, as required, for internal applications. Changes to the production processing environment are reviewed regularly.

Critical Infrastructure

Bank-A-Count leverages third-party hosted infrastructure to host the bank-a-count.com identity provider and portal components.

The third party provides multizone redundancy, auto-scaling capabilities, and multiregion failovers. It provides physical security, environmental protection, and redundant infrastructure to Bank-A-Count. Bank-A-Count’s Management Team obtains and reviews the third party’s System and Organization Controls (SOC) report to evaluate the internal control environment and the impact of exceptions noted for relevant Bank-A-Count controls.

Software

Bank-A-Count’s identity provider service, internal applications, and bank-a-count.com portal are applications developed and maintained by Bank-A-Count’s in-house Software Engineering group. The Software Engineering group enhances and maintains these services to support the needs of Bank-A-Count, its customers, and its end users.

Data

Data, as defined by Bank-A-Count, falls into one of the following classifications:

- Account
- Client
- Transactional
- Operational

Account data refers to data entered by end users and relying parties during registration and used by Bank-A-Count and its software to identify and communicate with the end user.

Attachment A – Description of the Boundaries of Bank-A-Count Corp.’s Print Services System

General Computer Controls (Continued)

Physical Access Controls

Bank-A-Count, as well as Bank-A-Count’s third-party colocation provider, has policies and procedures in place to control access to its data processing facilities and assets. These policies and procedures limit physical access to confidential data to individuals designated by Bank-A-Count’s Management Team.

Change and Configuration Control

Changes to system software are approved by management and deployed by a third-party IT security and support firm.

Major system changes and projects are accompanied by regular status reports to Bank-A-Count’s management for review of milestones and security implications.

Logical Security, Access, and Audit Controls

Bank-A-Count’s staff is responsible for developing standards and administering logical security for selected systems and applications. They follow documented policies and procedures to establish access to information assets based on employees’ roles in the organization on a need-to-know basis.

Fault Tolerance and Data Recovery

A tested backup system is in place.

Bank-A-Count’s servers are protected from hard disk failure with redundant array of independent disks (RAID) 5 configurations for disk storage. In addition, duplicate server and mainframe systems are maintained in offline mode, ready to be used if necessary.

Intrusion Detection and Incident Response

An active intrusion detection system (IDS) monitors the network for suspicious activity.

Firewall Controls

Bank-A-Count, in coordination with its third-party provider, has deployed a managed firewall solution to protect its network.

Antivirus and Antispyware Controls

The network environment is protected by a multilayered antivirus system.

Environmental Controls

Bank-A-Count and its third-party colocation facility install and maintain support equipment for controlling environmental conditions of the servers and telecommunications equipment.

Attachment A – Description of the Boundaries of Bank-A-Count Corp.’s Print Services System

Complementary User Entity Control Considerations

Bank-A-Count’s controls were designed with the assumption that certain complementary user entity controls would be operating effectively at user entities. The controls described in this report occur at Bank-A-Count and cover only a portion of a comprehensive internal controls structure. Each user entity must address the various aspects of internal control that may be unique to its particular system. This section describes the complementary user entity controls that should be developed, placed in operation, and maintained at user entities as necessary to meet the trust services criteria stated in the description of Bank-A-Count’s system. User entities should determine whether adequate controls have been established to provide reasonable assurance that:

Complementary User Entity Controls
The customer is responsible for providing the data in the agreed-upon format by the date specified in the contract to ensure proper processing.
The customer is responsible for approving paper stock or forms that meet equipment specifications.
The customer is responsible for approving proofs if provided.
The customer is responsible for providing Bank-A-Count with accurate data.
Access to the FTP site and web portal are secured by username and password. The customer is responsible for maintaining the security of their account.
The customer is responsible for tracking orders placed online through the website using the order tracking function.
The customer is responsible for reconciliation of orders based on information on the billing statement, information on the web, or reports made upon request.
The customer is responsible for providing notification of delivery or printing errors.

Attachment A – Description of the Boundaries of Bank-A-Count Corp.’s Print Services System

Complementary Subservice Organization Controls

Bank-A-Count’s controls related to the Print Services System cover only a portion of overall internal control for each user entity of Bank-A-Count. It is not feasible for the trust services criteria related to Print Services System to be achieved solely by Bank-A-Count. Therefore, each user entity’s internal control must be evaluated in conjunction with Bank-A-Count’s controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization(s) as described below.

Complementary Subservice Organization Controls
Subservice organizations providing hosting services have implemented procedures to authenticate users to any Bank-A-Count infrastructure and data.
Subservice organizations establish, monitor, and maintain sufficient internal controls to help ensure their security administration is effective.
Subservice organizations providing hosting services have implemented procedures to provide physical and environmental controls for any Bank-A-Count infrastructure device.
Subservice organizations have implemented procedures for identifying, investigating, remediating, and communicating security incidents.
Subservice organizations maintain a Disaster Recovery Plan and Business Continuity Plan.
Subservice organizations implement controls to prevent or detect and act on the introduction of unauthorized or malicious software.

Attachment B – Service Commitments and System Requirements of Bank-A-Count Corp.'s Print Services System

Attachment B – Service Commitments and System Requirements of Bank-A-Count Corp.'s Print Services System

Bank-A-Count designs its processes and procedures related to variably printed documents to meet its objectives for the successful delivery of printed products. Those objectives are based on the service commitments Bank-A-Count makes to user entities, the laws and regulations that govern the provision of checks and other printed products, and the financial, operational, and compliance requirements Bank-A-Count has established for the services. The print services of Bank-A-Count are subject to the security and privacy requirements of the Gramm-Leach-Bliley Act (GLBA) as well as state privacy security laws and regulations in the jurisdictions in which Bank-A-Count operates.

Security, processing integrity, and confidentiality commitments to user entities are documented and communicated in service level agreements (SLA) and other customer agreements, as well as in the description of the service offering provided online.

- Security commitments include principles within the fundamental designs to permit system users to access the information they need based on their roles in the system, while restricting them from accessing information not needed for their role.
- Processing integrity commitments include the complete and accurate processing of variably printed documents in accordance with specifications to meet customer objectives.
- Confidentiality commitments include the use of encryption technologies to protect customer data both at rest and in transit.

Bank-A-Count establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Bank-A-Count's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies related to how the service is designed and developed, the system is operated, the internal business systems and networks are managed, and employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required when providing variable print document services.