NOTICE: By accessing, downloading, using, viewing or receiving this document, which consists of the Service Organization Controls (SOC) Report, the following terms and conditions shall apply to you (the "Recipient"). Recipient may receive certain non-public information or materials relating to (i) Charles Schwab & Co., Inc.'s ("Schwab") products, services, intellectual property, and businesses, including the SOC 1 Report; and (ii) any information concerning Schwab's, its agents or licensors' financial or business plans or operations, such as operational techniques, internal controls, compliance policies, methods of operation, security procedures, and other confidential information and trade secrets **("Confidential Information").** Notwithstanding the foregoing, Confidential Information does not include information that: (a) is or becomes publicly available through no breach by the Recipient; (b) was previously known to Recipient prior to the date of disclosure, as evidenced by contemporaneous written records ; (c) was acquired from a third party without any breach of any obligation of confidentiality; (d) was independently developed by Recipient hereto without reference to Confidential Information of Schwab; or (e) is required to be disclosed pursuant to a subpoena or other similar order of any court or government agency, provided, however, Recipient shall promptly inform Schwab in writing and provide a copy thereof, and shall only disclose that Confidential Information necessary to comply with such subpoena or order.

Except as expressly permitted herein, Recipient will not use or disclose any Confidential Information of Schwab without Schwab's prior written consent, except disclosure to and subsequent uses by Schwab's employees or consultants on a need-to-know basis, provided that such employees or consultants have executed written agreements restricting use or disclosure of such Confidential Information that are at least as restrictive as Recipient's obligations hereunder. Subject to the foregoing nondisclosure and non-use obligations, Recipient agrees to use at least the same care and precaution in protecting such Confidential Information as Recipient uses to protect its own Confidential Information and trade secrets, and in no event less than reasonable care. Recipient acknowledges that due to the unique nature of Schwab's Confidential Information, Schwab may not have an adequate remedy in money or damages in the event of any unauthorized use or disclosure of its Confidential Information. In addition to any other remedies that may be available in law, in equity or otherwise, Schwab shall be entitled to seek injunctive relief to prevent such unauthorized use or disclosure. Recipient shall not remove or alter any proprietary markings (e.g., copyright and trademark notices) on Schwab's Confidential Information.

The foregoing confidentiality requirements and all matters arising under or relating hereto (whether in contract, statute, tort (such as negligence), or otherwise) shall be governed by, and construed in accordance with, the laws of the State of California (without regard to its conflicts of laws principles). In the event of a conflict between the confidentiality requirements set forth herein or as otherwise agreed to between Schwab and Recipient governing the subject matter herein, the terms more protective of Schwab shall govern.

Schwab Advisor Services

Charles Schwab Corporation's Advisor Services and Personal Choice Retirement Account Services

System and Organization Controls Report 1 (SOC 1)

For the period from October 1, 2023 to September 30, 2024

Schwab Advisor Services
9899 Schwab Way #100, Lone Tree, CO 80124
(720) 785 -8800

Dear Providers and Administrators,

At Schwab, we believe the best long-term growth strategy is one that puts clients first. Seeing our business "through clients' eyes" helps us earn our clients' trust as we strive daily to fulfill our purpose to champion every client's goals with passion and integrity, and act according to our values, which are:

Serve our clients in an ethical, empathetic, and proactive way.

Innovate constantly to improve the client experience.

Respect fellow employees and reinforce the power of teamwork.

Be good stewards of the resources entrusted to us--client assets, our brand, and stockholder value.

As part of this commitment, we have engaged Deloitte & Touche LLP to conduct an annual examination of controls related to the processing of brokerage transactions in Advisor Services. Our goal for this examination is to help us ensure that the controls in place are operating effectively so that we can continue to provide the highest-quality service to your clients and to be the most trusted leader in investment services.

Enclosed are the findings from the 2024 examination. We encourage you to read the accompanying report and discuss any questions or issues with your Schwab Advisor Services Representative. We hope you will find this report informative and a reflection of commitment to our values.

Thank you for allowing us the opportunity to serve you and your clients.

Cayla Culver

Cayla Culver
Managing Director
Schwab Advisor Services

SCHWAB
ADVISOR SERVICES

Section 1: Independent Service Auditor's Report

Deloitte & Touche LLP
JP Morgan Chase Tower
2200 Ross Avenue
Dallas, TX 75201-6778
USA
Tel: +1 214 840 7000
Fax: +1 214 840 7050
www.deloitte.com

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Board of Directors of
The Charles Schwab Corporation:

Scope

We have examined the description of the Advisor Services ("AS") and Personal Choice Retirement Account Services ("PCRA") system of Management of Charles Schwab & Co, Inc. (the "Service Organization" or "Schwab"), a subsidiary of The Charles Schwab Corporation, related to the processing of brokerage transactions throughout the period October 1, 2023 to September 30, 2024 included in Section 3. "Management of Schwab's Description of Its Advisor Services and Personal Choice Retirement Account Services System" (the "Description"), and the suitability of the design and operating effectiveness of controls included in the Description to achieve the related control objectives stated in the Description, based on the criteria identified in management of Schwab's assertion. The controls and control objectives included in the Description are those that management of Schwab believes are likely to be relevant to user entities' internal control over financial reporting and the Description does not include those aspects of the AS and PCRA system that are not likely to be relevant to user entities' internal control over financial reporting.

The information in Section 5, "Other Information Provided by Management of Schwab" is presented by management of Schwab to provide additional information and is not a part of management of Schwab's Description of its AS and PCRA system made available to user entities during the period October 1, 2023 to September 30, 2024. Information in Section 5 has not been subjected to the procedures applied in the examination of the Description of the AS and PCRA system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description of the AS and PCRA system and, accordingly, we express no opinion on it.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of Schwab's controls are suitably designed and operating effectively, along with related controls at Schwab. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 2, "Management of Schwab's Assertion," management of Schwab has provided an assertion about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. Management of Schwab is responsible for preparing the Description and its assertion, including the completeness, accuracy, and method of presentation of the Description and the assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination. Our examination was conducted in accordance with attestation standards

established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period October 1, 2023 to September 30, 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a Description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on the criteria in management's assertion.

- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the Description.

- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the Description were achieved.

- Evaluating the overall presentation of the Description, suitability of the control objectives stated therein, and suitability of the criteria specified by the Service Organization in its assertion.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4, "Management of Schwab's Description of Its Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results."

Opinion

In our opinion, in all material respects, based on the criteria described in management of Schwab's assertion:

a. The Description fairly presents the AS and PCRA system that was designed and implemented throughout the period October 1, 2023, to September 30, 2024.

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 October 1, 2023 to September 30, 2024, and user entities applied the complementary controls assumed in the design of Schwab's controls throughout the period October 1, 2023 to September 30, 2024.

c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved, throughout the period October 1, 2023 to September 30, 2024 if complementary user entity controls assumed in the design of Schwab's controls operated effectively throughout the period October 1, 2023 to September 30, 2024.

Restricted Use

This report, including the description of tests of controls and results in Section 4, is intended solely for the information and use of management of Schwab, user entities of Schwab's AS and PCRA system during some or all of the period October 1, 2023 to September 30, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Deloitte & Touche LLP

February 7, 2025

Section 2: Management of Schwab's Assertion

Management of Schwab's Assertion

For the period from October 1, 2023, through September 30, 2024

We have prepared the description of the Advisor Services ("AS") and Personal Choice Retirement Account Services ("PCRA") systems of Management of Charles Schwab & Co, Inc. ("Schwab"), a subsidiary of The Charles Schwab Corporation, related to the processing of brokerage transactions throughout the period October 1, 2023 to September 30, 2024, included in Section 3. "Management of Schwab's Description of Its Advisor Services and Personal Choice Retirement Account Services System" (the "Description"), for user entities of the system during some or all of the period October 1, 2023 to September 30, 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

The Description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Schwab's controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

1. The Description fairly presents the AS and PCRA system made available to user entities of the system during some or all of the period October 1, 2023 to September 30, 2024 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:

    a. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:

        i. The types of services provided including, as appropriate, the classes of transactions processed.

        ii. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

        iii. The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

        iv. How the system captures and addresses significant events and conditions other than transactions.

        v. The process used to prepare reports and other information provided for user entities.

        vi. Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

        vii. The specified control objectives and controls designed to achieve those objectives including, as

applicable, complementary user entity controls assumed in the design of the service organization's controls.

viii. Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b. Includes relevant details of changes to the service organization's system during the period covered by the Description.

c. Does not omit or distort information relevant to the service organization's system, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the AS and PCRA system that each individual user entity of the system and its user auditor may consider important in its own particular environment.

2. The controls related to the control objectives stated in the Description were suitably designed and operated effectively throughout the period October 1, 2023 to September 30, 2024 to achieve those control objectives if user entities applied the complementary controls assumed in the design of Schwab's controls throughout the period October 1, 2023 to September 30, 2024. The criteria we used in making this assertion were that:

   a. The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of Schwab.

   b. The controls identified in the Description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved.

   c. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section 3: Management of Schwab's Description of Its Advisor Services and Personal Choice Retirement Account Services System

Applicability of the Report

The Charles Schwab Corporation (the "Company"), headquartered in Westlake, Texas, is a nationwide financial services provider and parent company to Charles Schwab & Co., Inc. ("Schwab," the "Service Organization," or the "entity"), a fully wholly owned subsidiary that augments the Company's value proposition.

The Company and its subsidiaries are responsible for establishing internal control procedures to ensure that brokerage information sent to Schwab, either manually or electronically, is authorized and processed completely, accurately, and timely.

Schwab Advisor Services (AS) provides custodial, trading, and support services to more than 13,000 independent investment advisors (IAs or "user entities"). AS brokerage transactions are supported by the Operational Services organization within Schwab. Information technology (IT), as it relates to AS brokerage transactions, is supported by the IT organization within Schwab.

Corporate Brokerage Retirement Services (CBRS) provides brokerage services to retirement plans and health savings accounts through the Personal Choice Retirement Account (PCRA) and the Health Savings Brokerage Account (HSBA). PCRA and HSBA are supported by the CBRS organization in conjunction with Operational Services, and the IT organization within Schwab. Note that only Personal Choice Retirement Account (PCRA) is in scope for this report.

As a continuing service to clients, this report has been prepared to provide information on internal controls from October 1, 2023, to September 30, 2024, which may be relevant to the IAs using Schwab as custodian on behalf of their advised clients and users of brokerage services to retirement plans.

Scope and Objective of the Report

This Description is intended to provide sufficient information to IAs, users of personal choice retirement accounts and their independent auditors to understand Schwab's control environment and for their independent auditors to plan audits. This report has been prepared taking into consideration the guidance contained in the Attestation Standards of the American Institute of Certified Public Accountants (AICPA).

This description is intended to focus on features that may be relevant to internal controls for clients utilizing Schwab applicable to the brokerage and custody services for IAs as it relates to mutual funds, fixed income, equities, and options. It does not encompass all aspects of the services provided or procedures followed by the Company in servicing its client base.

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring Activities, Information and Communication, and Control Activities

Internal control is a process effected by an entity's board of directors, management, and other personnel and consists of five interrelated components:

1. **Control Environment**—The control environment sets the tone of an organization, influencing the control-consciousness of its people. It is the foundation for all components of internal control, providing discipline and structure.

2. **Risk Assessment**—The entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how risks should be managed.

3. **Monitoring Activities**—The entire process must be monitored, and modifications made as necessary. In this way, the systems react dynamically, changing as conditions warrant.

4. **Information and Communication**—Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control its operations.

5. **Control Activities**—Control policies and procedures must be established and executed to help ensure that the actions identified by management are necessary to address risks to achievement of the entity's control objectives.

1. Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure.

The control environment has a pervasive influence on the way business activities are structured, objectives are established, and risks are assessed. It also influences controls and monitoring procedures. An entity's history and managerial culture influences the control environment. Effectively controlled entities strive to have competent people, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive "tone at the top." These entities establish controls, which foster shared values and teamwork in pursuit of the service organization's objectives.

This is accomplished by establishing controls surrounding the processing of information and by developing policies, which promote adherence to the requirements of the control environment. The elements of the control environment include:

A. Organizational Structure
B. Assignment of Authority and Responsibility
C. Management's Philosophy and Operating Style
D. Participation of Those Charged with Governance
E. Human Resources Policies and Procedures
F. Communication of Integrity and Ethical Values

A. Organizational Structure

During the period covered by this report, the Head of Advisor Services oversees the AS business, operational, and risk environments. A senior management team assists the Head of Advisor Services in the daily management and control over certain functions. The AS organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility, appropriate lines of reporting, and functional alignment suited to the need, size, and nature of its activities.

- **Head of Advisor Services**— Responsible for Sales & Relationship Management, Retirement Business Services, Technology Solutions, Business Strategy, Custody and Trading Administration, Client Experience, Business Consulting, and Product Management.

AS brokerage transactions are supported by Operational Services. The Managing Director (MD) of Operational Services oversees the Operational Services business, operational, and risk environments. A senior management team assists the MD in the daily management and control over certain functions. The Operational Services organizational structure provides the framework within which its activities for achieving its objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility, appropriate lines of reporting, and functional alignment suited to need, size, and nature of its activities.

Operational Services senior management responsibilities are assigned as follows:

- **MD, Middle Office Services**—Responsible for Account Solutions, Asset Transfer Services, Customer Verification & Research Center, Document Control, Estate Processing, International Operations, Move Money Solutions, MOS Platform Support, and Retirement Processing.
- **MD, Business Process Transformation**—Responsible for Operations Business Process Transformation

- **MD, Custody and Asset Services**—Responsible for Client Reporting and Security Services Hotlines, Client Tax Reporting, Corporate Actions, Cost Basis Operations, Dividends, Purchase and Sales, Securities Operations, and Settlement Operations.
- **MD, Brokerage Product Services (BPS)**—Responsible for Alternative Investment Custody Services, Institutional Mutual Fund Trading, Managed and Advised Account Operations, Mutual Fund Clearing & Operations, and Payment Product Services.
- **MD, Trading**—Responsible for Trading Operations and Risk Management, Restricted Stock, Trading Platform Support, Reference and Market Data, Data Governance, Fixed Income Position Trading, Market Structure, Schwab Trading, Affiliate Trading, Regulatory Reporting, Margins Operations, Process Control, Technology & Information Control, Regulatory & Policy Control, Book & Records Control, Project and Initiatives, Automated Mailing Services, and Strategy.
- **MD, Corporate Brokerage Retirement Services (CBRS)** —Sales, Relationship Management, Product, Platform, Service, Operations and Participant contact center.

B. Assignment of Authority and Responsibility

The control environment is greatly influenced by the extent to which individuals recognize their accountability. This holds true from the staff level to the Chief Executive Officer, who has responsibility for activities within an entity, including internal controls. The extent of accountability includes the assignment of authority and responsibility for operating activities, and establishment of reporting relationships and authorization protocols. Policies describing the business practices, knowledge, and experience of key personnel and resources are communicated for carrying out duties.

C. Management's Philosophy and Operating Style

The purpose and values of Schwab focus on putting client needs first. Seeing our business "through clients' eyes" helps us earn our clients' trust as we strive daily to fulfill our purpose and act according to our values, which are:

- Serve our clients in an ethical, empathetic, and proactive way
- Innovate constantly to improve the client experience
- Respect fellow employees and reinforce the power of teamwork
- Will be good stewards of the resources entrusted to us—client assets, our brand, and stockholder value

Schwab management fosters employee engagement by encouraging employees to bring forth ideas and solutions. Schwab executives interact with managers and staff across all departments frequently. Recurring staff meetings are held to share company performance and information across the organization. Annual employee surveys monitor employee engagement, and the survey results are used to ensure Schwab's overall corporate philosophy and corporate purpose are reinforced.

D. Participation of Those Charged with Governance

The Board is responsible for holding senior management accountable for implementing the Corporate Board's approved risk tolerance; maintaining an effective risk management structure that appropriately identifies, measures, monitors, and controls major types of risk; and managing the Company's actions in a safe and sound manner. The Risk Committee assists the Corporate Board in fulfilling its responsibilities by setting the types and levels of risk the Company is willing to take and supporting the independence and stature of independent risk management. The Chief Risk Officer advises the Corporate Board and its committees on risk management activities consistent with the Company's risk appetite statements and strategic plan.

E. Human Resources Policies and Procedures

Schwab uses the Corporate Human Resources and Employee Benefits department to provide support for personnel recruitment, employee benefits, and employee-related activities. The hiring practices of Schwab are designed to ensure that new employees are qualified for their job responsibilities. The Talent Acquisition department and the hiring director and/or manager of the department requiring the position are involved in the sourcing and selection process. Hiring policies include minimum education and experience requirements, completion of background and credit investigation checks, and execution of confidentiality agreements.

Once hired, employees participate in an onboarding program that includes compliance and regulatory training, as well as access to organization-specific training and resources. Training of personnel is accomplished through supervised on-the-job training, professional seminars conducted by outside educators, professional designation course work, and internal courses developed by Schwab. Employees are encouraged to pursue appropriate further education and certifications by taking advantage of tuition reimbursement programs.

The department manager is responsible for ensuring that all personnel complete applicable training and encouraging training and development to continue to qualify personnel for their functional responsibilities.

F. Communication of Integrity and Ethical Values

Schwab is committed to the highest standards of ethical conduct and has policies designed to promote integrity and ethical values, called the *Code of Business Conduct and Ethics* (the "Code"), which applies to employees of Schwab and its subsidiaries and affiliates. The Code stresses ethical conduct in key areas:

- Ethical behavior and legal compliance
- Conflicts of interest
- Confidentiality of information
- Employment practices
- Business practices
- Compliance and reporting

Employees are responsible for reviewing and complying with the Code and Company policies. Employees are also required to promptly report violations of the Code. Reporting procedures are available on the Company's intranet site. Failure to follow the Code or report violations can result in disciplinary action up to and including termination of employment. Employees are required to complete Code training annually.

2. Risk Assessment

Risk Management Program

The Operational Risk Management (ORM) framework has been established to implement ORM's vision and oversee ORM within subsidiaries and business units, with the objective of maximizing value while remaining within risk appetite. This includes helping the Company meet its objectives through more informed decision making. The primary objective of the framework is to establish a repeatable operational risk life cycle that management at subsidiaries and business units can apply vertically and horizontally throughout the Company to identify, prevent, and mitigate operational risks. The following elements are included within the ORM framework:

- **Risk Governance**—Establish and maintain an approach for developing, supporting, and embedding operational risk strategy and accountability that cascade from the Board to all levels of the Company.

- **Risk Identification and Assessment**—Identify, assess, and categorize risk across the enterprise, including the consideration of internal and external changes on current risk exposures.

- **Risk Monitoring and Reporting**— Establish primary management activities that support the framework, including reporting, monitoring, and assurance activities, to provide insights into the strengths and weaknesses of the risk management program.

- **Risk Measurement**— Establish techniques and processes to measure, analyze, and consolidate operational risks.

- **Risk Mitigation and Control Optimization** — Establish techniques and processes for using risk and control information to improve effectiveness, including remediation oversight for any action plans.

3. Monitoring Activities

Internal Audit Program

The primary role of the Internal Audit Department (IAD) is to support Schwab (Company), the Boards of Directors (Boards), and management to protect the assets, reputation, and sustainability of the Company.

The IAD helps the Company to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. The IAD does not operate or manage any business function but acts as the third line in identifying, measuring, monitoring, and reporting the risks of the Company. The IAD provides the Boards and management with critical information about its independent assessment regarding the design, effectiveness, and sustainability of controls. The Boards and management are the final decision makers with respect to the appropriate action to be taken regarding the adequacy and effectiveness of governance, risk management, and control processes.

An annual risk assessment is conducted by the IAD to develop the Annual Internal Audit Plan (audit plan). The annual risk assessment includes confirming the completeness of the audit universe and assessing the inherent risk and the effectiveness of management's controls to determine the residual risk of each auditable entity in the audit universe. The results of the annual risk assessment and the proposed audit plan are presented to the Board Audit Committees for approval.

The audit universe, annual risk assessment, and annual audit plan are updated as needed throughout the audit plan year in response to internal audit results and key information obtained through various continuous monitoring activities including, but not limited to, business, industry, project, and regulatory monitoring. Issues identified by the IAD include management's action plan and timeline to effectively remediate the issue. Internal audit issues are validated by the IAD to confirm effective remediation, which is required for issue closure.

The IAD provides regular reporting to the Board Audit Committees that highlights key information including, but not limited to, emerging risks, audit plan progress, audit plan changes, volume and severity of issues raised by Internal Audit, management's internal audit issue remediation progress, and issue themes and trends.

Subservice Organizations

AS and PCRA do not have any subservice organizations relevant to the scope of this report.

The table below contains service providers for which AS's and PCRA's controls alone are sufficient to meet the needs of user entities' internal control over financial reporting (i.e., achievement of the control objectives in Section 4 is not dependent on the service provider's controls). Such service providers are classified as "vendors," and the scope of the report does not include controls and related control objectives of vendors.

Table 1—Vendor Services Provided

Vendor Services Provided
Various depositories, custodians, clearing corporations, and transfer agents (e.g., National Securities Clearing Corporation (NSCC))
Equity market venues (e.g., UBS Securities LLC)
Option market venues (e.g., NYSE Arca)
Pricing and/or Corporate Action Data Services (e.g., Thomson Reuters and Exchange Market Data)
Statement Fulfillment Services (Broadridge Customer Communications (BRCC))
Fraud Detection on outgoing wires (NICE Actimize)

4. Information and Communication

AS and PCRA executives frequently interact with managers and staff across all departments. Company performance, important initiative updates, and progress toward established goals are communicated in several ways, including monthly financial status reports to senior leadership, quarterly all-manager meetings, and recurring staff meetings.

Management maintains open communication to ensure that employees understand how their responsibilities relate to the work of others and how to escalate exceptions timely. Communication includes newly hired employee orientation and training and continuing education through periodic meetings that summarize significant events and changes, time-sensitive email messages, and information posted on internal websites.

Management communicates to employees via email, conference calls, meetings, and an internal website, the Schweb. Emails are widely used to keep employees apprised of training needs, corporate alerts and news, application change information, and vendor maintenance that may impact operations. Town halls and all-hands meetings are held to gather the broader groups together in order to keep all employees aware of overall business goals and educate them about the other affiliated businesses.

5. Control Activities

The control activities that assist in carrying out management's directives are described in Sections 3 and 4 of this report. The control objectives and related control activities are included in Section 4 and may not be stated in Section 3 to avoid repetition. However, they are, nevertheless, an integral part of the description of control for AS and PCRA.

Description of Internal Controls over AS and PCRA Brokerage Transactions

A. Client Accounts

New Accounts

Schwab accounts are opened electronically through Schwab's websites or manually in Client Central—see Applications section below for definition. New account applications may be completed on paper or by electronic methods and submitted by IAs via US mail or electronically for AS accounts or by individual users for PCRA accounts.

For AS accounts, the Operational Services Account Solutions team receives requests to open new accounts within the electronic workflow system daily. For PCRA accounts, a Client Service Manager receives requests for new accounts and verifies that the data is set up as per applications submitted by the clients from the Schwab Advisor Center. All records are maintained and archived electronically. All requests to open new accounts are fulfilled via MyQ—see Applications section below for definition—and Client Central. Client Central systematically blocks accounts from being opened until all regulatory required fields are complete.

All new account requests follow a review workflow, which allows for requests not auto approved by the system to be reviewed and approved within the electronic workflow system. An individual with a Financial Industry Regulatory Authority (FINRA) Series 9/10 license reviews all forms for completeness and accuracy, including ensuring documents are signed and dated by all authorized individuals. If any documentation or signature is missing, the account is restricted until the documentation is in good order. Once fulfilled, all jobs in the electronic workflow system are reviewed and approved.

Additionally, the Customer Verification and Research Center (CVRC) performs Patriot Act verification on new clients. If a client's identity cannot be ascertained, restrictions are placed on the client's account to prevent all transactions.

Account Maintenance

Account maintenance consists of adding features or making changes to existing accounts. Maintenance may include tasks such as changing name or address; adding margin, power of attorney, or other features; requesting duplicate paper statements; or requesting electronic statements. Maintenance requests submitted through any of Schwab's channels, as mentioned above, are also received within the workflow system.

Account maintenance requests received in the workflow are systematically time stamped, reviewed, and approved by service professionals. Once received, the AS and PCRA service professional analyze the digitized paperwork to ascertain that all required information (e.g., client signature) has been collected and data entry of client information can commence in Client Central.

Client Central systematically blocks maintenance tasks from being executed until all required documentation and fields are complete. Certain maintenance requests require principal review by a FINRA Series 9/10 licensed representative: for example, adding power of attorney, adding a joint account holder, and adding or removing margin.

B. Client Transactions

For client-requested transactions, restrictions are in place within Client Central and MyQ to ensure that the representative who set up and/or updated the transaction cannot also approve that transaction.

Wires

Incoming wires for Schwab's broker-dealer clients are received in Schwab's account at Citibank, N.A. The Move Money Solutions team receives a notification of incoming wires and allocates the funds to the appropriate client accounts. Incoming wires are reviewed for discrepancies; any inconsistencies are researched and resolved in order to post or return wired funds as applicable. Supervision by the Move Money Solutions team of the incoming wires process is designed to ascertain that incoming wires are authorized and processed completely, accurately, and timely, thus minimizing potential exposure.

For AS Outgoing wires, transfers may be submitted by end-clients or their IAs, depending on the authority on file for the account and the destination of the wire transfers. The Move Money Solutions team receives requests for outgoing wired funds within the electronic workflow system daily and fulfills requests for domestic outgoing wires via MyQ or Client Central. Outgoing wires are systemically reviewed in MyQ to detect risk and prevent fraud. All discrepancies found during processing in Client Central or MyQ are reviewed and resolved to ensure timely and accurate completion. Supervision by the Move Money Solutions team of the outgoing wires process is designed to ascertain that complete and accurate documentation is in place to identify any unusual or unauthorized activity.

For PCRA, the approving Corporate Brokerage Retirement Services (CBRS) representative reviews each transaction for authorizations and that the request was set up according to client instructions to ensure money movement requests are processed correctly. Check or wire distribution requests from third party are reviewed and signed off by Third-Party Administrator (TPA) to ensure the client signatures and instructions are authentic and that the authentication was consistent with established internal policies and procedures.

Approval limits are established in the workflow tools to ensure representatives are approving wires within their limits. A quarterly review is performed by Move Money Solutions management to ascertain that approval limits are authorized for outgoing wire transfers. If an approval limit is not consistent with expectations, the manager immediately has the approval limit updated within the system.

Transfers

The Asset Transfer Services team processes and monitors incoming and outgoing transfers of client assets between Schwab and other financial institutions. Supervision by the Asset Transfer Services team of the incoming and outgoing transfers process described below is designed to ascertain that transfers are processed completely, accurately, and timely and that rejected transfers are also addressed in a timely manner.

Incoming Automated Customer Account Transfer (ACAT) and Non-ACAT transfer requests—which may include Non-ACAT (Broker-Bank), deposit/withdrawal at custodian (DWAC—Broker-Transfer Agent), and Direct Registration System (DRS)—are manually reviewed by a representative for completeness and accuracy. Management reviews a monthly sample of incoming transfers to ascertain if they were authorized and processed completely, accurately, and timely. Management also ascertains if rejected transfers were addressed in a timely manner.

Outgoing ACAT transfers between Schwab and other ACAT participating financial institutions are processed through an automated transfer system. The system flags outgoing ACAT transfers that do not meet predetermined criteria such as registration, social security number, and whether there are open orders in the account. If flagged, a manual review is performed to ensure accuracy and resolve any open issues before the outgoing ACAT transfer is completed.

Outgoing non-ACAT transfer requests are manually reviewed by a representative for completeness and accuracy. Monthly, an Asset Transfer Services Manager reviews a sample of outgoing transfer reports to ascertain if outgoing transfers were processed in a complete, accurate, and timely manner. If exceptions are identified, corrective action is taken to resolve the issues.

C. Transaction Processing

Account Restrictions within Trading Systems

Client accounts at Schwab may be restricted temporarily or permanently from certain transactions or activities depending on the circumstances and the type of account. Restrictions may be placed on a client account for various reasons, including missing paperwork, transfer of assets, deceased account holder, or undeliverable US mail. To limit the acceptable transactions that can be processed or activities that can be performed, account-specific or client-specific restrictions are applied in Client Central that automatically block transactions and activities attempted from that account in Schwab's trading systems (Mainframe). For PCRA trades, Corporate Brokerage Retirement Services 9/10 professionals perform a review of client request to add or remove third parties trading authorities and to confirm processing was completed accurately.

Equity and Option Order Edit Checks

Equity and option orders are reviewed against predetermined credit and risk criteria and monitored by Trading Operations personnel to determine eligibility of processing. Annually, trade edit checks are tested by Trading Platform Strategy & Support personnel to ascertain that the configurations are operating completely and accurately. Testing results are reviewed and approved by management, and exceptions are monitored to resolution, as applicable.

Trade Adjustments

Post trade date trade adjustments may be required to correct inaccurate transmission or execution of the terms of an order, including price, number of shares, security, or account.

The AS Trade Support team handles the processing of post trade date trade adjustments when corrective action is required. Corrective action may take several forms, including market action, cancel or rebill of trades, or price

adjustments. Changes to account name or designation of the order resulting from client requests are reviewed for completeness and accuracy of processing by a FINRA Series 9/10 licensed representative. For an adjustment requiring post trade date trade movement, a supervisory review is performed by a FINRA Series 9/10 licensed representative for completeness and accuracy before the trade movement is processed.

Trade Settlement

With continuous net settlement (CNS), all transactions are netted by the NSCC in order to simplify the trade settlement process. The CNS balancing process reflects the balancing of positions and money balances between Schwab and NSCC on a settlement-date basis. A review and reconciliation is performed by various Operational Services teams to identify and assign breaks for resolution. On a daily basis, the manager ascertains if CNS breaks are resolved in a complete, accurate, and timely manner; determines the largest risk items; and assists with their resolution.

D. Dividends

Non-Mutual Fund Dividends

The Distributions team processes cash dividends, interest and principal payments, stock dividends, stock splits, and spin-offs for clients. The team monitors activity and resolves differences between Schwab's stock records and the corresponding records at Schwab's depositories using the Schwab distribution system (Mainframe), which automatically compares the two. The Schwab distribution system is used to pay out all stock and cash distributions.

On payable date, for payments that are not auto approved, an exception report is generated several times a day from a payment file received by the vendor, such as The Depository Trust & Clearing Corporation (DTCC), Citibank, or BNY Mellon. The Distributions team reviews and resolves exceptions and allocates to clients all cash and stock received that day. The manager performs a review of the exception reports at the end of each day to ascertain if all exceptions were resolved completely, accurately, and timely by the Distributions team.

Mutual Fund Dividends

The Mutual Fund Dividends team, a team in Brokerage Product Services (BPS), is responsible for the accurate and timely processing of mutual fund dividend and capital gains payments to Schwab clients. The team utilizes a variety of data sources to obtain payable date information for fund families on Schwab's platform and mirror fund payments on ex-dividend dates. The team balances daily and periodic activity for accurate payments, researches and resolves dividend payment breaks on a daily basis and reconciles payments with the fund families.

Schwab's clients can choose to have dividends and capital gains either reinvested or distributed as cash. Pay outs for Schwab clients who elect to receive cash distributions are processed by Schwab as dividend sell-off reconciliation transactions, with the fund families equal to the aggregate cash distribution amount. These correcting transactions are processed using the NSCC's Defined Contribution Clearance & Settlement service.

Mutual Fund Dividends Team Managers monitor the payment process throughout the day of the payable date to ascertain if all payable items are processed completely, accurately, and timely.

E. Corporate Actions I Reorganizations

Non-Mutual Fund Reorganizations

For voluntary reorganization offers, Schwab typically receives notifications from the depositories where securities are held, including DTCC, BNY Mellon, and Citibank. The Voluntary Reorganization Set-Up team obtains offering materials from various sources, including DTC reports and emails from agents. The team reviews and posts the information internally and sends client communications via email, US mail, or telephone summarizing the terms of the offers and the clients' choices. Management monitors designated folders daily to ascertain if complete and accurate information is on file for the setup process.

The Voluntary Reorganization team receives instructions from those clients via online communication channels, the US mail, or through IAs with delegated authority who decide to participate. The team is responsible for the timely and accurate processing of clients' instructions, which includes providing the instructions to depositories or transfer agent of the security involved in the reorganization. All participating client positions are segregated into a placeholder security to prevent inadvertent trading of the security position. Management monitors the process daily to ascertain if client instructions are ready for processing based on Schwab's cutoff (i.e., generally one day prior to reorganization expiration date).

For mandatory reorganizations, notices are generated by the depositories and pulled by Schwab. Operational Services updates the description and coding of the security master to prevent inadvertent trading of the security. Reorganization announcements are updated within the system for future use by representatives. There is no client pre-notification required since holders do not have a choice on whether or not to participate. Their shares are submitted for proceeds per the terms of the offer, and their accounts are adjusted accordingly. Based on the break report distributed daily by the Asset Reconciliation team, the respective Operational Services teams work to research and resolve corporate action breaks in a complete, accurate, and timely manner. Items aged over seven business days are moved into suspense and escalated until resolved.

Mutual Fund Reorganizations

The Mutual Fund Dividends team, a team in BPS, is responsible for the accurate and timely execution of fund-driven corporate actions for mutual funds on Schwab's platform. BPS receives notifications via email of upcoming mutual fund reorganizations and mirrors fund family activity in the Schwab Legacy system for clients who hold positions at Schwab.

BPS utilizes internal calendars and checklists to enable the accurate and timely execution of mandatory corporate action events. The calendars track important corporate action milestones and deadlines. Checklists are completed throughout the execution period of the event, beginning with notification of the event through execution on the system. Weekly, the manager inspects the reorganization calendars to ascertain if team updates are complete and accurate so that reorganization events occur timely.

Mutual fund corporate actions are executed via the Schwab Legacy system and approved by authorized representatives based on predesignated dollar thresholds. Based on the break report distributed daily by the Asset Reconciliation team, BPS teams work to research and resolve corporate action breaks in a complete, accurate, and timely manner. Items aged more than seven business days are moved into suspense and escalated until resolved.

F. Asset Reconciliation

Cash Reconciliation

The Cash Accounting team performs a daily reconciliation of cash activity between Schwab and multiple financial institutions to identify exceptions. This daily supervision is designed to ascertain if all variances that required research and resolution were identified and resolved in a complete, accurate, and timely manner. On a monthly basis, the Cash Accounting Senior Team Manager reviews each cash account reconciliation to ensure Schwab's books and records agree to the bank records, and any reconciling items are identified and resolved in a complete, accurate, and timely manner.

Asset Reconciliation

The Asset Reconciliation team performs a daily reconciliation of client and company positions in Schwab's stock record against the records of depositories, custodians, and mutual funds. All breaks are resolved or moved to suspense by the seventh business day. In addition, on a monthly basis an officer reviews and approves Internal Accounts reconciliation activity to ensure transactions are appropriate, accurate, and comply with FINRA Rule 4523.

- **NSCC**

On a daily basis, NSCC sends Schwab a transmission of the previous day's aggregated net settlement position file. A daily exception report is generated that identifies all security position differences between the Schwab stock record and NSCC, including breaks related to trading, corporate actions, and transfers. Breaks are reviewed and assigned to the various business units that are responsible for researching and resolving breaks on a daily basis. On a daily basis, the Asset Reconciliation Manager reviews one day's report for all open items and ascertains if exceptions are identified and resolved completely, accurately, and timely.

- **Depositories**

The DTCC maintains the physical custody of most securities held by Schwab's clients. Citibank is the depository for foreign securities, and BNY Mellon is the depository for government securities. Daily exception reports identify all security position differences between the Schwab stock record and the depositories, including breaks related to trading, corporate actions, and transfers. Based on a review of break list reports sent by the Asset Reconciliation team, the assigned business units are responsible for researching and resolving breaks on a daily basis. On a daily basis, the Asset Reconciliation Manager reviews the day's report for all open items and ascertains if exceptions are identified and resolved completely, accurately, and timely.

- **Mutual Fund Companies**

Mutual fund share reconciliations are performed daily by the Asset Reconciliation team to ensure that Schwab's books and records are in balance with the omnibus or subaccounts at the mutual fund companies. Schwab reconciles shares utilizing an internal system (currently Mutual Fund Reconciliation (MFR), previously Daily Stock Reconciliation (DSR)) and NSCC feeds to systematically compare activity and positions between Schwab records and mutual fund companies' records, identifying any discrepancies. Asset Reconciliation Management reviews various internal reports daily to ascertain if the team is monitoring the system for data completeness and accuracy. The Asset Reconciliation team distributes breaks to the various Mutual Fund Operations teams within BPS, including Mutual Fund Corporate Actions, Mutual Fund Transfer of Accounts, and Mutual Fund Trading, for research and resolution.

G. Security Master

Schwab maintains a central data repository known as the security master that is composed of two systems: Enterprise Security Master (ESM) and Legacy Security Master (ITEM). Schwab's security master stores reference and price data attributes related to financial instruments (i.e., fixed-income, equities, options, exchange-traded funds (ETFs), and mutual funds). Security master data is established and maintained primarily through automated feeds from external vendors supplemented with manual entry as necessary, and distributed to downstream consumers and platforms via files, APIs and publishing events.

Additions and Maintenance of Financial Instruments

Data attributes for Fixed Income, Exchange Traded Products and Mutual Funds are stored and managed in ESM. ESM utilizes systematic security completeness standards to prevent incomplete data from being published for downstream consumption. On a daily basis, management reviews exception reports to identify any CUSIP with incomplete or inaccurate data and ensures resolution in a timely manner.

For Mutual Funds, prior to April 24, 2020, manual additions and updates were monitored through daily quality assurance reviews by the Security Master Data Management team. Beginning April 24, 2020, the Security Master Data Management team, conducted a data validation review on mutual fund addition and changes received from the Mutual Fund Add and Support team as well as outside vendors, Management also reviews a series of daily exception reports to ascertain if manual updates are timely, complete, and accurate. Increased management oversight is performed for designated high-risk fields.

Pricing

For Fixed Income products, exchange traded securities and Mutual Funds, pricing is performed in ESM. Fixed Income and Exchange Traded Products are priced by various third-party vendor feeds, and if multiple data sources exist, a hierarchy is leveraged to achieve the most accurate price. Reviews are performed to monitor daily price changes on instruments outside of tolerance ranges to determine accuracy. On a daily basis, the manager reviews the Zero Priced Securities Report, Price Tolerance Report, Stale Priced Securities Report, and End of Day Price Checkout email to determine that changes in pricing have not exceeded tolerance levels, are accurate, and were processed accurately. Inaccuracies in pricing are corrected by using intraday pricing updates.

Mutual Funds securities are also priced in ESM. Daily Net Asset Values are received and processed electronically from industry or vendor feeds or via manual updates in ESM. On a daily basis, the Mutual Fund Trading team researches and resolves prior-day unpriced mutual fund symbols through the No Price Report. The report is reviewed by the manager daily to ascertain that all symbols have a current price, and any unpriced symbols are sent to the appropriate representative for resolution.

H. Account Statements

Typically, account statements are generated and delivered on a monthly basis. Clients who have provided their informed consent to receive electronic statements will receive an email directing clients to log into their Schwab account and view their account statement. Otherwise, clients receive paper copies of account statements in the US mail.

During the month-end statement production cycle, the Client Tax Reporting team reviews a sampling of statements to ascertain the accuracy of balances, positions, transactions, account registration information, as well as overall statement format. Once the review of samples from each statement platform is complete and any exceptions are researched and resolved, the vendor is instructed to proceed with the printing, processing, and delivery of statements.

For clients who receive paper copies of their account statements, the Automated Mailing Services team is responsible for ascertaining that the monthly statement files sent to the vendor are printed and mailed completely and timely. Evidence of this process is reviewed on the monthly Broker Dealer Drop Report, which includes vendor auto-generated reconciliation reports and vendor job status summary reports.

Description of Application Processing Systems

Processing Environment—Network and Infrastructure

Schwab utilizes both Mainframe and Distributed technology. The key system platforms are standardized on z/OS, UNIX, and Windows operating systems, and utilize Oracle, IBM DB2, and Microsoft SQL Server databases.

Applications

All applications are used at all locations unless otherwise noted. Major application processing systems used for AS brokerage transactions include the following:

System/Application	Description
Mainframe (Legacy) Systems	
Legacy refers to the group of applications that serve as Schwab's core broker-dealer platform. Legacy supports the execution, settlement, and reconciliation of brokerage transactions.	
BP&T	BP&T is used as the books and records for brokerage accounts. Its main functionality is real-time posting of brokerage accounting transactions to the customer ledger and

System/Application	Description
	calculation of customer balances.
Dividends Distribution	Dividends Distribution is used in the processing of dividends for domestic and foreign equities and mutual funds, as well as principal and interest payments on foreign and domestic fixed-income securities.
Integrated Cashiering	Integrated Cashiering is used for the controlled movement of funds and securities requested from various Client and Representative facing applications (e.g., Client Central, Schwab websites) for check processing, wires, fund transfers, and other various money movements.
ITEM	ITEM is the security master platform that stores reference and price data attributes for various asset classes, and it is the source of mutual fund securities data and pricing.
Stock Record	Stock Record is used in conjunction with other applications to maintain Schwab's brokerage books and records. The system also facilitates internal and external stock reconciliations between custodians (e.g., DTC, Citibank).
CRT	CRT (Client Reporting Technology) is used to identify Schwab client who has elected to participate in e- statement communications.
Distributed Systems	
Broadridge Portal [1]	The Broadridge Portal is a secure web-based application that provides a single-entry point into Broadridge Output Reports and applications. Schwab utilizes Broadridge as a print and mail vendor for account statement distribution, and the Portal is used to obtain production and postage reports, job status information, and validation, as well as part of the statement review.
Client Central	Client Central is a unified desktop platform used by Schwab front-line branches, call centers, and operations representatives to provide a one-call resolution in their daily interactions with clients.
Break Management (MFR/REM)	The Mutual Fund Reconciliation (MFR)/Reconciliation Exception Manager (REM) application is used to manage the reconciliation of the Mutual Fund Stock Record activity and settlement date positions against the mutual fund companies' activity and settlement date positions. The application automatically ages and suspends all unresolved breaks.
ESM	Enterprise Security Master (ESM) is a comprehensive, enterprise-wide Security Master reference data platform that serves as the system of record for the majority of security descriptive information (e.g., fixed-income, options, equities, and ETFs) and end-of-day pricing data.
MyQ	MyQ is a scanning, electronic workflow, and archival system used to store client documents, such as new account applications. This system is referred to as the "electronic workflow system" in this report.

[1] *This department, outside entity, service or system is not part of the scope of this report. Descriptions of policies, procedures and control objectives for this department, outside entity or system have been intentionally excluded from this report and any information provided is for information purposes only.*

System/Application	Description
Trade Reconciliation System (TRS-CASA)	The Trade Reconciliation System performs a Schwab versus DTCC settlement date, cash, and position reconciliation for equities and fixed-income securities.
OEMS	The Order Execution Management System (OEMS) manages and routes order flow for the Schwab broker-dealer. It is also referred to as XpressRouter.
Genesis	Genesis is a portal and backend service used by the Mutual Fund teams to on-board new funds and update current fund agreements.

Overview of the Schwab Information Technology (IT) Organization

Schwab IT is a customer-focused technology service provider that combines people, processes, and technologies to provide relevant business solutions and levels of service, while supporting the overall goals of Schwab. Schwab IT has demonstrated experience in developing, sustaining, and growing operational services for user entities. Furthermore, Schwab IT has developed the infrastructure and required managed services to operate complex network and system environments in support of its internal business units and external customers (the business unit's user entities).

Schwab IT's portfolio is composed of a range of solutions, such as data center, network, security, server (operating system), and application (e.g., Web services) services. Customers can choose from a variety of solutions depending on their technical requirements (i.e., reliability, performance, security, and support) and the cost associated with the selected services. This approach allows user entities to subscribe to solutions that reflect their business and technical requirements, while providing the flexibility of managing risk against cost.

The following are the services and capabilities that are available and provided to entities by the Schwab IT organization:

- **Access Management Services**—Manages the access privileges and entitlements for Schwab workers, ensuring the appropriate controls are provided to system/data owners.

- **Collaboration**—Supports a number of services designed to increase the collaborative effectiveness between Schwab employees and teams. These services include email, instant messaging, Microsoft SharePoint, and conferencing.[2]

- **Co-location**—Delivers facility services for systems installed within one of Schwab IT's enterprise data centers. Services provided include space, power, cooling, physical security, fire suppression, outbound network firewalls, environmental controls, and facility plan operations.[2]

- **Data Center**—Provides user entities with server hosting and administration services. These services include maintaining the computing environment to be compliant with relevant security, compliance, and audit standards.

- **Disaster Recovery**—The Operational Continuity team coordinates with various support teams to help ensure the preparedness and execution of disaster recovery plans for Schwab's systems.[2]

- **Personal Computing**—Provides Schwab user entities with general computing tools and life cycle management services for desktops and/or laptops, and workgroup printers. The Workplace Technology team also provides deskside support services.[2]

- **Service Desk**—Provides a contact point between users of Schwab IT services and the technicians that provide

[2] *This department, outside entity, service or system is not part of the scope of this report. Descriptions of policies, procedures and control objectives for this department, outside entity or system have been intentionally excluded from this report and any information provided is for information purposes only.*

problem resolution and service installation.[2]

- **Data Storage and Management Services**—Provides a comprehensive range of shared storage solutions, including storage area network (SAN), network attached storage, and data backup technologies.[2]

- **Distributed Services**—Provides complete, secure application hosting, connectivity, and technology management solutions to support business products, functions, enterprises, and domains. Services by the Distributed Services team include the ongoing administration and management for applications and solutions.

- **Internal Supporting Services**—Assists internal initiatives and groups with a number of services that include vendor management, technology planning, portfolio management, and incident and change management.[2]

- **Mobility**—Provides a number of services designed to allow Schwab employees to productively work outside of the traditional "in-office" environment. These services include cell phones, personal digital assistants, air cards, audioconferencing, and remote employee telephony.[2]

- **Network**—Provides network services, including local area network/wide area network (WAN) service offerings and corporate virtual private network (VPN), to Schwab employees.

- **Voice Communication Services**—Provides Schwab employees with the technology needed to make, receive, and route phone calls with colleagues, vendors, and user entities.[2]

- **Shared Print, Scan, Copy, and Fax**—Provides Schwab employees with shared solutions for print output and imaging.[2]

Description of General Information Technology Controls

A. Change Management

Schwab IT has developed formal standards and procedures over the change management process, which requires system software, hardware, database, and network changes to be approved, tested (if applicable), implemented, and documented.

Generally, change requests are initiated using Schwab's workflow ticket system where relevant change information is captured and an assignment is made to the applicable technical support group during submission. The ticket system assigns a unique tracking number and systematically designates the appropriate individual(s) to approve the change and sends a notification informing the approver of the change request. Once the ticket is routed to the change approver(s), it is evaluated to confirm the level of risk, impact, and priority associated with the change. Multiple change approvers may be required based on the defined risk level associated with a change request.

There can be several levels of change review and approval. The number of approvals required for each ticket is dependent on a number of factors which include the classification of the ticket, the risk level associated with the change, the change management credit score of the organization deploying the change, the overall Change Awareness Level (which can require elevated levels of leadership to approve normal, expedited and at times standard changes), and if the change is subject to any additional restrictions (including activities such as month end, etc.).

Any approver in the cycle has the authority to accept or reject a change. If rejected, the ticket system sends a notification to the requestor, who updates the ticket and works with the change approver to correct the reason for the rejection. If approved, the change request is carried out and completed and is certified by the appropriate IT, business, or quality assurance personnel to ensure that the change is operating as intended by the requestor.

---

[2] *This department, outside entity, service or system is not part of the scope of this report. Descriptions of policies, procedures and control objectives for this department, outside entity or system have been intentionally excluded from this report and any information provided is for information purposes only.*

Changes require testing based upon the change management standards and procedures. These standards allow for some changes to bypass testing, for example, in some instances where testing is not possible, time-critical break/fix-type changes, and low-impact routine infrastructure changes. Issues identified during testing are captured as needed in the area implementation owner's documentation and resolved by the change owner prior to implementing the change.

Standard changes are low risk and require approval from the change manager associated with the group accountable for deploying the change to production. Some examples of standard tickets include installing or repairing backup software agents, SAN volume expansions, and installing or modifying database monitors and agents. Standard changes are preapproved by the area owner/management personnel and the change management group. Testing for standard changes has been previously benchmarked and additional testing is not required for subsequent changes that occur. Changes are tested by individual(s) or group(s) depending on the type of change, and the results are captured within change documentation, or the ticket associated with the change, in accordance with change management standards, guidelines, and procedures.

Development, test, and production environments are logically and/or physically separated in compliance with Schwab standard. If the creation of a testing environment is not feasible (i.e., mainframe platforms), testing is performed in the development environment by restricting access to authorized testers only.

Management has established a Change Advisory Board (CAB), which reviews and approves new change requests with an associated risk level of 'high' (risk level 4 or 5). The CAB meets, when required, to discuss, approve, and schedule the implementation date for proposed changes. Proposed changes are tested prior to being presented to the CAB for approval. The CAB approval is documented within the change ticket.

In addition to the approvals derived from risk, credit score and restrictions, expedited changes require an approval from the Schwab IT Managing Director and the Managing Director of the affected business unit. Once the change has received all required approvals, it is scheduled for implementation.

Emergency changes can result due to various reasons, such as system outages, incident prevention, software problems, or hardware failures. Emergency changes are approved by the IT Operations organization prior to their implementation. If there is a an acutely time sensitive matter, IT Operations can provide verbal or written approval for a change to be implemented prior to a ticket being opened, however, a Latent ticket, including the documentation of approvals, testing, and other relevant information, is required within 24 hours (or the next business day) of the urgent change deployment.

A detailed implementation plan, including a back-out plan where applicable, is also documented within change tickets. Access to implement changes into databases and system software production environments is restricted only to personnel commensurate with their job responsibilities. Once the change has been successfully implemented, the ticket is closed by the requestor or a technical team member.

In certain instances, developers are allowed access to production environments. To mitigate risks associated with this access, the Detected Change Reconciliation Process (DCRP) was established to monitor for unauthorized changes to critical applications and infrastructure. Undocumented changes are tracked and correlated daily basis utilizing industry standard tools, internal Schwab data sources, and rules-based analytics. Upon detection, the application owner and manager are notified that a potential infraction has occurred. The notification requests that the application owner provide one of the following items to demonstrate the change activity was authorized:

- Change Record
- Incident Record

The application owner must respond with the necessary supporting information. Delayed responses are escalated to the DCRP owner for follow up and resolution.

For MyQ and CASA applications, the PEGA platform team performs a monthly review of changes implemented into the production environments.

For mainframe systems, segregation of duties is logically enforced by the ChangeMan tool by requiring approval and/or prevents self-approval of any change before it is released into the production environment.

System Patch Management

Notification of new vendor patches, service packs, bug fixes, or security alerts is received by the Schwab IT organization through various channels. A majority of the Schwab IT technical teams subscribe to major vendors who regularly notify the applicable teams of new system updates or security related information. Additionally, regular monitoring of vendor websites is performed by the Schwab IT technical team members to determine the availability of new system updates, threats, and/or vulnerabilities. The Schwab Cybersecurity Services (SCS) – Security Operations Center (SOC) also distributes periodic emails to the various technical teams of security-related threats and vulnerabilities that may potentially affect the Schwab IT infrastructure or environment.

If a system update is deemed necessary, the affected team follows the established Schwab IT change management process described above, which requires a documented approval and testing within the workflow ticketing system.

B. Logical Access

Schwab's Identity and Access Management (IAM) group has developed formal policies and procedures specific to logical security to ensure access to sensitive system resources and data are properly restricted and monitored. Access and authentication control technologies, such as unique user IDs, two-factor authentication, access profiles, and passwords logically restricted access to hosts, data, and information of user entities' systems and data. Multiple layers of authentication are required to access user entities' systems outside of the Schwab IT environment. The first level of authentication requires a user ID and token password to access the Schwab VPN. The second level of access requires a user ID and password to authenticate to the Schwab internal network. The third layer of access requires a user ID and password to authenticate to a server.

Provisioning of General and Privileged Access

Applications (Distributed and Mainframe), System Software, and Network

New and modified user access requests require approvals. In cases involving higher risk access provisioning, the approval workflow must include two levels of approval. Once approvals are captured the request follows the workflow defined by an appropriate subject matter expert to provision the requested resource.

User access requests submitted electronically using an Oracle tool (MyAccess) generate a Request ID and have an automated approval process. After the approval process completes, access is automatically provisioned in "MyAccess Managed" systems. Systems designated "IAM Managed" generate a Workorder number for provisioning by a centralized Identity and Access Management (IAM) Operations team.

Databases (Oracle, DB2, and SQL)

Database access requests that do not follow the "MyAccess Managed" process are fulfilled through the submission of a ticket to the Distributed Database Services (DDS) team. Once approved, the DDS team will follow the standard change management process to fulfill the request.

Termination of Full Time Employees, Contractors, and Professional Services

Applications (Distributed and Mainframe), Systems Software, and Network

Access is revoked for terminated users (Full Time Employees, Contractors, and Professional Services) when the user's manager submits a Termination task in Workday, including submission of the person's Last Day of Work. Workday feeds the worker termination records, including Last Day of Work, to MyAccess via an automated connector. An Incremental reconciliation job runs every 15 minutes, and a full reconciliation job runs for every 12 hours at 8AM and

8PM daily. MyAccess runs a scheduled job nightly which identifies workers with enabled network access and current termination date and disables such network access.

In a separate series of steps, access to applications is deprovisioned based on integration type:

- "MyAccess Managed"– Access is deprovisioned automatically in MyAccess.
- "IAM Managed" MyAccess automatically creates a work order when the removal request is submitted as described above, and IAM Operations completes the deprovisioning.
- Non-centralized application teams obtain semi-automated termination reports, and then revoke user access.

Databases (Oracle, DB2, and SQL)

1. Automation is in place that receives and processes HR personnel data daily to identify database accounts associated with terminated personnel. Identified accounts are then disabled, and later deleted.

Periodic User Access Review

Applications (Distributed and Mainframe), System Software, and Network

Access rights associated with system users are reviewed for appropriateness on a periodic basis. The review process is described in detail below.

- Certifying user access at least annually by user manager for database and network roles and entitlements which are not identified as Enterprise Roles.
- Certifying user access at least semi-annually by Role Owner and or User Manager for higher risk and privileged network layer roles which are not identified as Enterprise Roles.

For MyAccess Managed and IAM Managed systems, once the user access review has been completed, any required changes are formally documented and reflected within the Identity Management attestation tool by the appropriate reviewer. Users who no longer require access are revoked. Non-centralized application and database teams document certification completion, remove revoked access, and store evidence in their identified evidence repositories.

Password Settings

Access and administration of logical security for systems have been established by SCS and rely upon user IDs and passwords to authenticate Workforce members (both local and remote full-time employees and contractors).

When possible, security controls built into the systems, such as specified characteristics and expiration, are used to enforce the appropriate password standards. In other cases, Schwab IT employees are responsible for implementing the appropriate standards on passwords for which they have responsibility.

Password requirements within the Schwab technology standard for normal user accounts are as follows:

- Passwords must be a minimum of eight characters in length.
- The password must contain at least three out of four of the following categories:
    - Uppercase characters
    - Lowercase characters
    - Number
    - Non-alphanumeric characters
- Passwords must be changed at least every 365 days to new and unique password. Human network access account

passwords are changed at least every 90 days.

- After five consecutive incorrect password attempts, the system will lock out the user's account.

- Workforce members on the network must not be able to construct Windows Active Directory passwords that are identical to the 24 previous passwords used. Selections for new passwords are automatically checked against the history and rejected if there is a match.

- Other systems for Workforce member authentication may be implemented and combined. For example, biometric readers, one-time tokens, and cryptographic authentication certificates approved by Technology Risk Management (TRM) may be used.

Client access to the online website is restricted via a user ID and password. Passwords require various security parameters (e.g., minimum length, lockout on invalid attempts, complexity, etc.) as per Schwab's technology standard. Once a user has authenticated to the online website, they will have the ability to access their personal and financial information. If the user ID and password are not valid, a denial screen is presented requiring the user to go through the password reset protocol.

C. Network Security

Schwab has a defense-in-depth network architecture to secure its information assets as it allows an efficient way to achieve information assurance and risk management in highly networked environments. This architecture relies on the intelligent application of existing techniques and technologies, and seeks a balance between the protection capability, cost, performance, and operational considerations. Schwab utilizes this architecture in conjunction with risk management to create and maintain security policies, standards, procedures, and guidelines.

D. Physical Access

Charles Schwab primarily uses a photo ID badge system (controlled access system) to protect its facilities, with biometric and multi-factor access authentication measures for non-exceptional access into the data centers. All door locks are proprietary high security locks and maintained in-house. In addition, security officers are stationed in lobby areas and monitoring room 24x7. Security officers are contracted from a security services vendor. Video systems (digital video systems) are utilized in the data centers and surrounding property, as well as exterior presence and perimeter detection complimented with random patrols using closed-circuit television (CCTV) and personnel.

Physical access to the Data Center is restricted to staff with a business requirement for this access. Access is controlled, monitored, and logged through an automated electronic badge management system used throughout the firm and administered by Corporate Security. Access requests are standardized through forms available on the Company intranet and require dedicated authorizer approval prior to being processed. Semi-annually, a list of users with badge access to the data centers is sent to dedicated authorizers for their review to ensure the access remains appropriate. Each authorizer is responsible for certifying the appropriateness of user's access and returning the certified report to action on any inappropriate access rights.

E. Backup and Disaster Recovery

Schwab Data Centers are located in Central Arizona with the primary in Phoenix with a backup facility located in Chandler. All Schwab Data Center infrastructure components are redundant and are supported by an Uninterrupted Power Source. Production Servers and Data Stores are backed up utilizing a Commvault backup system that creates a copy of data onsite and transmits the backups to an alternate, secure, Schwab data enter location. The data centers and their supporting infrastructure are monitored and maintained by authorized staff and all changes require fully approved and scheduled change tickets.

Backups are performed automatically as per the configured client schedules in the Commvault backup system.

Data backup is monitored using the inbuilt monitoring functionality of Commvault. A report that captures the status of the backup is generated daily. A subsequent issue ticket is created in Schwab's Incident Management System. A

Backup and Recovery team is responsible for identifying the root cause and resolving the issue.

F. Application and System Processing

Schwab's Enterprise Batch Services (EBS) team uses a dynamic workload scheduler to run and monitor the status of all scheduled batch jobs. EBS personnel continually monitor the functioning and completion of all jobs, including a display of all failed jobs, and follow up on exceptions for research and resolution. For any job that cannot be restarted by EBS personnel, the party responsible for the associated job is contacted for resolution.

Complementary User Entity Controls

Processing of transactions for accounts serviced by AS and the controls at AS cover only a portion of the overall internal controls. It is not feasible for the control objectives related to the processing of transactions to be solely achieved by AS; therefore, internal controls must be evaluated in conjunction with AS controls, and testing is summarized in the following section of this report.

This section highlights those internal control responsibilities that AS believes should be present for each IA and have been considered in designing the controls described in this report. In order for IAs to rely on the controls reported herein, each IA should evaluate its own internal control environment to determine if the following controls are in place.

Furthermore, the following list of controls is intended to address only those controls affecting the interface and communication between each user organization and AS. Accordingly, this list does not purport to be, and is not, a complete listing of the controls and responsibilities that are appropriate to provide a basis for the assertions underlying the financial statements of AS clients.

Complementary User Entity Control Considerations	Related Control Objective(s)
New Accounts, Changes to Accounts, Client Transactions, and Trades	
User entities are responsible for ensuring that Schwab is provided with complete and accurate contact information for Schwab change authorization, emergency notification, and problem escalation.	1, 2, 3, and 5
User entities are responsible for aspects of their clients' accounts, including, but not limited to, Know Your Customer rules, suitability, and compliance with all client documentation requirements.	1, 2, and 3
User entities' advisors or registered representatives are responsible for reviewing the applicable documentation of each client's account and verifying that the persons who provided the respective authorizations to act on such client's behalf were properly authorized.	1, 2, and 3
User entities are responsible for reviewing modifications to critical information in their clients' accounts to determine the accuracy and completeness of client account changes.	1, 2, 3, 4, and 8

Complementary User Entity Control Considerations	Related Control Objective(s)
User entities are responsible for performing the appropriate reviews using the following activities and reports to determine that requests were processed completely and accurately: • Daily review and follow-up of transaction anomalies • Review and correction of any rejected items • Timely review of alerts posted to Schwab Advisor Center (SAC) • Timely review of SAC Service Request status	2 and 3
User entities are responsible for determining whether check, wire, Automated Clearing House (ACH), and journal and Electronic Funds Transfer (EFT) disbursement instructions are valid and authorized and should submit accurate and complete instructions timely for processing, including supporting documentation.	2
User entities are responsible for submitting properly authorized instructions, including, but not limited to, trade instructions, disbursement requests, asset movements, and change of address instructions.	2, 3, and 8
User entities are responsible for ensuring that erroneous or incomplete instructions are reviewed, corrected, and resubmitted in a timely manner.	2, 3, and 8
User entities are responsible for reviewing the accuracy and completeness of trade orders, including, but not limited to, aggregating orders of multiple client accounts. User entities bear the cost of trade corrections for orders they submit incorrectly.	3
User entities are responsible for submitting timely cancellations and correct trade instructions.	3
Corporate Actions	
User entities should review the Schwab systems daily to identify voluntary reorganizations and should review information sent, whether through electronic channels or alerts, or manual delivery of reorganization actions and provide Schwab with timely responses and feedback on errors.	5
Securities	
User entities should establish procedures to review their valuations of all securities, including securities automatically priced via a pricing vendor and securities manually priced, in the context of current trade information, market data, and other relevant matters, such as significant events when evaluating their portfolios for financial statement purposes.	7 and 8
Account Statements and Client Reports	
User entities are responsible for timely review of notifications, client statements, and confirmations.	8

Complementary User Entity Control Considerations	Related Control Objective(s)
Logical and Physical Access	
User entities are responsible for ensuring that access to Schwab systems is authorized, documented, periodically reviewed, and commensurate with job responsibilities. Additionally, modifications to user access, such as new hires, transfers, terminations, or changes to user profiles, are to be communicated to Schwab in a timely manner, if applicable.	9 and 11
User entities are responsible for periodically reviewing their employees' physical and logical access to Schwab systems.	9 and 11

Changes to the System Description from the Prior Period

There were no changes affecting the AS & PCRA system description from the prior period.

Control Objectives and Related Controls Provided by Schwab

Control objectives and related controls provided by Schwab are included in Section 4, "Management of Schwab's Description of Its Control Objectives and Related controls and Independent Service Auditor's Description of Tests of Control and Results. Although the control objectives and related controls are included in Section 4 and may not be included in Section 3, they are, nevertheless, an integral part of the description of controls of Schwab.

Section 4: Management of Schwab's Description of Its Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results

Description of Testing Procedures Performed

Deloitte & Touche LLP performed a variety of tests relating to the controls listed in this section throughout the period from October 1, 2023 through September 30, 2024. Our tests of controls were performed on controls as they existed during the period of October 1, 2023 through September 30, 2024 and were applied to those controls specified by Schwab.

In determining the nature, timing, and extent of tests, we considered (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the assessed level of control risk, (d) the expected effectiveness of the test, and (e) our understanding of the control environment.

In addition to the tests listed below, we ascertained through multiple inquiries with management and the control owners that each control activity listed below operated as described throughout the period. Tests performed are described below:

Test	Description
Corroborative Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control during the report period to evidence application of the specific control activity.
Examination of Documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of Monitoring Activities or Manual Controls	Obtained documents used in the monitoring activity or manual control activity, independently reperformed the procedures, and compared any discrepancies identified with those identified by the responsible control owner.
Reperformance of Programmed Processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Testing of tools supporting control activities

For the tools used in the performance of control activities in Section 4, we performed procedures to address the risks associated with their use. While these procedures were not specifically included in the test procedures listed in Section 4, they were completed as part of the testing to support our conclusions.

Reliability of Information Produced by the Service Organization

We performed procedures to evaluate whether the information provided by the service organization, which includes (a) information in response to ad hoc requests from the service auditor (e.g., population lists), and (b) information used in the execution of a control (e.g., exception reports or transaction reconciliations), was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Our procedures to evaluate whether this information was sufficiently reliable included procedures to address (a) the accuracy and completeness of source data, and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently

precise and detailed for purposes of fully testing the controls identified by the Service Organization.

Use of the work of others

Members of Schwab's internal SOX Compliance Office (SCO) function performed tests of operating effectiveness of controls for a portion of the control activities. We evaluated the competence and objectivity of the individuals within the internal audit function performing such tests.

Where the work of internal audit was utilized, we evaluated the adequacy of such work. We reperformed the testing of selected control activities that had been tested by the members of the internal audit function and noted our conclusion was consistent with that of the internal audit testing.

Reporting on the Results of Testing

The concept of materiality is not applied when reporting the results of control tests because Deloitte & Touche LLP does not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, Deloitte & Touche LLP reports all exceptions.

#1	Controls provide reasonable assurance that new accounts and changes to existing accounts are authorized and established in accordance with client instructions and industry guidelines in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
1A	Customer Account Technology performs systematic reviews for completeness and accuracy on accounts opened. Rules are applied against the data entered to determine if the account can be auto-approved. If the account cannot be auto-approved, the account moves into a manual Series 9/10 queue for review by a Series 9/10, 24, 24/4 licensed representative.	**Observation**— Observed the auto review logic workflow within CAT production environment and ascertained that the rules were applied against the data entered and determined whether the account can be auto-approved or not. Negative Test: Observed a sample of accounts that violated the pre-defined rules in the CAT production environment and ascertained that the accounts did not pass the auto review. Further, ascertained that the account application was subsequently moved to the 9/10 manual review queue and resolved by a series 9/10, 24, 24/4 licensed representative. Positive Test: Observed a sample of account that passed all the pre-defined rules in the CAT production environment and ascertained that the account passed the auto review. Further, ascertained that account application details were complete and accurate, and was processed through auto-approval.	No exceptions noted.
1B	Account information is reviewed prior to account opening for completeness and accuracy. Accounts opened without all required documents or lacking authorizing signatures are restricted. A Series 9/10 or Series 24 licensed representative performs a review of new accounts in the manual queue that were not processed automatically by the system.	**Inspection**—For a sample of client applications that required manual review during the examination period, inspected the new account requests and ascertained that they were reviewed and approved within Client Central and electronic workflow systems by Series 9/10 or Series 24 representative prior to the opening of the accounts. Ascertained that account applications without required documentation were followed up on or rejected. Inspected the Series 9/10 verification and ascertained that the reviewer confirmed all account information was complete and accurate, including appropriate name, address, account type detail, etc.	No exceptions noted.

#1	Controls provide reasonable assurance that new accounts and changes to existing accounts are authorized and established in accordance with client instructions and industry guidelines in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
1C	The Customer Verification & Research Center (CVRC) systematically reviews client identities by comparing new account information to existing public records (e.g. client name, address, SSN) to ascertain that the client's information is complete and accurate. If information can't be confirmed, restrictions are placed on the account until authorization can be completed.	**Observation**—Observed a sample account that had complete and accurate information (considered 'low-risk') and ascertained that the account was authorized according to systematic rules. Additionally, observed a sample of accounts that had variations of incomplete and inaccurate information (considered 'high-risk') and ascertained that they were flagged and queued for review and restrictions were put in place according to systematic rules.	No exceptions noted.
1D	Daily, account maintenance requests are systematically routed for Series 9/10 review (e.g., adding account holders, power of attorney) and are inspected by a Series 9/10 or 24 representative to ascertain that account maintenance requests are complete and accurate. Any exceptions are researched and resolved.	**Inspection**—For a sample of account maintenance requests, inspected the request and ascertained that it was reviewed and approved by a Series 9/10 or 24 licensed representative and the review was complete and accurate. **Observation**—For a sample of one account maintenance request, observed the request workflow and ascertained that it was systematically routed for Series 9/10 review as expected.	No exceptions noted.
1E	Series 9/10 , Series 24 or Series 4 licensed Representative reviews all new PCRA account applications and applicable account update jobs within 3 Business Days for required information and signatures.	**Inspection**—For a sample of new account or account update jobs during the examination period, inspected the new account and account update request and ascertained that it was reviewed and approved within MyQ by Series 9/10, Series 24 or Series 4 representative within 3 business days of the application or request being submitted.	No exceptions noted.

#2	Controls provide reasonable assurance that client transactions (i.e., wires and transfers) are authorized and processed in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
2A	Systematic blocks and controls in Client Central (CC) system exist pertaining to system access, appropriate approval levels, and type of requests. Systematic blocks restrict access to authorized individuals and require approval by a second party depending on transaction type and size.	**Observation**—For a sample of users during the examination period, observed a positive and negative test and ascertained that transactions cannot be initiated, updated, or approved by the same users. In addition, for a sample of users, ascertained that the user has an appropriate level of authority to perform the corresponding approval.	No exceptions noted.
2B	MyQ systematically prevents individuals from initiating or updating and approving the same transaction.	**Observation**—Observed a positive and negative test and ascertained that transactions cannot be initiated, updated, or approved by the same individual. **Observation**—Inspected the MyQ configurations and ascertained the system is configured to prevent individuals from initiating or updating and approving the same transaction.	No exceptions noted.
2C	Outgoing Wires are systematically reviewed against configured STP rules to detect risk and potential fraud. If no STP rules are triggered, the outgoing wire will automatically be posted. Outgoing wires which do not pass STP rules are researched and resolved by the Banking Operations Team in a timely manner.	**Observation**—Performed a positive test and observed a Banking Operations representative entered an outgoing wire which did not trigger any STP rules within MyQ. D&T ascertained that the outgoing wire was automatically processed and posted. **Observation**—For a sample of STP rules, performed negative tests and observed the Banking Operations representative entered wires that triggered the sampled STP rules within MyQ and ascertained that the outgoing wires were not processed. Ascertained that the STP rules were configured appropriately. **Inspection**—For a sample of outgoing wires, inspected the MyQ ticketing tool and ascertained the Banking Operations Team researched and resolved the triggered STP rules prior to processing the outgoing wires in a timely manner. **Inspection**—For a sample of outgoing wires, inspected that the ERE tool reviews outgoing wires against 2 variants, "Allowed" and "Delayed." D&T ascertained delayed wires were reviewed and resolved by the Banking Operations Team. Also ascertained that allowed wires were not reviewed by an individual as no intervention was required.	No exceptions noted.
2D	The Banking Operations team reviews incoming wired funds to customer accounts or returns to the counter bank within 7 business days. The Banking Operations team researches and resolves discrepancies, if applicable.	**Inspection**—For a sample of incoming wires within the examination period, inspected the Client Central screenshots with the processing details and ascertained that the Banking Operations team reviewed and processed the wires completely, accurately, and timely, and that discrepancies, if identified, were researched and resolved.	No exceptions noted.

#2	Controls provide reasonable assurance that client transactions (i.e., wires and transfers) are authorized and processed in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
2E	Wire approval limits are configured within the workflow tools to restrict representatives from approving a wire transaction above their configured limit.	**Observation**—Observed an MMS representative attempt to process wires above (negative test) and below (positive test) their listed approval to ascertain that approval limits were appropriately configured in the workflow tool.	No exceptions noted.
2F	Monthly, an Asset Transfer Services Manager or Team Lead reviews a sample of incoming transfer requests (ACAT, Non-ACAT, DWAC, and Direct from Fund) to ascertain if ATS representatives processed incoming transfers in a complete, accurate, and timely manner. If exceptions are identified, corrective action is taken to resolve the issue or prevent the issue from reoccurring, as applicable.	**Inspection**—For a sample of incoming transfers, inspected evidence of review by the Asset Transfer Services Manager of incoming transfers, and ascertained that the representative had reviewed the transfers for completeness and accuracy. Ascertained that all exceptions were monitored and followed through to resolution.	No exceptions noted.
2G	ACAT transfers of assets (between Schwab and other ACAT participating financial institutions) that are flagged by the system for manual review are reviewed by an Asset Transfer Services representative for accuracy and to identify and resolve any open issues before the transfer request is complete.	**Observation**—Observed the ACAT configuration and ascertained the system is configured to flag outgoing ACAT transfers for review. **Observation**—Observed a transfer that passed the system checks and was not flagged for review. Observed a transfer that did not pass the system checks and was flagged for review and ascertained the system is configured to flag transfers for manual review. **Inspection**—For a sample of flagged ACAT transfers during the examination period, ascertained that all flagged transfers were reviewed and processed timely. Any discrepancies if identified were researched and resolved.	No exceptions noted.
2H	Monthly, an Asset Transfer Services Manager or Team Lead reviews a sample of outgoing transfer requests to ascertain ATS representatives processed outgoing transfers in a complete, accurate, and timely manner. If exceptions are identified, corrective action is taken to resolve the issue from reoccurring, as applicable.	**Inspection**—For a sample of outgoing transfers, inspected evidence of review by the Asset Transfer Services Manager of outgoing transfers, and ascertained that the representative had reviewed the transfers for completeness and accuracy in a timely manner. **Reperformance**—For a sample of outgoing transfers, reperformed the review process, including tracing each transfer to supporting documentation, as well as any additional supporting documentation, as needed. For any exceptions identified, ascertained that the Asset Transfer Services Manager also identified the exceptions and took corrective action to resolve the issues or prevent the issues from reoccurring, as applicable.	No exceptions noted.

#2	Controls provide reasonable assurance that client transactions (i.e., wires and transfers) are authorized and processed in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
2I	Wire approval limits are attested periodically by the representative's authorized manager.	**Inspection**—For a sample of quarters and semi-annual periods during the examination period, inspected MyQ and Client Central wire approval limits and ascertained that wire approval authorization limits were reviewed by an appropriate manager.	No exceptions noted.
2J	Outgoing Wires are processed completely, accurately, and timely by an authorized Banking Operations representative. Discrepancies identified during processing are researched and resolved.	**Inspection**— For a sample of outgoing wires, inspected the processing history log and ascertained that an authorized Banking Operations representative processed the outgoing wire completely, accurately, and timely. Further ascertained that, any discrepancies identified were research and resolved.	No exceptions noted.
2K	Daily, the approving Personal Choice Investment Services representative reviews each transaction for authorizations and that the request was set up according to client instructions to ensure money movement requests are processed correctly. Check or wire distribution requests from third party are reviewed and signed off by Third-Party Administrator (TPA) to ensure the client signatures and instructions are authentic and that the authentication was consistent with established internal policies and procedures.	**Inspection**—For a sample of money movement transactions, inspected the request forms and the Client Central transactions screenshots, and ascertained that the request was authorized and was processed accurately per the request. Further, obtained the Client Central Authorized Agent list for the selected accounts and ascertained that the request form is signed by the authorized Third-Party Administrator (TPA).	No exceptions noted.
2L	Transaction approval limits are configured within the workflow tool to restrict representatives from approving transaction above their configured limit.	**Inspection**—Observed a sample of representatives attempt to process wire above (negative test) and below (positive test) their listed approval to ascertain that approval limits were appropriately configured in the workflow tool.	No exceptions noted.

#3	Controls provide reasonable assurance that trades are authorized and processed in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
3A	Account restrictions are configured in Client Central to ensure trades cannot be placed prior to the account restrictions being cleared.	**Observation**—For a sample of account restrictions during the examination period, performed positive and negative tests and ascertained that the account restrictions operated as designed to prevent trading on accounts with restrictions and allow trading on accounts without restrictions.	No exceptions noted.
3B	Systemically, client-placed equity and option orders are reviewed against predetermined credit and risk criteria and are monitored continuously by Trading Operations personnel to determine eligibility of processing. Exceptions are monitored to resolution, as applicable.	**Observation**—Observed trades in the system for equity orders and ascertained that the orders were reviewed against predetermined credit and risk criteria and that the orders appeared in the trading system queue for real-time monitoring. Additionally ascertained that steps were taken to resolve any exceptions if applicable.	No exceptions noted.
3C	Annually, trade edits checks are tested by Trading Platform Strategy & Support personnel to ascertain that the configurations are operating completely and accurately. Testing results are reviewed and approved by the Managing Director of Trading Operations.	**Inspection**—For the annual trade edit checks testing performed during the examination period, inspected the testing documentation and ascertained trade edit checks were tested to ensure they were operating completely and accurately, and resolution action items were identified and tracked to closure. Inspected the testing documentation and ascertained test results were reviewed and approved by the Managing Director of Trading Operations.	No exceptions noted.

#3	Controls provide reasonable assurance that trades are authorized and processed in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
3D	A Series 9/10 review is performed for certain documents received and processed by AS representatives (e.g., account agreements, account feature changes, etc.), escalating any discrepancies to the appropriate party.	**Inspection**—For a sample of client requests during the examination period, inspected advisor checklists completed by a 9/10 representative and ascertained that the requests were identified and processed after the changes and trades had been reviewed for completeness and accuracy and signed off by manual review.	No exceptions noted.
3F	Daily, the Manager or above - Operations reviews and approves the CNS Reconciliation Report in the CASA application to ensure the report balances and that breaks between Schwab and NSCC are resolved in a timely manner.	**Inspection**—For a sample of breaks within the CNS Reconciliation Report during the examination period, inspected the reconciliation review process performed by the team member and ascertained that exceptions were resolved. Ascertained that each discrepancy on the CNS Reconciliation Report has been reviewed and approved by the Manager or designee in a timely manner. **Note**: D&T used the work of SCO to test this control.	No exceptions noted.
3G	As needed, Personal Choice Investment Services 9/10, Series 24 or Series 4 professionals perform a review of client request to add or remove third parties trading authorities and to confirm processing was completed accurately. The reviews are completed within 3 days of processing.	**Inspection**—For sample of requests to add or remove third parties trading authorities during the examination period, inspected the signed request form and MyQ audit log. Ascertained that the requests were reviewed by Series 9/10, Series 24 or Series 4 professionals to confirm the accuracy within 3 business days of processing the request.	No exceptions noted.

#4	Controls provide reasonable assurance that dividend rates are authorized, and payments are calculated and distributed to shareholders of record in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
4A.1	Daily, the Dividends Manager reviews the Payment Exception Reports (Fixed Income) for depositories BNY Mellon and DTCC to ascertain if the reports were reviewed and worked by representatives and that errors were researched and resolved.	**Inspection**—For a sample of days during the examination period, inspected the Fixed Income Exception Report for BNY Mellon and DTCC and ascertained that the Dividends Manager had reviewed each report. Ascertained that all errors identified were researched and the resolution details were documented.	No exceptions noted.
4A.2	Daily, the Dividends Manager reviews the Payment Exception Reports (Foreign Security) for various depositories (Citibank) to ascertain if the reports were reviewed and worked by representatives and that errors were researched and resolved.	**Inspection**—For a sample of days during the examination period, inspected the Cash Exception Spreadsheet for Citibank and ascertained that the Foreign Distributions Team Manager had reviewed each report. Noted that all errors identified were researched and the resolution details were documented.	No exceptions noted.
4A.3	Daily, the Dividends Manager reviews the Payment Exception Reports (Equity Security) for depository DTC to ascertain if the reports were reviewed and worked by representatives and that errors were researched and resolved.	**Inspection**—For a sample of days, inspected the Payment Exception Reports from DTC and ascertained that the Dividends' Senior Manager had reviewed each report. Noted that all errors identified were researched and the resolution details were documented.	No exceptions noted.
4B	On payable date, the Mutual Fund Distributions Manager monitors dividend payment processes for accurate and timely dividend payment. Exceptions are identified, and researched, and resolved in a timely manner.	**Inspection**—For a sample of days during the examination period, inspected the corresponding Dividend Monitoring Suspense Report and ascertained that the Mutual Fund Distribution Team Manager monitored the report for accurate and timely processing of dividend payments. In addition, ascertained that all exceptions were researched and resolved in a timely manner.	No exceptions noted.
4C	On payable date + 1, the Mutual Fund Distribution Team monitors reconciliation systems to identify and resolve payment differences (dividend breaks). Any dividend errors are escalated to the team manager for resolution and business partners are notified.	**Inspection**—For a sample of days during the examination period, inspected the corresponding Dividend Payable Oversight reports and ascertained that the Mutual Fund Distribution Team correctly identified dividend breaks. For any breaks noted, inspected the resolution or escalation and notification to the Team Manager and business partner.	No exceptions noted.

#5	Controls provide reasonable assurance that corporate action notices are identified and received from an authorized source and are updated in the system in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
5A	Daily, the Reorganization Set-up Team Manager, or delegate, ascertains if information collected on upcoming corporate actions is complete and accurate and stored appropriately within the corporate actions folder prior to communicating terms of the offer to the client.	**Inspection**—For a sample of corporate actions during the examination period, inspected the Voluntary Corporate Action Checklist and ascertained the Team Manager collected information on upcoming corporate actions completely and accurately and stored the information within the corporate actions folder prior to communicating terms of the offer to the client.	No exceptions noted.
5B	Daily, the Voluntary Reorganization Team Manager reviews corporate actions with upcoming cut-off and expiration dates to ascertain that corporate action information is complete and accurate and ready for processing according to client instructions. Exceptions are researched and resolved or escalated as needed for resolution.	**Inspection**—For a sample of corporate actions during the examination period, inspected the corresponding Expiring Offers Report and ascertained that the Voluntary Reorganization Team Manager reviewed the corporate action information for completeness, accuracy, and in accordance with client instructions and based on cutoff and expiration dates and ascertained that listed exceptions are researched and resolved or escalated as needed.	No exceptions noted.
5C	Weekly, the Manager inspects the mutual fund reorganizations calendar to ascertain if the calendar has been updated completely and accurately to monitor for the timely processing of organization events. If any upcoming actions are noted as incomplete or inaccurate, the necessary updates are made to the calendar.	**Reperformance**—For a sample of reorganization events during the examination period, obtained the reorganization calendar and reperformed the weekly review by tracing each sample to the BPS checklists as well as the originating email from the Fund company communicating the reorganization event. Noted no incomplete or inaccurate action items requiring update. **Inspection**—For a sample of weeks during the examination period, obtained evidence of the Mutual Fund Distribution Team Manager review of the mutual fund reorganizations calendar. Ascertained no incomplete or inaccurate action items requiring update for the weekly samples selected.	No exceptions noted.
5D	Prior to the approval of a mutual fund reorganization on Schwab's systems, the Managers with authorized approval levels review reorganization information versus Fund provided information to ascertain accurate execution at Schwab. Any discrepancies are confirmed with the Fund.	**Inspection**—For a sample of mutual fund reorganizations during the examination period, inspected the reorganization checklists and ascertained that they were completed timely and that the reorganization information matched to Fund provided information as reviewed by a Mutual Fund Distribution Manager. In addition, ascertained discrepancies were confirmed with the Fund.	No exceptions noted.

#6	Cash and security positions are reconciled completely, accurately and on a timely basis between the custodian and depositories.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
6A	On a monthly basis, an Accounting team member at least one level higher than the preparer reviews all cash account reconciliations to ensure the GL details agree to the bank and any reconciling items are identified and followed-up on/cleared in a timely manner.	**Inspection**—For a sample of cash accounts during the examination period, inspected the monthly cash reconciliation report and ascertained that reconciliations were performed timely and included a detailed level of review, and any discrepancies identified were research and resolved. Ascertained that a review was performed by the Senior Manager, and research and resolution was performed completely, accurately, and timely. **Note**: D&T used the work of SCO to test this control.	No exceptions noted.
6B	On a daily basis, the Asset Recon Manager reviews the Mutual Fund Reconciliation (MFR) Reports to determine if position breaks between custodian and fund companies are reconciled completely, accurately, and timely. Exceptions are researched and resolved by the assigned business unit.	**Inspection**—For a sample of days during the examination period, inspected the MFR Reports and ascertained that the position breaks between the custodian and Fund companies were reconciled completely, accurately, and timely. No exceptions were identified for further research.	No exceptions noted.
6C	Monthly, Officer reviews and approves Internal Accounts reconciliation activity to ensure transactions are appropriate, accurate, and comply with FINRA Rule 4523.	**Inspection**—For a sample of monthly reconciliation emails during the examination period, inspected the emails to ascertain that they contain the appropriate month-end FABP and non-FABP reconciliation reports and approved by the Officer to ensure all transactions were appropriate, accurate, and in compliance with FINRA 4523.	No exceptions noted.

#7	Controls provide reasonable assurance that new securities, changes to existing securities, and pricing of securities are authorized and entered in the security master file in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
7B	As needed, the Security Master Data Management team will conduct a data validation review on mutual fund additions and changes received from Mutual Fund Add and Support and outside vendors. The review is to determine completeness and accuracy for funds that fall outside the parameters of Genesis and vendor feeds. Exceptions are researched and resolved.	**Inspection**—For a sample of mutual fund additions and changes during the examination period, including fund cut-off changes, received from Mutual Fund Add and Support (MFAS) and outside vendors, inspected email evidence and ascertained that the Security Master Data Management team conducted a data validation review in a completely, accurately and timely manner. Ascertained that exceptions for the selected samples were researched and resolved.	No exceptions noted.
7C	Additional mutual fund maintenance, including transaction fees, fund cutoff changes, loads, redemption fees, initiated by the Mutual Fund Add and Support Team are subject to review before updates are made to the system of record. Specifically, changes are reviewed by a peer and/or manager based on the complexity of the change. Users are systematically prevented from adding, peer reviewing, or providing supervisory approval for the same mutual fund change.	**Inspection**—For a sample of mutual fund changes during the examination period, inspected the corresponding QC review and change ticket. Ascertained that the review was performed and that a user cannot review and approve their own changes. **Observation**—D&T observed a user from the Operations team performed a negative test where the user was unable to review and approve their own changes. Further, D&T observed another user reviewed and/or approved changes they did not make. D&T ascertained that the systematic configuration prevented the review and approval of the user's own changes but allowed the change to continue when a different user reviewed and/or approved the change they did not make.	No exceptions noted.
7D	Daily, the Manager, Security Master Quality Management monitors the Incomplete/Restricted SOI (Securities of Interest) Report and Confirmation Error Report to determine if security completeness standards are met and ascertain that incomplete data is not published. Exceptions are researched and resolved.	**Inspection**—For a sample of days during the examination period, inspected the Incomplete/Restricted SOI Report and Confirmation Error Report for evidence of timely review by the Security Master Quality Management Manager. Ascertained that exceptions within the report were researched and resolved.	No exceptions noted.

#7	Controls provide reasonable assurance that new securities, changes to existing securities, and pricing of securities are authorized and entered in the security master file in a complete, accurate, and timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
7E	Daily, Security Master Quality Management team resolves the exception reports and identifies securities with stale pricing (ESM – Stale Price Report) and price changes that break through tolerance levels (ITD-85A Price Change Report), and further ascertains if they are accurate and complete. If pricing data is deemed to be inaccurate, intraday pricing updates are made to the system to correct the market value in client accounts.	**Inspection**—For a sample of days during the examination period, inspected the Stale Price Report and ITD-85A Price Change Report for evidence of review by the Security Master Quality Management Manager.	10/1/2023- 8/30/2024: Exception noted. The Stale Price Report was displaying Thursday's data for each Friday, resulting in the Friday's Stale Price review being performed on inaccurate data. Incorrect Price Change Report was being utilized, resulting in an incomplete, or inaccurate review of price changes that broke through the tolerance levels. 9/1/2024 - 9/30/2024: No exceptions noted.
7F	Security prices (nonmutual fund) are received via batch processing jobs from third-party vendor pricing feeds and uploaded to ESM on a daily basis. Pricing feed errors are monitored by the Security Master Data Management team to resolution.	**Inspection**—For a sample of days during the examination period, inspected the corresponding supporting documentation of daily security prices received from third-party vendors and ascertained prices are reviewed daily and pricing feed errors are monitored to resolution by the Security Master Data Management team.	No exceptions noted.
7G	Mutual fund price data is electronically obtained daily using third-party pricing vendor. Price data is uploaded into ESM completely and accurately.	**Inspection**—For a sampled of day during the examination period, obtained data file from the pricing vendors and inspected pricing feeds to note data is uploaded into ESM completely and accurately. No variances were identified during testing that required follow up.	No exceptions noted.
7H	On a daily basis, the Mutual Fund Trading team review the list of funds without a price from the previous business day. The missing prices are researched and gathered from Mutual Fund Pricing source and then manually updated. Upon completion, the pricing reports are notated by the team member and then signed off by the team manager.	**Inspection**—For a sample of days during the examination period, inspected the Pricing Log/Missing Price Report and ascertained that funds not priced on the previous business day were researched or priced. Ascertained a Mutual Fund Operations Team Manager or delegate reviewed and signed off on the Missing Price Report & NSCC Price Correction Report.	No exceptions noted.
7I	During each transfer weekend, Management reviews exceptions between position quantities transferred from Green (TD Ameritrade) vs. position quantities posted to Blue (CS&Co) customer accounts for all transferred customers. Management ensures all exceptions are investigated and resolved timely, prior to open of business on the first business day following the transfer weekend.	**Inspection**—For a sample of conversion groups, ascertained that conversion exceptions were identified and monitored to resolution.	No exceptions noted.

#8	Controls provide reasonable assurance that account statements and client reports detailing client account holdings and market values are complete, accurate, and provided to clients in a timely manner.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
8A	Monthly, account statements detailing client account holdings and transactions are inspected by the Client Tax Reporting Team prior to the mail run. Issues are researched and escalated if necessary for resolution.	**Inspection**—For a sample of months during the examination period, inspected the reports utilized by the Client Tax Reporting Team and noted evidence of review for completeness and accuracy of statements prior to the mail runs. Ascertained there were no variances for the samples selected that required research or resolution. **Note**: D&T used the work of SCO to test this control.	No exceptions noted.
8B	Monthly, a reconciliation of physical statements to be mailed is performed between Schwab and Printing and Mailing Vendor (Broadridge).	**Inspection**—For a sample of months during the examination period, inspected the reconciliation reports between the data images sent to Broadridge and the physical records of printed statements and ascertained that they had been reviewed by the AMS (Automated Mailing Services) Team Senior Manager for completeness and accuracy. Ascertained that unreconciled items were researched and resolved. **Note**: D&T used the work of SCO to test this control.	No exceptions noted.
8C	On a monthly basis, customer statements generated by CRT are loaded to OnDemand and made available to customers through Schwab.com.	**Observation**—Observed configuration that CRT is configured to load customer statement to OnDemand. **Inspection**—For sample of one month during the examination period, inspected job load and ascertained that statements were loaded into OnDemand. For a sample of accounts, inspected OnDemand and ascertained that account statement details were appropriately loaded to OnDemand.	No exceptions noted.

#9	Controls provide reasonable assurance that logical access to application programs, operating systems, database programs, and the network are restricted to authorized personnel.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
9A.1	Upon hire or transfer, the user's manager approves the nature and extent of user access privileges, including privileged-level access to applications prior to access being provisioned.	**Inspection**—For a sample of users requiring new or modified access to in-scope applications, including privileged user granted access during the examination period, inspected the corresponding access requests and ascertained that access was approved by the requesting user's manager prior to access being granted.	No exceptions noted.
9A.1a	Upon request, the user's manager approves access to Mainframe prior to access being provisioned.	**Inspection**—For a sample of users requiring new access to Mainframe, inspected the corresponding access requests and ascertained that access was approved by the requesting user's manager prior to access being granted.	No exceptions noted.
9A.2	Upon hire or transfer, the user's manager approves the nature and extent of user-access privileges, including privileged-level access to operating systems prior to access being provisioned.	**Inspection**—For a sample of users requiring new or modified access to in-scope operating systems, including privileged user granted access during the examination period, inspected the corresponding access requests and ascertained that access was approved by the requesting user's manager prior to access being granted.	No exceptions noted.
9A.3	Upon hire or transfer, the user's manager approves the nature and extent of user access privileges, including privileged-level access to databases prior to access being provisioned.	**Inspection**—For a sample of users requiring new or modified access to in-scope databases, including privileged user granted access during the examination period, inspected the corresponding access requests and ascertained that access was approved by the requesting user's manager prior to access being granted.	No exceptions noted.
9A.4	Upon hire or transfer, the user's manager approves the nature and extent of user access privileges, including privileged-level access to the network, prior to access being provisioned.	**Inspection**—For a sample of users requiring new or modified access to the network, including privileged user granted access during the examination period, inspected the corresponding access requests and ascertained that access was approved by the requesting user's manager prior to access being granted.	No exceptions noted.
9B.1	On a weekly basis, Identity and Access Management reconciles differences in account access between source system access listings and MyAccess. Discrepancies are identified and resolved.	**Inspection—**Inspected reconciliation performed between system-generated employee and contractor listings against system-generated user access listings for all in-scope systems and ascertained that Management performed reconciliation, and investigated and remediated the discrepancies, if identified. **Re-performance—**For a sample of weeks during the examination period, D&T reperformed the reconciliation between MyAccess and system-generated user listing and ascertained that all access discrepancies were resolved as applicable.	No exceptions noted.

#9	Controls provide reasonable assurance that logical access to application programs, operating systems, database programs, and the network are restricted to authorized personnel.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
9B.1a	Upon termination and/or transfer, the system administrator revokes user access from Mainframe.	**Inspection**—For a sample of terminated and/or transferred users with access to Mainframe, inspected the user status and Mainframe log and ascertained that users' access were disabled timely and no longer retained access to Mainframe post termination and/or transfer.	No exceptions noted.
9B.2	Upon termination, the system administrator revokes user access from the network.	**Inspection**—Inspected system generated user access listings for the Schwab Active Directory network and ascertained whether access to the system was removed timely for all terminated employees and contractors within the testing period.	Exception noted. For 4.96% of Schwab terminated employees and contractors tested during the examination period, the employee/contractor managers did not notify Access Management of the termination timely, thus resulting in untimely removal of users' Windows Active Directory IDs.
9C.1	At least annually, the user's manager reviews user access to applications to determine if accounts are authorized based on their job responsibilities. Unauthorized users are disabled/modified, and the reviews are documented.	*Applicable for Distributed and Mainframe Applications* **Inspection**—Inspected a sample of user access reviews performed during the examination period and ascertained that user access was reviewed by the user's manager to confirm that access to the in-scope system was restricted to personnel based on their job responsibilities. For modifications identified as part of the review, ascertained through inspection of the user access listings that the modifications were implemented by the administrators.	Distributed Applications: No exceptions noted. Mainframe Applications: 10/1/2023 – 4/17/2024: Exception noted. The Mainframe access review was not performed using a complete and accurate user list. 4/18/2024 – 9/30/2024: No exceptions noted.
9C.2	At least annually, the user's manager reviews user access to operating systems to determine if accounts are authorized based on their job responsibilities. Unauthorized users are disabled/modified, and the reviews are documented.	*Applicable for Operating Systems (Windows, UNIX, Linux)* **Inspection**—Inspected a sample of user access reviews performed during the examination period and ascertained that user access was reviewed by the user's manager to confirm that access to the in-scope system was restricted to personnel based on their job responsibilities. For modifications identified as part of the review, ascertained through inspection of the user access listings that the modifications were implemented by the administrators.	No exceptions noted.

#9	Controls provide reasonable assurance that logical access to application programs, operating systems, database programs, and the network are restricted to authorized personnel.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
9C.3	At least annually, the user's manager reviews user access to databases to determine if accounts are authorized based on their job responsibilities. Unauthorized users are disabled/modified, and the reviews are documented.	*Applicable for Oracle Databases* **Inspection**—Inspected a sample of user access reviews performed during the examination period and ascertained whether the user access was reviewed by the user's manager to confirm that access to the in-scope system was restricted to personnel based on their job responsibilities. For modifications identified as part of the review, ascertained through inspection of the user access listings that the modifications were implemented by the administrators. *Applicable for SQL Databases* **Inspection**—Inspected a sample of user access reviews performed during the examination period and ascertained whether the user access was reviewed by the user's manager to confirm that access to the in-scope system was restricted to personnel based on their job responsibilities. For modifications identified as part of the review, ascertained through inspection of the user access listings that the modifications were implemented by the administrators.	No exceptions noted.
9C.4	On a biannual basis for administrator and service accounts, the user's managers review user access to the network. Any modifications identified as part of the review are completed by the network administrators.	*Applicable for Windows Active Directory* **Inspection**—For the network administrator and service accounts access reviews, ascertained that the access reviews were completed timely by the user's manager. For a sample of modifications, ascertained through inspection of the system-generated user access listings that the modifications were implemented timely by the network administrators.	No exceptions noted.
9D.1	Password parameters, including password minimum length and complexity, expiration, and account lockout for applications, have been configured per the Information Security Policy.	**Inspection**—Inspected the Information Security Policy and ascertained that standards have been documented by IT for password complexity, length, expiration, and account lockout. **Observation**—Observed password settings for the in-scope applications and ascertained that user and privileged support accounts follow the Schwab Technology Standard for password complexity, length, expiration, and account lockout.	No exceptions noted.
9D.2	Password parameters, including password minimum length and complexity, expiration, and account lockout for operating systems have been configured per the Information Security Policy.	**Inspection**—Inspected the Information Security Policy and ascertained that standards have been documented by IT for password complexity, length, expiration, and account lockout. **Observation**—Observed password settings for the in-scope operating systems and ascertained that user and privileged support accounts follow the Schwab Technology	No exceptions noted.

#9	Controls provide reasonable assurance that logical access to application programs, operating systems, database programs, and the network are restricted to authorized personnel.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
		Standard for password complexity, length, expiration, and account lockout.	
9D.3	Password parameters, including password minimum length and complexity, expiration, and account lockout for databases have been configured per the Information Security Policy.	**Inspection**—Inspected the Information Security Policy and ascertained that standards have been documented by IT for password complexity, length, expiration, and account lockout. **Observation**—Observed password settings for the in-scope databases and ascertained that user and privileged support accounts follow the Schwab Technology Standard for password complexity, length, expiration, and account lockout.	No exceptions noted.
9D.4	Password parameters, including password minimum length and complexity, expiration, and account lockout for the network have been configured per the Information Security Policy.	**Inspection**—Inspected the Information Security Policy and ascertained that standards have been documented by IT for password complexity, length, expiration, and account lockout. **Observation**—Observed password settings for the network and ascertained that user and privileged support accounts follow the Schwab Technology Standard for password complexity, length, expiration, and account lockout.	No exceptions noted.
9E.1	Privileged access to applications is restricted to authorized individuals based on job responsibilities.	**Inspection**—Inspected system-generated user access listings and roles for the in-scope applications and ascertained that privileged access was assigned to authorized individuals based on job responsibilities.	No exceptions noted.
9E.2	Privileged access to operating systems is restricted to authorized individuals based on job responsibilities.	**Inspection**—Inspected system-generated user access listings and roles for the in-scope operating systems and ascertained that privileged access was assigned to authorized individuals based on job responsibilities.	No exceptions noted.
9E.3	Privileged access to databases is restricted to authorized individuals based on job responsibilities.	**Inspection**—Inspected system-generated user access listings and roles for the in-scope databases and ascertained that privileged access was assigned to authorized individuals based on job responsibilities.	No exceptions noted.
9E.4	Privileged access to the network is restricted to authorized individuals based on job responsibilities.	**Inspection**—Inspected system-generated user access listings and roles for the in-scope network and ascertained that privileged access was assigned to authorized individuals based on job responsibilities.	No exceptions noted.

#10	Controls provide reasonable assurance that changes to application programs, systems software, data management systems, and network infrastructure are documented, tested, approved.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
10A	The Detected Change Reconciliation Process Team investigates unusual or anomalous activity, as needed to determine that changes in the infrastructure are authorized.	**Observation—**Observed Tripwire console settings and ascertained that the changes implemented for in-scope application production servers and files were configured to be monitored. **Inspection—**For all in-scope applications monitored by Tripwire, inspected the applications' respective attestation and ascertained that the application production servers and files changes were being continuously monitored. **Inspection-** For a sample of changes during the examination period, inspected incident tickets and ascertained that Detected Change Reconciliation Process Team reviewed filtered Change Reports and investigated unusual or anomalous activity on a daily basis and ascertained that changes in the infrastructure were authorized.	No exceptions noted.
10A.1	Mainframe System Engineers configure the release management tool (ChangeMan) to require approvals and/or prevent self-approval of change packages as needed prior to migration to production.	**Observation—**Observed the mainframe release management tool (ChangeMan) system configurations and ascertained that the system was configured to require approval and prevent self-approval approval of change packages as needed prior to migration to production.	No exceptions noted.
10A.2	For MyQ and CASA a monthly review of changes implemented into production environment is performed by the PEGA support team to ensure only authorized changes were implemented.	**Observation—**Observed the configuration the system and ascertained whether it was configured to e-mail a list of implemented changes monthly to the PEGA support team. **Inspection—**For a sample of months during the examination period, inspected the review of the monthly changes for the MyQ and CASA applications and ascertained that all implemented changes were authorized and appropriate.	No exceptions noted.
10B	When applications, system software, or database changes are made, authorized personnel in Change Management Group test and document the change in a change ticket prior to implementation.	**Inspection**—For a sample of changes implemented during the examination period, inspected change tickets from the ticketing system and ascertained that changes were documented and tested by authorized personnel prior to implementation into production.	No exceptions noted.
10C	When applications, system software or database changes are made, authorized personnel approve the changes prior to implementation.	**Inspection**—For a sample of changes implemented during the examination period, inspected change tickets from the ticketing system and ascertained that changes were documented and approved by management prior to implementation.	No exceptions noted.

#10	Controls provide reasonable assurance that changes to application programs, systems software, data management systems, and network infrastructure are documented, tested, approved.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
10D	When network infrastructure changes are made, authorized personnel track and document the changes within the change ticketing system. These changes are tested in a development area and approved by authorized users prior to implementation of changes.	**Inspection**—For a sample of changes implemented during the examination period, inspected change tickets from the ticketing system and ascertained that changes to the network were tracked, documented, tested in a development area, and approved by authorized users prior to implementation.	No exceptions noted.

#11	Controls provide reasonable assurance that physical access to the data centers is restricted to authorized personnel as per their job responsibilities.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
11A	Before the granting of new physical access to data centers, the operations team approves user access.	**Inspection**—For sample of new users who received access to the data centers during the examination period, inspected approval documentation and ascertained that each user was approved by management prior to access being granted, and access commensurate with the user's job responsibilities.	No exceptions noted.
11B	At least semiannually, an appropriate data center access authorizer performs a review of the data centers user access listing. Any modification identified as part of the review is implemented by the Operations team.	**Inspection**—Inspected a semiannual data center access review and ascertained that the review was performed by management. Ascertained that access changes requested as part of the review were completed, through inspection of the user's account on the system.	No exceptions noted.
11C	Upon termination and/or transfer of a user, the Operations team revokes or modifies user access to the data centers in accordance with documented company policy.	**Inspection**—Inspected system-generated user access listings to the data centers and ascertained that for identified terminated employees and contractors during the examination period, access to the data center were removed within one business day per the documented company policy.	No exceptions noted.
11D	Physical access mechanisms (e.g., access card readers, biometric devices, man traps/portals, CCTV cameras, alert notifications) have been implemented to restrict and detect unauthorized access to the data centers.	**Observation**—Observed physical access mechanisms during the examination period and ascertained that the data centers had physical access mechanisms in place, including but not limited to access card readers, biometric devices, man traps/portals, CCTV cameras, alert notifications and locked cabinets.	No exceptions noted.

#12	Controls provide reasonable assurance that backup and recovery procedures exist, and that data is backed up regularly.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
12A	Schwab Technology and Business Continuity Services implement and execute data backup, off-site replication, and data recovery procedures for its production servers. Exceptions are followed through to resolution.	**Inspection**—Inspected the job schedule settings and ascertained production servers were configured to be backed up on a daily basis. For a sample of days during the examination period, inspected data mirroring status logs and ascertained production servers were backed up successfully and replicated to an off-site location. Further, ascertained that any exceptions were followed through to resolution. Additionally, inspected data recovery test results and ascertained that the annual test was completed, and recovery procedures were successfully performed for all relevant applications.	No exceptions noted.

#13	Controls provide reasonable assurance that job processing is monitored and that processing deviations are identified and resolved.		
Advisor Services Control #	**Controls Specified by Advisor Services**	**Testing Performed by Deloitte & Touche LLP**	**Deloitte & Touche LLP Test Results**
13A	Batch jobs are monitored by the Enterprise Batch Services team, and processing errors are corrected to ensure successful completion.	**Inspection**—For a sample of job failures, ascertained that the job failures were identified and monitored to resolution. **Note**: D&T used the work of SCO to test this control.	No exceptions noted.
13B	Access to update the batch job scheduler is restricted to authorized individuals based upon job responsibilities.	**Inspection**—Inspected the system-generated user access listings from the job scheduler and ascertained that privileged access to the job scheduler was restricted to authorized personnel based upon their job responsibilities.	No exceptions noted.

Section 5: Other Information Provided by Management of Schwab

The information included in Section 5 is presented by Schwab to provide additional information to user entities and is not a part of Schwab's description of the system. The information in Section 5 has not been subjected to the procedures applied in the examination of the aforementioned description of the AS system and, accordingly, D&T expresses no opinion on the information contained within Section 5.

Management Responses to Testing Exceptions

Control Objective 7

Control 7E:

Report Exception:

10/1/2023- 8/30/2024: Exception noted.

The Stale Price Report was displaying Thursday's data for each Friday, resulting in the Friday's Stale Price review being performed on inaccurate data.

Incorrect Price Change Report was being utilized, resulting in an incomplete, or inaccurate review of price changes that broke through the tolerance levels.

9/1/2024 - 9/30/2024: No exceptions noted.

Management's Response:

The Microsoft Excel macro used for the Stale Price report to review prior day prices and ensure accounts remain within appropriate tolerance levels, was incorrect, resulting in the Monday Stale Price report displaying Thursday prices instead of the Friday prices. Management identified the discrepancy as part an internal evaluation and remediated by updating the macro to display the appropriate Friday prices for the reviews of the Monday Stale Price report.

Management also identified the data source used for the Price Change report to review price changes that exceeded tolerance levels, was incorrect. Reviewers initially viewed the Price Tolerance report from the ITEM data source that rounded and truncated values which could have potentially impacted a price change value exceeding a tolerance level. Management remediated the issue by transitioning the source of the Price Change report to the ESM system with a more robust rounding and truncating method to provide more extensive pricing data for the Price Change report.

Control Objective 9

Control 9B.2:

Report Exception: For 4.96% of Schwab terminated employees and contractors tested during the examination period, the employee/contractor managers did not notify Access Management of the termination timely, thus resulting in untimely removal of users' Windows Active Directory IDs.

Management's Response:

For most accounts, the user's termination information was provided to the Identity Access Management (IAM) team after the termination date. The IAM team disabled access within the appropriate timeframe for these user accounts upon notification by the employee's/contractor's manager. Management will continue to re-educate managers on proper termination procedures, including prompt entry into the enterprise HR system.

In addition, when evaluation control effectiveness across an entire population of manual control instances, a small percentage of tolerable exceptions is expected. Management has set a tolerable error rate of 5% when considering full populations of control execution. The actual error rate identified by the service auditor falls within Management's tolerable error range of up to 5%.

Control 9C.1:

Report Exception:

10/1/2023 – 4/17/2024: Exception Noted. The Mainframe access review was not performed using a complete and accurate user list.

4/18/2024 – 9/30/2024: No Exceptions Noted

Management's Response:

Management's research indicated most of the discrepancies were the result of duplicate Mainframe IDs in MyAccess. As the same ID was assigned to the same user twice in MyAccess, the system did not know which instance of the ID to assign the profile. As a result, access existed in the Mainframe that did not reconcile to MyAccess and was not included in user certifications. However, these entitlements followed our provisioning approval process before they were granted hence access was appropriate. The amount of these discrepancies represent only .02% of the active reviewed profiles.

Management performed lookback procedures to identify discrepancies that did not show up in the reconciliation report. Each instance identified was researched and resolved. No account identified as a discrepancy belonged to a terminated user. A daily monitoring process has been put in place to identify duplicate IDs going forward.

Business Continuity and Disaster Recovery

The stability of Schwab's business practices, as well as its technology systems, is vital to earning and maintaining client trust and protecting Corporation and client assets. Schwab makes every effort to provide uninterrupted services through a comprehensive business continuity program.

Schwab's Business Continuity Program is:

- Aligned with FINRA rules and Federal Financial Institutions Examination Council's Business Continuity guidance.
- Managed by the Business Continuity Planning and Incident Management team within First Line Risk Management Office
- Led and managed by a dedicated group of experienced business continuity and incident management professionals.
- Subject to ongoing internal and external examiner review
- Reviewed annually by the Board of Directors or their delegated Subcommittee and Senior Management

Schwab's comprehensive business continuity plans include, but are not limited to:

- Recovery time objectives and priorities based on a thorough business impact analysis process.
- Predefined teams and members responsible for coordinating and facilitating business unit response and recovery from distributions.
- Predefined recovery strategies for a loss of personnel, workspace, required dependencies, and communications resources
- Multiple geographically diverse service centers allowing transfer of work to alternate locations.
- Predetermined systems and data recovery requirements
- Identification of internal and external resource dependencies and contingency plans
- Annual employee awareness and business continuity training

- Testing of recovery capabilities.

Technology is a critical component in business continuity planning and Schwab is proactive in protecting its IT environment. Primary and backup data centers are designed and maintained with redundant power and site environmental control paths and redundant components, where required. Site locations are subject to few traditional natural hazards. In the event of a utility company supply failure, uninterruptible power supply (UPS) will provide power to key servers, databases, and critical systems while diesel-powered generators come online to supply the facility's electrical demand. Multiple UPS units and generators are available to provide critical infrastructure component redundancy. Standard safeguards include:

- Redundant communications lines delivered through diverse building entrance facilities
- State-of-the-art computer rooms—controlled access, with redundant critical facilities
- 24x7 critical facility plan and physical security monitoring
- 24x7 on-call staff
- Real-time data mirroring, system monitoring, and nightly backups with off-site storage

In addition, Schwab's Business Continuity, Technology Disaster Recovery, Security, and Corporate Real Estate groups develop collaborative emergency response procedures for each location and take a proactive approach to integrating with local police and fire departments, government agencies, and key vendors. While no contingency plan can eliminate all risk of service interruption, we continually assess, test, and update our business continuity plans, disaster recovery plans, and program to mitigate reasonable risk.

The Technology Disaster Recovery team performs regular testing of recovery plans, processes and procedures to ascertain that Disaster Recovery Plans function as expected to support the IT operations for the firm in case of a disaster declaration at one of the primary data centers.

Compliance Oversight

Schwab provides AS with compliance services. The following key functions are performed by Compliance: regulatory consulting, compliance monitoring, responding to applicable regulatory inquiries/complaints, communications with the public (CWTP), and compliance training.

Regulatory Consulting

Compliance provides regulatory guidance to business units with a view toward managing regulatory risk to protect the Company's reputation and avoid disciplinary action in the context of applicable rules and regulations as mandated by FINRA, the US Federal Reserve Board, or the SEC, and various state securities regulation. Compliance serves as a liaison for regulatory examinations impacting business units.

Compliance Monitoring

Compliance performs regular compliance assessment of product development and delivery, including fees and services, and coordinates with the Corporate Compliance Department on compliance monitoring, streamlining company-wide processes, and resolving exceptions relative to the supported business units.

Responding to Regulatory Inquiries/Complaints

Compliance is responsible for responding to written regulatory inquiries/complaints received from the SEC, the US Federal Reserve Board, FINRA, state, and other regulatory agencies as related to the assigned business units. In responding to the inquiry/complaint, it is important to distinguish between recordkeeping and broker-dealer activities to maintain appropriate regulatory oversight. The Office of Investor Education and Advocacy and FINRA require that customer complaints be responded to within 14 days.

Communications with the Public

All communications with the public are maintained in Workfront, an electronic workflow system, in which approved employees can submit applicable communications with the public for review and approval by the business supervisory approver designated by the head of each business unit. Workfront maintains the files with the approval date, final copy of the communication, Compliance comments, name of the approver, and type of communication.

Compliance Training

Compliance is responsible for providing information to its business partners and employees on changes in applicable rules, regulations, regulatory expectations, and Compliance manual policies. At times, due to changes in the business or regulatory environment, Compliance may assist in the preparation and facilitation of training. This is done on an ad hoc basis.

Bonding and Insurance

The Company, its subsidiaries, and affiliates fully satisfy the levels of coverage required under regulation. Schwab maintains a comprehensive corporate insurance program that is commensurate with the risks attendant in the services we provide to clients. Key coverages that Schwab carries include:

- Blended program is "claims made" coverage that includes Errors & Omissions, Financial Institution Bond, and Computer Crime. Primary coverage is through Markel Bermuda Limited.

The Financial Institution Bond and Computer Crime coverages provide protection for loss due to dishonest or fraudulent acts of employees and known and unknown third persons; loss of property through burglary; loss on premises; loss in transit while in the custody of an employee messenger; forgery or alteration of checks, drafts, acceptances, and related instruments; forged and counterfeit securities accepted or held; and the use by outside parties of any computer system utilized by Schwab for fraudulent or dishonest acts.

The Financial Institution Professional Liability coverage provides protection against loss from errors and omissions, breaches of fiduciary duty, and other wrongful acts arising out of the performance of professional services for a client for a fee.

- Casualty program is "occurrence" based coverage that includes General Liability, Workers Compensation, and Automobile Liability.

General Liability coverage provides protection for claims made by a third party for bodily injury, death, broad form property damage, contractual liability, independent contractors, and personal and advertising injury for which the Company is liable.

Workers Compensation coverage provides statutory benefits to employees for occupational injury or disease received in the performance of their job duties.

Automobile Liability coverage provides protection against claims made by a third party for damages caused by the operation of a vehicle in the performance of Company business for which the Company is legally liable.

The insurance carriers for all policies are **A.M. Best** rated A-VII or better.

Schwab does not warrant that the aforementioned insurance coverages will be continuously maintained, and Schwab reserves the right to alter its insurance coverage as it deems prudent and appropriate to its business.

Privacy Policy

Schwab has adopted a Privacy Policy that explains what and how personal information can be used by Schwab, its affiliates, and third parties. The policy is mailed annually to account owners and with each new account opening.

Schwab handles personal information in accordance with the practices and safeguards described in its privacy policy at www.schwab.com/privacy.

Asset Safety and Protection

The Securities Investor Protection Corporate (SIPC) is a nonprofit, membership corporation, funded by its member securities broker-dealers. It is not a government agency or regulatory authority. All broker-dealers (Schwab included) registered with the SEC are required to be members of SIPC. SIPC helps restore funds to individuals whose money, stocks, and other securities are put at risk by bankrupt and otherwise financially troubled brokerage firms. SIPC does not protect investors against market risks. These are the key factors for clients to consider about overall asset safety at Schwab:

- **SIPC Protection:** (Schwab brokerage accounts) SIPC protects members up to $500,000, including $250,000 for cash claims.
- **Excess SIPC Protection:** Additional account protection for client brokerage accounts is provided by Lloyd's of London and other London insurers. Coverage is up to $149,500,000 per client account (based on ownership type) for securities, including $900,000 for cash claims, with an aggregate limit of $600 million.