A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
Bank-A-Count

Year:
2025

Bank A Count Corp.

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

November 1, 2024 to April 30, 2025

Table of Contents

SECTION 1

ASSERTION OF BANK-A-COUNT MANAGEMENT

ASSERTION OF BANK-A-COUNT MANAGEMENT

July 10, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within Bank-A-Count's ('the Company') Print Services System throughout the period November 1, 2024 to April 30, 2025, 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, Availability, Processing Integrity, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Bank-A-Count's Description of Its Print Services System throughout the period November 1, 2024 to April 30, 2025" 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, 2024 to April 30, 2025, to provide reasonable assurance that Bank-A-Count's service commitments and system requirements were achieved based on the 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 "Bank-A-Count's Description of Its Print Services System throughout the period November 1, 2024 to April 30, 2025".

Bank-A-Count uses Strata Defense (or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Bank-A-Count, to achieve Bank-A-Count's service commitments and system requirements based on the applicable trust services criteria. The description presents Bank-A-Count's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Bank-A-Count's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Bank-A-Count's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Bank-A-Count's controls.

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.

Except for the matter described in the following paragraph, we assert that the controls within the system were effective throughout the period November 1, 2024 to April 30, 2025 to provide reasonable assurance that Bank-A-Count's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Bank-A-Count's controls operated effectively throughout that period.

Accompanying description states that changes to the system will be authorized and approved by management prior to implementation. However, as noted in Section 4, controls relating to the change management process were not operating effectively throughout the period November 1, 2024 to April 30, 2025. As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on criteria CC8.1, "The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives."

Matt Fillmore
President
Bank-A-Count

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Bank-A-Count:

Scope

We have examined Bank-A-Count's ('Bank-A-Count' or 'the Company') accompanying assertion titled "Assertion of Bank-A-Count Management" (assertion) that the controls within Bank-A-Count's Print Services System were effective throughout the period November 1, 2024 to April 30, 2025, 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, Availability, Processing Integrity, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Bank-A-Count uses Strata Defense to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Bank-A-Count, to achieve Bank-A-Count's service commitments and system requirements based on the applicable trust services criteria. The description presents Bank-A-Count's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Bank-A-Count's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Bank-A-Count, to achieve Bank-A-Count's service commitments and system requirements based on the applicable trust services criteria. The description presents Bank-A-Count's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Bank-A-Count's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

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 (Bank-A-Count 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 AICPA. 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 the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its 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.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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.

Basis for Qualified Opinion

Bank-A-Count states in its description that changes to the system will be authorized and approved by management prior to implementation. However, as noted in Section 4, controls related to were not operating effectively throughout the period November 1, 2024 to April 30, 2025 . As a result, controls did not provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on CC8.1, "The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives."

Opinion

In our opinion, except for the matter described in the preceding paragraph, management's assertion that the controls within Bank-A-Count's Print Services System were suitably designed and operating effectively throughout the period November 1, 2024 to April 30, 2025, 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, if complementary subservice organization controls and complementary user entity controls assumed in the design of Bank-A-Count's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Bank-A-Count's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Bank-A-Count, user entities of Bank-A-Count's Print Services System during some or all of the period November 1, 2024 to April 30, 2025, business partners of Bank-A-Count subject to risks arising from interactions with the Print Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
July 10, 2025

SECTION 3

BANK-A-COUNT'S DESCRIPTION OF ITS PRINT SERVICES SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2024 TO APRIL 30, 2025

OVERVIEW OF OPERATIONS

Company Background

Bank-A-Count, a privately owned corporation, was founded in 1956 as a provider of bookkeeping information through an automated check recording system. In the 1960s and 1970s, Bank-A-Count was a national leader in the supply of loan amortization schedules and related financial computations. As the need for amortization schedules declined, payment coupons were developed as a product line in the late 1970s, and check printing was established in the 1980s. Statement printing was developed in the early 2000s. In the 2010s, Bank-A-Count diversified its product offerings yet again by creating the variable print mailings product line. These mailings include statements, newsletters, advertising, proxy ballots, etc.

Today, Bank-A-Count provides processing services for a variety of industries and companies across the United States. Bank-A-Count's customers include financial institutions, property management companies, and other businesses. Services include payment coupons, variable print mailings, personal and business checks, and pre-inked stamps.

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.

Description of 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.

Principal Service Commitments and System Requirements

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. Availability commitments to user entities are not documented in the customer agreements:

- 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.

Components of the System

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 multi-region 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.

For custom applications, Bank-A-Count services are made available to pre-approved third-parties for implementation via a secure application programming interface (API).

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.

People

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.

Customer Service

Customer Service is responsible for day-to-day customer communications, order and file receipt, and order preprocessing.

Operations

The Operations area is responsible for order entry, file conversion, and daily production processing, resulting in the accurate and timely delivery of a quality finished product.

Information Technology

The Information Technology (IT) department is responsible for the development and ongoing maintenance of the applications used at Bank-A-Count. Management monitors information processing to determine that activities support current and future operating needs. In developing Bank-A-Count's strategic IT plan, management considers customer and internal service requirements, as well as Bank-A-Count's business goals and objectives.

Human Resources

Human Resources is responsible for recruiting and retaining qualified employees, plus overseeing staffing, compensation, employee relations and communications, training, employee benefits selection, and administration. Employees are regularly evaluated based on performance related to their specific job descriptions. Employees are required to sign confidentiality agreements.

Marketing

The Marketing department is responsible for developing and maintaining programs in support of the Company's efforts to identify and profitably meet the needs of their customers. This includes managing sales growth opportunities while considering profitability and evolution of changing market segments. Marketing support is provided for customer products using related and appropriate channel delivery methods (online, advertising, direct mail, tradeshows, etc.). The Marketing team works closely with Bank-A-Count's IT, Customer Service, and Operations Personnel to identify and respond to potential threats and opportunities among customers, competitors, suppliers, and channels.

Management Team

Members of the Management Team oversee the segments described above, in addition to sales, accounts receivable, accounts payable, and facilities management functions.

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. Account data for end users includes first name, last name, e-mail address, account globally unique identifier (GUID), and authorization history. For third-party implementations of Bank-A-Count's API, account data includes but is not limited to customer identifiers and customer secrets.

Processes, Policies and Procedures

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 establish the control environment in which computer application systems are developed and operated. The general computer control environment has an impact on the effectiveness of controls in application systems, including those used by Bank-A-Count.

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

- Overview of Processing Environment
- Production Processing
- Physical Security
- Logical Access
- Computer Operations - Backups
- Computer Operations - Availability
- Change Control

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. 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 Wausau, 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 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.

Physical Security

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.

Entrances to Bank-A-Count's facility are secured.

Bank-A-Count's data processing equipment is secured by a locked server cabinet with limited access. Co-located equipment is kept in a secure co-location facility, with access limited to individuals designated by Bank-A-Count's Management Team.

If contractors or vendors are in Bank-A-Count's facility, they are required to sign the visitor log and are accompanied by an employee of Bank-A-Count.

The physical storage media for equipment that is being retired is destroyed prior to disposal.

Logical Access

The IT Compliance Coordinator is responsible for developing standards and administering logical security for selected systems and applications. The IT Compliance Coordinator reports to the President and follows formal policies and procedures to establish appropriate access to information assets based on employees' roles in the organization on a need-to-know basis.

Bank-A-Count uses logical network security. Authorized employees are required to have user identifications (ID) and passwords established at the network level to access production applications and customer and business information.

The IT Compliance Coordinator establishes and administers security parameters and maintains user IDs on the network system. A process is followed when granting customer IDs for access to the file transfer protocol (FTP) sites. This process includes the application of file system permissions that limit access to authorized customer employees.

User IDs and passwords for the network include internal settings that allow a limited number of invalid access attempts before lockout. When a password has been deactivated, the account is unable to log in to the network for an established period of time. Passwords have a defined length and complexity and will be changed at established intervals. The system remembers a specified number of passwords and prevents reuse of these passwords.

Changes to user access are requested of and subject to approval by the President.

User accounts are disabled immediately when an employee leaves the organization. They are then deleted after being reviewed by a manager. User accounts are reviewed regularly to determine accuracy and necessity.

Normal network user accounts are not members of the domain administrator group.

Computer Operations - Backups

Incremental data backups are performed daily on systems, with full data backups being performed on a weekly basis. Monthly mainframe backups to drives are also made for archival purposes.

Bank-A-Count's servers are protected from hard disk failure with a redundant array of independent disks (RAID) 5 configurations for disk storage. The server equipment is covered under on-site maintenance agreements from vendors to facilitate replacement in the event of hardware component failure. In addition, duplicate server and mainframe systems are maintained in a secondary facility in offline mode, ready to be used if necessary.

Computer Operations - Availability

Bank-A-Count's third-party IT infrastructure provider has deployed a managed firewall solution to protect Bank-A-Count's network. Firewall administration is conducted via an encrypted method. Remote access by a third-party consultant is allowed via a password-protected virtual private network (VPN) connection. Firewall changes are authorized by the President.

The network environment is protected by a multilayered antivirus system. Antivirus protection is deployed in both server and desktop systems. Antispyware components are also active within the desktop systems. The environment is managed by a central console, which is reviewed on a weekly basis by the network administrator. Full system scans of the servers and desktops occur on a weekly basis. Checks for new virus definition files occur daily and, if available, are downloaded and installed automatically.

An active intrusion detection system (IDS) monitors the network for suspicious activity. The IDS notifies appointed staff of any high-level alerts immediately via e-mail. The IDS is monitored daily for any lower-level alerts or other activity that may need to be addressed.

FTP site activity and log review occur throughout the day to monitor logons, uploads, downloads, and suspicious activities.

Bank-A-Count has policies and procedures in place in the event a suspicious activity is identified.

Change Control

Changes to system software are approved by management and deployed by a third-party IT security and support firm. The President has been assigned responsibility for the patch management program. Critical security updates are downloaded and applied automatically to systems.

Desktop computer configurations are documented, inventoried, and managed with the assistance of a monitoring tool. Server configurations and network architecture are documented for disaster recovery purposes.

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

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses.

Redundancy is built into the physical infrastructure supporting the data center services to help ensure that there is no single point of failure that includes power and network connectivity.

Authorized employees may access the system via the Internet using a leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes Print Services System performed at two facilities located in Rudolph Wisconsin, as well as marketing and support systems performed at a facility located in Wisconsin Rapids Wisconsin.

This report does not include cloud hosting services provided by Strata Defense at facilities in Wausau, Wisconsin.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common/Security, Availability, Processing Integrity and Confidentiality criterion was applicable to the Bank-A-Count Print Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by Strata Defense at their facilities in Wausau WI.

Subservice Description of Services

Subservice Organizations	
Subservice Organization	**Function**
StrataDefense	IT Infrastructure Management

Complementary Subservice Organization Controls

Bank-A-Count's services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for the trust services criteria related to Bank-A-Count's services to be solely achieved by Bank-A-Count control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of Bank-A-Count.

The following subservice organization controls should be implemented by StrataDefense to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - StrataDefense		
Category	**Criteria**	**Control**
Logical and physical access controls	CC6.4	Bank-A-Count has procedures in place to control physical access to its data processing facilities and assets.
	CC6.8	Critical security updates are applied to systems. The software patch management program is utilized to track configuration, modifications, and management of infrastructure and software.
		Centrally managed antivirus software is in place and is configured for real-time scanning and full daily scans. Virus signatures are updated daily.
		Intrusion detection/prevention systems and other tools are used to identify, log, and report potential security breaches and other incidents. The system notifies the security administration team and/or the network administrator of potential incidents in progress.
System Operations	CC7.1	Management has defined configuration standards in the information security policies and procedures.

Subservice Organization - StrataDefense		
Category	**Criteria**	**Control**
	CC7.2	CCTV cameras monitor physical access to the entity's facilities and visitor access to the facility and server room require the visitor to sign a visitor log prior upon arrival.
		The badge access system logs successful and failed physical access attempts and the logs could be pulled for review when necessary.

Bank-A-Count management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet the relevant trust services criteria through written contracts, such as SLAs. In addition, Bank-A-Count performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and the subservice organization
- Reviewing attestation reports over services provided by vendors and the subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Bank-A-Count's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for the Trust Services Criteria related to Bank-A-Count's services to be solely achieved by Bank-A-Count control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Bank-A-Count's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Bank-A-Count.
2. User entities are responsible for notifying Bank-A-Count of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Bank-A-Count services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Bank-A-Count services.
6. User entities are responsible for providing Bank-A-Count with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Bank-A-Count of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.