

SOC or OTHER ATTESTATION REVIEW CHECKLIST

Attestation Type:	2023 SOC 1 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 to 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 cloud hosting services to Amazon Web Services (AWS). 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

SOC or OTHER ATTESTATION REVIEW CHECKLIST

Attestation Type:	2023 SOC 1 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.



<ul style="list-style-type: none"> - SendGrid - Customer communication platform for transactional and marketing email. SendGrid outsources its data center hosting services to Steadfast data center. - 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. 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.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
10. User/Client Control Considerations:	Attach Pages:

SOC or OTHER ATTESTATION REVIEW CHECKLIST

Attestation Type:	2023 SOC 1 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.

	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:  <small>Adrian Glace (Apr 3, 2024 21:57 EDT)</small> Date: _____ Email: adrianglace@amalgamatedbank.com
Product Development	Signature: <i>Carol Ng</i> Date: _____ Email: carolng@amalgamatedbank.com
Commercial Banking	Signature:  <small>Joseph Bae (Mar 29, 2024 11:48 EDT)</small> Date: _____ Email: joebae@amalgamatedbank.com
Information Security	Signature: <i>Sal Mannino</i> <small>Sal Mannino (Mar 29, 2024 17:33 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 (SOC1)

Type: SOC1 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 SOC1 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, based on the criteria described in Mantl's assertion,

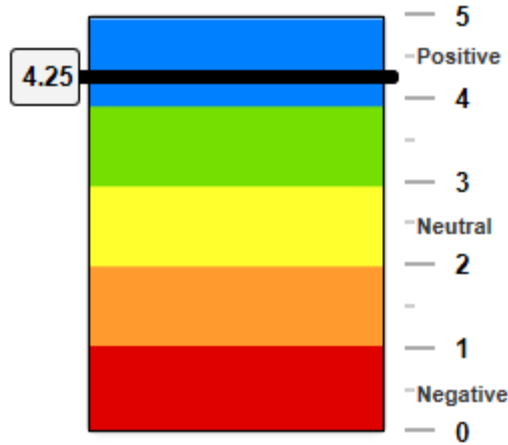
a. the description fairly presents the information technology general control system that was designed and implemented throughout the period April 1, 2022 to March 31, 2023.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period April 1, 2022 to March 31, 2023 and subservice organizations and user entities applied the complementary user entity controls contemplated in the design of Mantl's controls throughout the period April 1, 2022 to March 31, 2023.

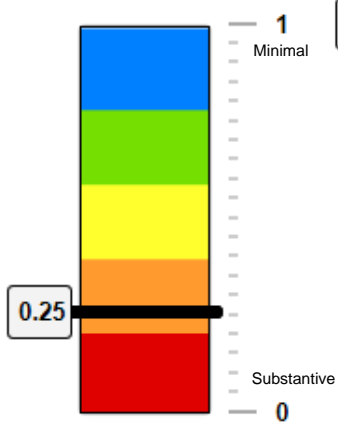
c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period April 1, 2022 to March 31, 2023, if complementary subservice organization and user entity controls assume in the design of Mantl's controls operated effectively throughout the period April 1, 2022 to March 31, 2023."

Summary

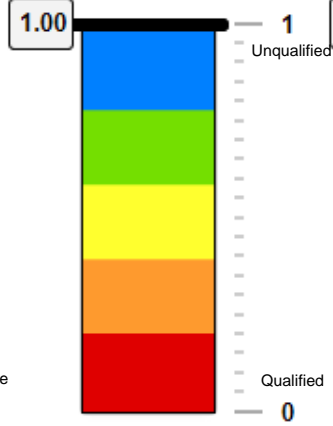
Overall Score



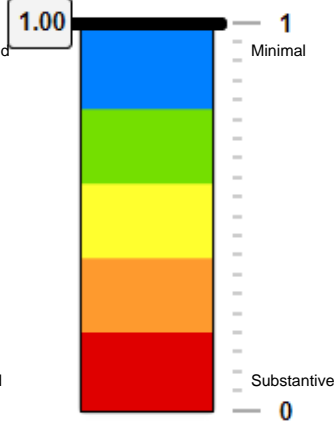
Fourth Parties



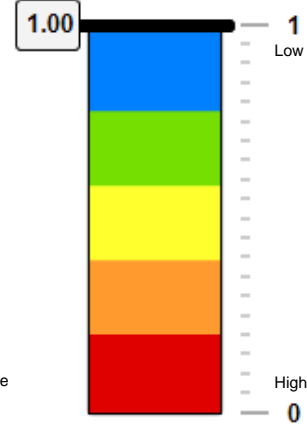
Audit Opinions



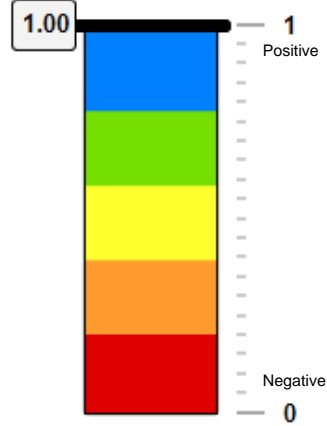
of Exceptions



Exception Severity



Management Response





Main Narrative

Control Objectives

INFORMATION SECURITY - Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.

DATA COMMUNICATIONS - Controls provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines.

CHANGE CONTROL - Controls provide reasonable assurance that new development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.

COMPUTER OPERATIONS - AVAILABILITY - Controls provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete accurate and timely manner.

COMPUTER OPERATIONS - BACKUP - Controls provide reasonable assurance that timely system backups of critical files to an off-site location are performed and available for restoration in the event of unexpected processing interruptions, with respect to user entities' internal control over financial reporting.

ACCOUNT SETUP - Controls provide reasonable assurance that Mantl books the account and subservices on behalf of the customer and passes all necessary customer information into the core banking application.

User Entity Control #1

CUEC: Information Security - User entities are responsible for documenting information security policies and procedures.

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: Information Security - User entities are responsible for granting appropriate access to new hires on their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #3

CUEC: Information Security - User entities are responsible for revoking access for terminations on their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #4

CUEC: Information Security - User entities are responsible for utilizing role-based security on their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #5

CUEC: Information Security - User entities are responsible for restricting administrative access on their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #6

CUEC: Information Security - User entities are responsible for utilizing strong password parameters on their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #7

CUEC: Information Security - User entities are responsible for utilizing account lockout and timeout on their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #8

CUEC: Information Security - User entities are responsible for logging and alerting unauthorized activity and threats on their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #9

CUEC: Information Security - User entities are responsible for reviewing access on a periodic basis on their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #10

CUEC: Information Security - User entities are responsible for restricting access to sensitive data on their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #11

CUEC: Data Communications - User entities are responsible for documenting information security policies and procedures.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #12

CUEC: Data Communications - User entities are responsible for utilizing firewalls to filter unauthorized inbound network traffic from the internet and deny all types of traffic not explicitly authorized by the firewall system rules.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #13

CUEC: Data Communications - User entities are responsible for limiting access to their firewalls.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #14

CUEC: Data Communications - User entities are responsible for securing data transmissions using strong encryption.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #15

CUEC: Data Communications - User entities are responsible for utilizing multi-factor authentication for remote access to their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #16

CUEC: Data Communications - User entities are responsible for revoking access for their terminated employees.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #17

CUEC: Data Communications - User entities are responsible for performing vulnerability scans and penetration tests on their systems on a periodic basis.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #18

CUEC: Data Communications - User entities are responsible for monitoring for security threats on their systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #19

CUEC: Data Communications - User entities are responsible for utilizing antivirus on their workstations and updating virus definitions regularly.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #20

CUEC: Change Control - User entities are responsible for documenting change control policies and procedures.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #21

CUEC: Change Control - User entities are responsible for authorizing, testing, and approving changes by management prior to implementation.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #22

CUEC: Change Control - User entities are responsible for tracking system changes in a change management tracking system.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #23

CUEC: Change Control - User entities are responsible for utilizing version control systems.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #24

CUEC: Change Control - User entities are responsible for separating development, test, and production environments.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #25

CUEC: Change Control - User entities are responsible for limiting access to development, test, and production and utilizing file integrity monitoring when segregations of duties incompatibilities exist.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #26

CUEC: Change Control - User entities are responsible for communicating bugs and requesting enhancements.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #27

CUEC: Change Control - User entities are responsible for user acceptance testing and approval.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #28

CUEC: Change Control - User entities are responsible for clearly communicating requirements.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #29

CUEC: Availability - User entities are responsible for documenting incident response procedures.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #30

CUEC: Availability - User entities are responsible for tracking incidents in a ticket tracking application.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #31

CUEC: Availability - User entities are responsible for monitoring ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #32

CUEC: Availability - User entities are responsible for performing backups on a regular basis.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #33

CUEC: Availability - User entities are responsible for monitoring backup failures.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #34

CUEC: Availability - User entities are responsible for documenting business continuity and disaster recovery plans.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #35

CUEC: Availability - User entities are responsible for performing vulnerability scans and penetration tests on a periodic basis.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #36

CUEC: Availability - User entities are responsible for installing antivirus on workstations and updating definitions regularly.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #37

CUEC: Backups - User entities are responsible for documenting backup and restore procedures.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #38

CUEC: Backups - User entities are responsible for automatically backing up systems on a regular schedule.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #39

CUEC: Backups - User entities are responsible for monitoring backups for failures.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #40

CUEC: Backups - User entities are responsible for documenting business continuity and disaster recovery plans.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #41

CUEC: Backups - User entities are responsible for testing business continuity and disaster recovery plans on a periodic basis.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #42

CUEC: Backups - User entities are responsible for storing backups and/or data in an encrypted format.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :



User Entity Control #43

CUEC: Backups - User entities are responsible for notifying Mantl of any issues in a timely manner.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

User Entity Control #44

CUEC: Backups -User entities are responsible for taking ownership of the account once the account has been created.

Comment

Applicable (Y/N) :

Monitored (Y/N) :

Control Owner :

Initial & Date :

Subservice Organization Control #1

CSOC: Customers are granted access to the production applications based on fraud scores and authentication tests.

Comment

Applicable (Y/N) : Yes

Responsible 4th Party Vendor : Alloy

Monitored (Y/N) : Yes, Information Security

Control Owner : Fin Technologies, Inc. dba Mantl

Initial & Date :

Subservice Organization Control #2

CSOC: Electronic files with approved funding transactions from customers are processed accurately and timely to initiate funding of new customer accounts via ACH or debit card/credit processing.

Comment

Applicable (Y/N) : Yes

Responsible 4th Party Vendor : First Data

Monitored (Y/N) : Yes, Information Security

Control Owner : Fin Technologies, Inc. dba Mantl

Initial & Date :



Subservice Organization Control #3

CSOC:

Plaid has a defined process for granting customers access to Plaid's API which is a Plaid product offering. Customers must be registered prior to obtaining access to Plaid's information system and services.

All emails sent from the Plaid's server are encrypted.

Customer authentication and session data is encrypted while in transit.

Comment

Applicable (Y/N) : Yes

Responsible 4th Party Vendor : Plaid

Monitored (Y/N) : Yes, Account Setup, Data Communications

Control Owner : Fin Technologies, Inc. dba Mantl

Initial & Date :

Subservice Organization Control #4

CSOC:

Data backups housing customer data are encrypted at rest.

Customer passwords and API keys are individually salted and hashed while stored.

Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.

Comment

Applicable (Y/N) : Yes

Responsible 4th Party Vendor : SendGrid

Monitored (Y/N) : Yes, Data Communications

Control Owner : Fin Technologies, Inc. dba Mantl

Initial & Date :

Subservice Organization Control #5

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.

Critical data is stored in encrypted format using software supporting AES- 256.

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, Uninterruptible Power Supply (UPS) units, and redundant power supplies.

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

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 SQL-Specific - If enabled by the customer, Google Cloud SQL 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.

Critical data is stored in encrypted format using software supporting AES- 256.

Comment

Applicable (Y/N) : Yes

Responsible 4th Party Vendor : Google Cloud Platform

Monitored (Y/N) : Yes, Information Security, Data Communications, Computer Operations -Availability, Computer Operations - Backup

Control Owner : Fin Technologies, Inc. dba Mantl

Initial & Date :



Closing Narrative

Based on our review of the SOC1 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 1, 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
1	INFORMATION SECURITY - Control activities provide reasonable assurance that system information, once entered into the system, is protected from unauthorized or unintentional use, modification, addition, or deletion.	Relevant	Role-Based-Access-Controls
2	DATA COMMUNICATIONS - Controls provide reasonable assurance that data transmissions between the service organization and its clients are complete, accurate, and secure and that data received is posted to the relevant systems in accordance with the Company's guidelines	Relevant	
3	CHANGE CONTROL - Controls provide reasonable assurance that new development of and changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transaction processing.	Relevant	
4	AVAILABILITY - Controls provide reasonable assurance that system processing is authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete accurate and timely manner.	Relevant	
5	BACKUP - Controls provide reasonable assurance that timely system backups of critical files to an off-site location are performed and available for restoration in the event of unexpected processing interruptions, with respect to user entities' internal control over financial reporting.	Relevant	
6	ACCOUNT SETUP - Controls provide reasonable assurance that Mantl books the account and subservices on behalf of the customer and passes all necessary customer information into the core banking application.	Relevant	

CUEC No.	CUEC Description	Relevant Control Objectives	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 documenting information security policies and procedures.	Control Objective 1: Information Security	Yes	Information Security	Information Security		This is done per Bank's information security policies.
2	CUEC: User entities are responsible for granting appropriate access to new hires on their systems.	Control Objective 1: Information Security	Yes	Information Technology	Information Security		Information Security Policy for Bank Personnel This is done per Bank's information security policies. Logical Access controls are enforced via RSA IGI tool, which is administered by IT/Access Management Team. Identity & Access Management Procedures (IAM 2023)
3	CUEC: User entities are responsible for revoking access for terminations on their systems.	Control Objective 1: Information Security	Yes	Information Technology	Information Security		This is done per Bank's information security policies. Logical Access controls are enforced via RSA IGI tool, which is administered by IT/Access Management Team. Identity & Access Management Procedures (IAM 2023)
4	CUEC: User entities are responsible for utilizing role-based security on their systems.	Control Objective 1: Information Security	Yes	Information Technology	Information Security		INFORMATION SECURITY GOVERNANCE POLICY (Section 2: Roles and responsibilities in Information Security Management)
5	CUEC: User entities are responsible for restricting administrative access on their systems.	Control Objective 1: Information Security	Yes	Information Technology/ Identity Access Management	Information Security		This is done per Bank's information security policies. Logical Access controls are enforced via RSA IGI tool, which is administered by IT/Access Management Team. Identity & Access Management Procedures (IAM 2023)
6	CUEC: User entities are responsible for utilizing strong password parameters on their systems.	Control Objective 1: Information Security	Yes	Information Technology	Information Security		INFORMATION SECURITY POLICY FOR BANK PERSONNEL (Section 7: Password Protection)
7	CUEC: User entities are responsible for utilizing account lockout and timeout on their systems.	Control Objective 1: Information Security	Yes	Information Technology/Engineering Team	Information Security		This is done per Bank's information Technology policy known as Information Technology Standards.
8	CUEC: User entities are responsible for logging and alerting unauthorized activity and threats on their systems.	Control Objective 1: Information Security	Yes	Information Security	Information Technology		Security Incident Response Plan Reference Section: Appendix A -> Third Party Service provider
9	CUEC: User entities are responsible for reviewing access on a periodic basis on their systems.	Control Objective 1: Information Security	Yes	Information Security	Information Technology		IDENTITY AND ACCESS MANAGEMENT PROCEDURES (IAM 2023) (Section 3: Responsibilities). User re-certification process is done annually.
10	CUEC: User entities are responsible for restricting access to sensitive data on their systems.	Control Objective 1: Information Security	Yes	Information Technology	Information Security		APPLICATION SECURITY POLICY (Section 3: Sensitive Data)
11	CUEC: User entities are responsible for documenting information security policies and procedures.	Control Objective 2: Data Communications	Yes	Information Security	Information Technology		Concur, reference the Information Security Policy for Overall Governance.
12	CUEC: User entities are responsible for utilizing firewalls to filter unauthorized inbound network traffic from the Internet and deny all types of traffic not explicitly authorized by the firewall system rules.	Control Objective 2: Data Communications	Yes	Information Security	Information Technology		Concur, reference the Information Security Policy for Overall Governance.
13	CUEC: User entities are responsible for limiting access to their firewalls.	Control Objective 2: Data Communications	Yes	Information Security	Information Technology		The Information Security Program 2023 Policy also references the Bank's utilization of firewalls. (Section 4: Firewall and Intrusion Prevention System).
14	CUEC: User entities are responsible for securing data transmissions using strong encryption.	Control Objective 2: Data Communications	Yes	Information Security	Information Technology		Concur, reference the Information Security Policy for Overall Governance.
15	CUEC: User entities are responsible for utilizing multi-factor authentication for remote access to their systems.	Control Objective 2: Data Communications	Yes	Information Security	Information Technology		Concur, reference the Information Security Policy for Overall Governance.
16	CUEC: User entities are responsible for revoking access for their terminated employees.	Control Objective 2: Data Communications	Yes	Information Security	Information Technology		Concur, reference the Information Security Policy for Overall Governance.
17	CUEC: User entities are responsible for performing vulnerability scans and penetration tests on their systems on a periodic basis.	Control Objective 2: Data Communications	Yes	Information Security	Information Technology		Concur, reference the Information Security Policy for Overall Governance.
18	CUEC: User entities are responsible for monitoring for security threats on their systems.	Control Objective 2: Data Communications	Yes	Information Security	Information Technology		Concur, reference the Information Security Policy for Overall Governance.
19	CUEC: User entities are responsible for utilizing antivirus on their workstations and updating virus definitions regularly.	Control Objective 2: Data Communications	Yes	Information Security	Information Technology		Concur, reference the Information Security Policy for overall governance. This is referenced in Information Technology Standards (Section 9: Security Infrastructure) and part of our Hardening process.
20	CUEC: User entities are responsible for documenting change control policies and procedures.	Control Objective 3: Change Control	Yes	Information Security	Information Technology		Change controls are practiced and are documented within ServiceNow and stakeholders meet before changes are implemented. (Control Changes)
21	CUEC: User entities are responsible for authorizing, testing, and approving changes by management prior to implementation.	Control Objective 3: Change Control	Yes	Information Security	Information Technology		Change controls are practiced and are documented within ServiceNow and stakeholders meet before changes are implemented. (Control Changes)
22	CUEC: User entities are responsible for tracking system changes in a change management tracking system.	Control Objective 3: Change Control	Yes	Information Security	Information Technology		Change controls are practiced and are documented within ServiceNow and stakeholders meet before changes are implemented. (Control Changes)
23	CUEC: User entities are responsible for utilizing version control systems.	Control Objective 3: Change Control	No	N/A	N/A		Not applicable, the Bank does not have a Dev System.
24	CUEC: User entities are responsible for separating development, test, and production environments.	Control Objective 3: Change Control	No	Information Security	Information Technology		Change controls are practiced and are documented within ServiceNow and stakeholders meet before changes are implemented. (Control Changes)
25	CUEC: User entities are responsible for limiting access to development, test, and production and utilizing file integrity monitoring when segregations of duties/incompatibilities exist.	Control Objective 3: Change Control	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
26	CUEC: User entities are responsible for communicating bugs and requesting enhancements.	Control Objective 3: Change Control	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
27	CUEC: User entities are responsible for user acceptance testing and approval.	Control Objective 3: Change Control	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
28	CUEC: User entities are responsible for clearly communicating requirements.	Control Objective 3: Change Control	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
29	CUEC: User entities are responsible for documenting incident response procedures.	Control Objective 4: Availability	Yes	Information Security	Information Security		The Security Incident Response Plan references the Bank's incident response procedures.
30	CUEC: User entities are responsible for tracking incidents in a ticket tracking application.	Control Objective 4: Availability	Yes	Information Security	Information Technology		Tickets are open in ServiceNow and incidents are handled by IT/IS
31	CUEC: User entities are responsible for monitoring ongoing system performance, security threats, changing resource utilization needs, and critical system activity.	Control Objective 4: Availability	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
32	CUEC: User entities are responsible for performing backups on a regular basis.	Control Objective 4: Availability	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
33	CUEC: User entities are responsible for monitoring backup failures.	Control Objective 4: Availability	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
34	CUEC: User entities are responsible for documenting business continuity and disaster recovery plans.	Control Objective 4: Availability	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.
35	CUEC: User entities are responsible for performing vulnerability scans and penetration tests on a periodic basis.	Control Objective 4: Availability	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
36	CUEC: User entities are responsible for installing antivirus on workstations and updating definitions regularly.	Control Objective 4: Availability	Yes	Information Security	Information Technology		The Information Security Program 2023 Policy references antivirus on workstations being set up and actively monitored along with Information Technology. The Information Technology Standards also mentions antivirus on workstations being set up and actively monitored along with Information Security.
37	CUEC: User entities are responsible for documenting backup and restore procedures.	Control Objective 5: Backups	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
38	CUEC: User entities are responsible for automatically backing up systems on a regular schedule.	Control Objective 5: Backups	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
39	CUEC: User entities are responsible for monitoring backups for failures.	Control Objective 5: Backups	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
40	CUEC: User entities are responsible for documenting business continuity and disaster recovery plans.	Control Objective 5: Backups	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.
41	CUEC: User entities are responsible for testing business continuity and disaster recovery plans on a periodic basis.	Control Objective 5: Backups	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.
42	CUEC: User entities are responsible for storing backups and/or data in an encrypted format.	Control Objective 5: Backups	No	N/A	N/A		All environments will reside with Manti; not applicable to Amalgamated Bank.
43	CUEC: User entities are responsible for taking ownership of the account once the account has been created.	Control Objective 6: Account Setup	Yes	Commercial Banking	Commercial Banking		Commercial Banking AE will take ownership of the account. Part of Commercial Banking's Operating Procedures.
44	CUEC: User entities are responsible for notifying Manti of any issues in a timely manner.	Control Objective 6: Account Setup	Yes	Commercial Banking	Commercial Banking		Commercial Banking AE will take ownership of the account. Part of Commercial Banking's Operating Procedures.











Fin Technologies, Inc. dba Mantl_2023 SOC 1 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:	CBJCHBCAABAA_M4wtFHGrYUBKMMI5hff9VleS9yexTMR

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


-  Document created by Brandon Singh (BrandonSingh@AmalgamatedBank.com)
2024-03-29 - 3:07:05 PM GMT
-  Document emailed to Edie Friedel (ediefriedel@amalgamatedbank.com) for signature
2024-03-29 - 3:08:42 PM GMT
-  Document emailed to Carol Ng (carolng@amalgamatedbank.com) for signature
2024-03-29 - 3:08:42 PM GMT
-  Document emailed to Sal Mannino (salmannino@amalgamatedbank.com) for signature
2024-03-29 - 3:08:42 PM GMT
-  Document emailed to Thomas Rivara (thomasrivara@amalgamatedbank.com) for signature
2024-03-29 - 3:08:42 PM GMT
-  Document emailed to Joseph Bae (joebae@amalgamatedbank.com) for signature
2024-03-29 - 3:08:42 PM GMT
-  Email viewed by Carol Ng (carolng@amalgamatedbank.com)
2024-03-29 - 3:09:51 PM GMT
-  Document e-signed by Carol Ng (carolng@amalgamatedbank.com)
Signature Date: 2024-03-29 - 3:10:11 PM GMT - Time Source: server
-  Email viewed by Edie Friedel (ediefriedel@amalgamatedbank.com)
2024-03-29 - 3:21:36 PM GMT
-  Document e-signed by Edie Friedel (ediefriedel@amalgamatedbank.com)
Signature Date: 2024-03-29 - 3:22:49 PM GMT - Time Source: server

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

2024-03-29 - 3:48:14 PM GMT

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


Signature Date: 2024-03-29 - 3:48:20 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 - 3:55:44 PM GMT

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


2024-03-29 - 3:55:44 PM GMT

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


2024-03-29 - 6:44:35 PM GMT

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


2024-03-29 - 9:33:04 PM GMT

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

Signature Date: 2024-03-29 - 9:33:20 PM GMT - Time Source: server

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

2024-04-04 - 1:57:07 AM GMT

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

Signature Date: 2024-04-04 - 1:57:39 AM GMT - Time Source: server

 Agreement completed.

2024-04-04 - 1:57:39 AM GMT