

SOC or OTHER ATTESTATION REVIEW CHECKLIST

Attestation Type:	2023 SOC 2 Type 2 Report
Vendor Name:	Fin Technologies, Inc. dba Mantl
Report Date Range:	April 1, 2022 to March 31, 2023
Service Addressed by Report:	Platform to allow commercial and small business clients to open deposit accounts online (checking). This SOC Report is being reviewed as a new vendor onboarding for the implementation of Mantl.

1. Vendor Data Classification	<input type="checkbox"/> Public <input checked="" type="checkbox"/> Bank Confidential <input type="checkbox"/> Customer Confidential. <input type="checkbox"/> Employee Confidential
2. The date range is within the last 18 months?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
3. This SOC Attestation is relevant to the service the Bank receives from this Vendor? A-Lign Assurance is the independent auditor.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
4. The report cover letter opinion addresses both the design and effectiveness of control and the opinions are favorable and unqualified:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Section I
5. The management assertion addresses both the design and effectiveness of control and the opinions are favorable and unqualified:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Section II
6. Has the report been subjected to a 3 rd party review? <u>Comment:</u> VI's review resulted in an overall score of 4.25 out of 5 which is considered very positive. The score was impacted by the vendors reliance on fourth parties. Fin Technologies, Inc. dba Mantl uses the following fourth parties: <ul style="list-style-type: none"> - Alloy - The Identity Decisioning Platform that assists banks and fintech companies automate their decisions for onboarding, transaction monitoring and credit underwriting. - First Data - Provides secure and innovative payment technology and services solutions to merchants, including small-and mid-sized businesses, financial institutions, and government agencies around the world. - Plaid - Instant Account Verification (IAV) provider allowing end users to easily obtain their bank account and routing numbers by providing their bank account login information. Plaid outsources its physical facility security to Amazon Web Services (AWS). Plaid ensures that AWS has sufficient availability and security control in place and monitors 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

SOC or OTHER ATTESTATION REVIEW CHECKLIST

Attestation Type:	2023 SOC 2 Type 2 Report
Vendor Name:	Fin Technologies, Inc. dba Mantl
Report Date Range:	April 1, 2022 to March 31, 2023
Service Addressed by Report:	Platform to allow commercial and small business clients to open deposit accounts online (checking). This SOC Report is being reviewed as a new vendor onboarding for the implementation of Mantl.

<p>adherence to those processes and procedures.</p> <ul style="list-style-type: none"> - SendGrid - Customer communication platform for transactional and marketing email. SendGrid outsources its physical facility security to Steadfast data center. SendGrid ensures that Steadfast has sufficient availability and security control in place and monitors adherence to those processes and procedures. - GCP - Cloud services provider for Mantl servers, infrastructure, databases and other cloud building blocks. <p>There are no Exceptions in the Report.</p>	
7. The scope of control addressed by the report is relevant?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
8. a. Are control weaknesses or exceptions noted in the report? (List) b. If yes, Control weaknesses are acceptable and/or the vendor's management has sufficient plans to address noted weaknesses? Comment: There are no Exceptions in the Report.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No Not Applicable
9. Does the SOC Attestation indicate the existence of a BC Plan? See page 14 of the SOC report which mentions Mantl's approach in taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel. Specific control activities that the service organization has implemented in this area are described below: 1) Business and industry risks discussed during the periodic management risk assessment meetings, discussed below, and that impact employees are communicated to the employee base via conferences or email by Management. 2) Annual Security Awareness Training is attended by personnel which focuses on maintaining the security, availability and confidentiality of the proprietary and customer-servicing systems and related data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

SOC or OTHER ATTESTATION REVIEW CHECKLIST

Attestation Type:	2023 SOC 2 Type 2 Report
Vendor Name:	Fin Technologies, Inc. dba Mantl
Report Date Range:	April 1, 2022 to March 31, 2023
Service Addressed by Report:	Platform to allow commercial and small business clients to open deposit accounts online (checking). This SOC Report is being reviewed as a new vendor onboarding for the implementation of Mantl.

3) Mantl's management team has frequent, direct communication via "stand-up" and similar meetings with employees to ensure employees understand the most critical tasks and receive clear guidance from management on those tasks.	
10. User/Client Control Considerations:	Attach Pages: See CUEC Mapping for Bank response.
11. All user/client control considerations are, or will be, sufficiently performed? Reviewed by: Information Security, Information Technology, Product Development, Commercial Banking & Third Party Risk Management. <u>Comment: All applicable user controls will be in place upon implementation.</u>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

ATTESTATION REVIEWED BY

Third Party Risk Management	Signature: <i>Edie Friedel</i> Date: _____ Email: ediefriedel@amalgamatedbank.com
Information Technology	Signature: <i>Adrian Glace</i> <small>Adrian Glace (Apr 3, 2024 21:58 EDT)</small> Date: _____ Email: adrianglace@amalgamatedbank.com
Product Development	Signature: <i>Carol Ng</i> Date: _____ Email: carolng@amalgamatedbank.com
Commercial Banking	Signature: <i>Joseph Bae</i> <small>Joseph Bae (Mar 29, 2024 11:49 EDT)</small> Date: _____ Email: joebae@amalgamatedbank.com
Information Security	Signature: <i>Sal Mannino</i> <small>Sal Mannino (Mar 29, 2024 17:34 EDT)</small> Date: _____ Email: salmannino@amalgamatedbank.com



Created By : Chandler French on Feb-27-2024

Status : Completed by Chandler French on Feb-27-2024

Name : Financial Software-as-a-Service Platform Services System (SOC2)

Type: SOC2 Type2

Vendor : Fin Technologies, Inc. dba Mantl

Scope Start : Apr-01-2022

Contract : Commercial Digital Acct Opening

Scope End : Mar-31-2023

Fourth Party : N/A

Bridge Letter :

Opening Narrative

We have received and reviewed the Service Organization Control SOC2 Type 2 Report on controls for Fin Technologies, Inc. dba Mantl - Financial Software-as-a-Service Platform Services System. The report, issued by A-Lign Assurance, is for the period April 01, 2022 to March 31, 2023. The report includes testing of specific controls.

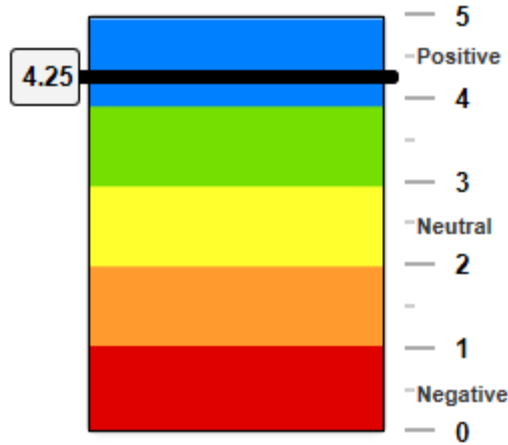
Auditor's Opinion

In A-Lign Assurance's opinion, "in all material respects,

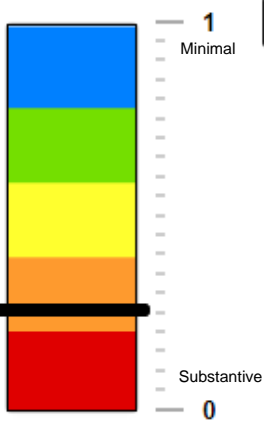
- a. the description presents Mantl's Financial Software-as-a-Service Platform Services System that was designed and implemented throughout the period April 1, 2022 to March 31, 2023, in accordance with the description criteria.
- b. the controls stated in the description were suitably designed throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Mantl's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Mantl's controls throughout that period.
- c. the controls stated in the description operated effectively throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that Mantl'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 Mantl's controls operated effectively throughout that period."

Summary

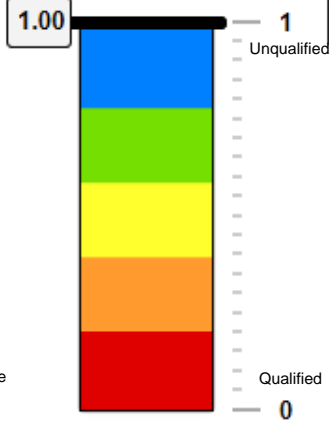
Overall Score



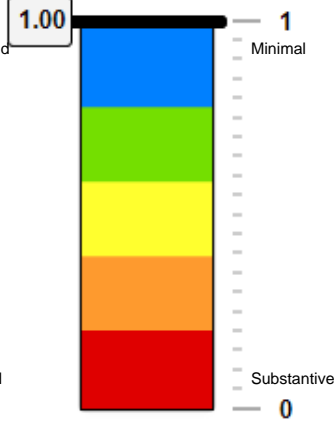
Fourth Parties



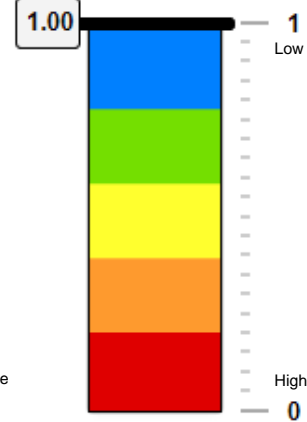
Audit Opinions



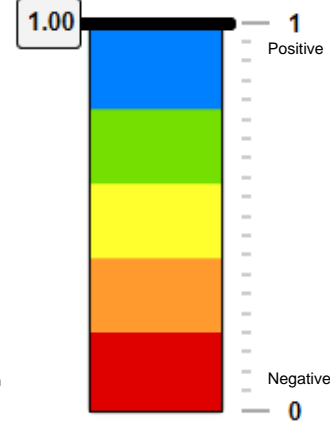
of Exceptions



Exception Severity



Management Response



Main Narrative

Control Objectives

Control Environment – The entity demonstrates a commitment to integrity and ethical values.

Control Environment – The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control Environment – Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control Environment – The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.



Control Environment – The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Communication and Information – The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Communication and Information – The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Communication and Information – The entity communicates with external parties regarding matters affecting the functioning of internal control.

Risk Management and Implementation of Controls – The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Risk Management and Implementation of Controls – The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Risk Management and Implementation of Controls – The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Risk Management and Implementation of Controls – The entity identifies and assesses changes that could significantly impact the system of internal control.

Monitoring Activities – The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Monitoring Activities – The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control Activities – The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control Activities – The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control Activities – The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Logical and Physical Access Controls – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Logical and Physical Access Controls – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

Logical and Physical Access Controls – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Logical and Physical Access Controls – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

Logical and Physical Access Controls – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

Logical and Physical Access Controls – The entity implements logical access security measures to protect against threats



from sources outside its system boundaries.

Logical and Physical Access Controls – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Logical and Physical Access Controls – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

System Operations – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

System Operations – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

System Operations – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

System Operations – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

System Operations – The entity identifies, develops, and implements activities to recover from identified security incidents.

Change Management – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Risk Mitigation – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Risk Mitigation – The entity assesses and manages risks associated with vendors and business partners.

Availability – The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Availability – The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data-backup processes, and recovery infrastructure to meet its objectives.

Availability – The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Confidentiality – The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

Confidentiality – The entity disposes of confidential information to meet the entity's objectives related to confidentiality.



User Entity Control #1

CUEC: User entities are responsible for understanding and complying with their contractual obligations to Mantl.

Comment

Applicable (Y/N) : Bank response to the CUECs may be found in a separate CUEC Mapping worksheet.

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #2

CUEC: User entities are responsible for notifying Mantl of changes made to technical or administrative contact information.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #3

CUEC: User entities are responsible for maintaining their own system(s) of record.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #4

CUEC: User entities are responsible for ensuring the supervision, management, and control of the use of Mantl services by their personnel.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #5

CUEC: User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Mantl services.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #6

CUEC: User entities are responsible for providing Mantl with a list of approvers for security and system configuration changes for data transmission.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #7

CUEC: User entities are responsible for immediately notifying Mantl of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



Subservice Organization Control #1

CSOC:

Documented policies and procedures are in place regarding systems authentication and access.

Documented hardening procedures are in place for setting up and hardening servers.

Assets are assigned owners who are responsible for evaluating access based on job roles.

The entity uses a Single Sign On (SSO) functionality to access the entity's network and applications.

Asymmetric keys are utilized to authenticate to the server.

A role-based security process has been defined with an access control system that is required to use roles when possible.

Comment

Applicable (Y/N) : Yes

Responsible 4th Party Vendor : Alloy

Monitored (Y/N) : Yes, CC6.1

Control Owner : Fin Technologies, Inc. dba Mantl

Initial & Date :



Subservice Organization Control #2

CSOC:

Physical access to data centers is approved by an authorized individual.

Physical access is revoked within 24 hours of the employee or vendor record being deactivated.

Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.

Physical access points to server locations are managed by electronic access control devices.

Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Google-owned data centers are protected by fire detection and suppression systems.

Google-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.

Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Google-owned data centers.

Google-owned data centers have generators to provide backup power in case of electrical failure.

Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.

GCP performs periodic reviews of colocation service providers to validate adherence with GCP security and operational standards.

Google Cloud Storage (GCS)-Specific - Google Cloud Storage performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.

GCS-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.

GCS-Specific - Objects are stored redundantly across multiple fault-isolated facilities.

GCS-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.

Google Cloud PostgreSQL-Specific - If enabled by the customer, Google Cloud PostgreSQL backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.

Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.

Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.

Critical GCP system components are replicated across multiple Availability Zones and backups are maintained.

Backups of critical GCP system components are monitored for successful replication across multiple Availability Zones.

Comment

Applicable (Y/N) : Yes

Responsible 4th Party Vendor : Google Cloud Platform

Monitored (Y/N) : Yes, CC6.4; 7.2; A1.2

Control Owner : Fin Technologies, Inc. dba Mantl

Initial & Date :

Subservice Organization Control #3

CSOC:
Key Management Services (KMS)-Specific - Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
KMS-Specific - Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.
Physical access to data centers is approved by an authorized individual.
Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Physical access points to server locations are recorded by closed CCTV. Images are retained for 90 days, unless limited by legal or contractual obligations.
Physical access points to server locations are managed by electronic access control devices.
Amazon-owned data centers are protected by fire detection and suppression systems.
Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
UPS units provide backup power in the event of an electrical failure in Amazon-owned data centers.
Amazon-owned data centers have generators to provide backup power in case of electrical failure.
Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.
AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
Incidents are logged within a ticketing system, assigned severity rating, and tracked to resolution.
Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

Comment

Applicable (Y/N) : Yes

Responsible 4th Party Vendor : Plaid

Monitored (Y/N) : Yes, CC6.4; A1.2

Control Owner : Fin Technologies, Inc. dba Mantl

Initial & Date :

Subservice Organization Control #4

CSOC:
Access to physical facilities housing hosted systems is restricted to authorized users.
Environmental mechanisms provide protection over fire, water, power outages, temperature changes and natural disasters.
Software and recovery infrastructure are implemented over hosted systems.

Comment

Applicable (Y/N) : Yes

Responsible 4th Party Vendor : SendGrid

Monitored (Y/N) : Yes, CC6.4; A1.2

Control Owner : Fin Technologies, Inc. dba Mantl

Initial & Date :



Closing Narrative

Based on our review of the SOC2 Type 2 Report and A-Lign Assurance's opinion it can be reasonably assumed that adequate controls were in place for Fin Technologies, Inc. dba Mantl - Financial Software-as-a-Service Platform Services System for the period from April 01, 2022 to March 31, 2023.

Based upon the information provided, reviewed, and upon the number of exceptions identified by the auditor we have no reason to express any level of concern.

SOC Review Form

Instruction

Click on each tab, or use the links to the right, to take you to review of the Control Objectives, Complimentary User Entity Controls (CUECs), or Exceptions. With the third party engagement in mind, select the appropriate response for each control objective that is relevant for your engagement. Subsequently, the CUECs and Exceptions will only apply to the relevant control objectives selected.

LINKS

[Control Objectives](#)

[CUECs](#)

[Exceptions](#)

SOC Information

SOC Report Type: SOC 2, Type 2

Coverage Period: April 1, 2022 to March 31, 2023

Product / Services in Scope: Mantl
(if different then services above)

Summary of Vendor Services

Vendor Name / Engagement: Fin Technologies, Inc. dba Mantl

Business Unit / Business Owner: Product Development / Carol Ng

Description of Services (VI): Platform to allow commercial and small business clients to open deposit accounts online (checking).

This SOC Report is being reviewed as a new vendor onboarding for the implementation of Mantl.

Classification of Data Shared: Bank Confidential

SOC Attestation

Has a SOC review been conducted previously for this engagement? No

Have there been changes to relevant control objectives since implementation? No

SOC Control Objectives Review Form

Instruction:

When performing the SOC review of your third party engagement, the relevant control objectives will need to be identified to ensure compliance. Review each of the Control Objectives listed below, select whether the control objective is relevant or not relevant to your engagement. If the control objective is not relevant, or unsure of relevance, please use the Notes section to provide additional context and Third Party Risk Management will assist.

#	SOC Control Objectives	Relevance	Justification / Notes
CC 1.1	Control Environment -The entity demonstrates a commitment to integrity and ethical values.	Relevant	
CC 1.2	Control Environment - The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Relevant	
CC 1.3	Control Environment – Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Relevant	
CC 1.4	Control Environment – The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Relevant	
CC 1.5	Control Environment – The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Relevant	
CC 2.1	Communication and Information – The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Relevant	
CC 2.2	Communication and Information – The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Relevant	
CC 2.3	Communication and Information – The entity communicates with external parties regarding matters affecting the functioning of internal control.	Relevant	
CC 3.1	Risk Management and Implementation of Controls – The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Relevant	
CC 3.2	Risk Management and Implementation of Controls – The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Relevant	
CC 3.3	Risk Management and Implementation of Controls – The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Relevant	
CC 3.4	Risk Management and Implementation of Controls – The entity identifies and assesses changes that could significantly impact the system of internal control.	Relevant	
CC 4.1	Monitoring Activities – The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Relevant	
CC 4.2	Monitoring Activities – The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Relevant	
CC 5.1	Control Activities – The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Relevant	
CC 5.2	Control Activities – The entity also selects and develops general control activities over technology to support the achievement of objectives.	Relevant	
CC 5.3	Control Activities – The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Relevant	
CC 6.1	Logical and Physical Access Controls – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Relevant	
CC 6.2	Logical and Physical Access Controls – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Relevant	
CC 6.3	Logical and Physical Access Controls – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Relevant	
CC 6.4	Logical and Physical Access Controls – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Relevant	
CC 6.5	Logical and Physical Access Controls – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Relevant	
CC 6.6	Logical and Physical Access Controls – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Relevant	
CC 6.7	Logical and Physical Access Controls – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Relevant	
CC 6.8	Logical and Physical Access Controls – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Relevant	
CC 7.1	System Operations – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Relevant	
CC 7.2	System Operations – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Relevant	
CC 7.3	System Operations – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Relevant	
CC 7.4	System Operations – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Relevant	
CC 7.5	System Operations – The entity identifies, develops, and implements activities to recover from identified security incidents.	Relevant	
CC 8.1	Change Management – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Relevant	
CC 9.1	Risk Mitigation – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Relevant	
CC 9.2	Risk Mitigation – The entity assesses and manages risks associated with vendors and business partners.	Relevant	
A1.1	Availability – The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Relevant	
A1.2	Availability – The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data-backup processes, and recovery infrastructure to meet its objectives.	Relevant	
A1.3	Availability – The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Relevant	
C1.1	Confidentiality – The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Relevant	
C1.2	Confidentiality – The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	Relevant	

CUEC No.	CUEC Description	Is this control applicable to the Bank?	Process Owner	Control Owner 1	Control Owner 2 (if applicable)	Amalgamated Bank's Internal Control
1	CUEC: User entities are responsible for understanding and complying with their contractual obligations to Mantl.	Yes	Commercial Banking	Commercial Banking	Legal	The Relationship Owner will partner with Legal to understand and comply with contractual obligations listed within the agreement.
2	CUEC: User entities are responsible for notifying Mantl of changes made to technical or administrative contact information.	Yes	Commercial Banking	Identity Access Management		This control will be determined and established upon implementation.
3	CUEC: User entities are responsible for maintaining their own system(s) of record.	Yes	Information Technology	Information Technology		The Bank maintains our own system(s) of record.
4	CUEC: User entities are responsible for ensuring the supervision, management, and control of the use of Mantl services by their personnel.	Yes	Commercial Banking	Identity Access Management	Information Technology	Logical Access controls are enforced via RSA IGL tool, administered by IT/Access Management Team and supported by the Identity & Access Management Procedures (IAM 2023)
5	CUEC: User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Mantl services.	Yes	Commercial Banking	Business Continuity		Commercial Banking, in collaboration with Business Continuity, completes their Business Impact Analysis (BIA) on an annual basis, ensuring that all systems and engagements are entered into the overall Bank Business Continuity and Disaster Recovery plan.
6	CUEC: User entities are responsible for providing Mantl with a list of approvers for security and system configuration changes for data transmission.	Yes	Commercial Banking	Information Technology / Engineering	Information Security	Commercial Banking will work with the Information Technology, Information Security and Engineering team to establish security and system configuration controls upon implementation.
7	CUEC: User entities are responsible for immediately notifying Mantl of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.	Yes	Information Security	Information Security		Security Incident Response Plan Reference Section: Appendix A -> Third Party Service provider Stipulates notification to vendor











Fin Technologies, Inc. dba Mantl_2023 SOC 2 Type 2 REVIEW_April 1 2022 to March 31 2023


Final Audit Report

2024-04-04

Created:	2024-03-29
By:	Brandon Singh (BrandonSingh@AmalgamatedBank.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAy43vtP0Juc7E3mH5hHv5hhmmUR5YokLa

"Fin Technologies, Inc. dba Mantl_2023 SOC 2 Type 2 REVIEW _April 1 2022 to March 31 2023" History


-  Document created by Brandon Singh (BrandonSingh@AmalgamatedBank.com)
2024-03-29 - 3:20:42 PM GMT
-  Document emailed to Carol Ng (carolng@amalgamatedbank.com) for signature
2024-03-29 - 3:22:17 PM GMT
-  Document emailed to Edie Friedel (ediefriedel@amalgamatedbank.com) for signature
2024-03-29 - 3:22:18 PM GMT
-  Document emailed to Joseph Bae (joebae@amalgamatedbank.com) for signature
2024-03-29 - 3:22:18 PM GMT
-  Document emailed to Sal Mannino (salmannino@amalgamatedbank.com) for signature
2024-03-29 - 3:22:18 PM GMT
-  Document emailed to Thomas Rivara (thomasrivara@amalgamatedbank.com) for signature
2024-03-29 - 3:22:18 PM GMT
-  Email viewed by Edie Friedel (ediefriedel@amalgamatedbank.com)
2024-03-29 - 3:23:11 PM GMT
-  Document e-signed by Edie Friedel (ediefriedel@amalgamatedbank.com)
Signature Date: 2024-03-29 - 3:24:10 PM GMT - Time Source: server
-  Email viewed by Carol Ng (carolng@amalgamatedbank.com)
2024-03-29 - 3:33:01 PM GMT
-  Document e-signed by Carol Ng (carolng@amalgamatedbank.com)
Signature Date: 2024-03-29 - 3:33:12 PM GMT - Time Source: server

 Email viewed by Joseph Bae (joebae@amalgamatedbank.com)

2024-03-29 - 3:49:37 PM GMT

 Document e-signed by Joseph Bae (joebae@amalgamatedbank.com)

Signature Date: 2024-03-29 - 3:49:44 PM GMT - Time Source: server

 Brandon Singh (BrandonSingh@AmalgamatedBank.com) replaced signer Thomas Rivara (thomasrivara@amalgamatedbank.com) with Adrian Glace (adrianglace@amalgamatedbank.com)


2024-03-29 - 3:56:26 PM GMT

 Document emailed to Adrian Glace (adrianglace@amalgamatedbank.com) for signature

2024-03-29 - 3:56:27 PM GMT

 Email viewed by Sal Mannino (salmannino@amalgamatedbank.com)


2024-03-29 - 9:33:55 PM GMT

 Document e-signed by Sal Mannino (salmannino@amalgamatedbank.com)

Signature Date: 2024-03-29 - 9:34:15 PM GMT - Time Source: server

 Email viewed by Adrian Glace (adrianglace@amalgamatedbank.com)

2024-04-04 - 1:58:03 AM GMT

 Document e-signed by Adrian Glace (adrianglace@amalgamatedbank.com)

Signature Date: 2024-04-04 - 1:58:16 AM GMT - Time Source: server

 Agreement completed.

2024-04-04 - 1:58:16 AM GMT