Brown & Brown Written Supervisory Procedures

Customer Privacy Policies and Procedures [SEC Regulation S-P]

[Gramm-Leach-Bliley Act Sections 501-503; SEC Regulation S-AM and S-P; Evolution of a Prototype Financial Privacy Notice: http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf; FINRA web site Customer Information Protection: http://www.finra.org/industry/customer-information-protection; Fair Credit Reporting Act; SEC Risk Alert on Regulation S-P: https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf]; NIST Cybersecurity Framework 2.0: https://www.nist.gov/cyberframework

Introduction

At Brown & Brown we are committed to protecting your privacy and the confidentiality of your personal and financial information. We are required, by federal law, to provide you with this notice, which outlines our business practices to protect your privacy, as well as how we collect and share personal information about you. This policy applies to both current and former clients. The measures we take to keep your personal information private and secure are outlined below.

Information regarding customer accounts for individuals is subject to SEC Regulation S-P "Privacy of Consumer Financial Information." This section explains employees' obligation to maintain the privacy of information.

1. Regulation S-P requirements apply to individual and not institutional accounts and include U.S. and foreign accounts.
2. Protected information is termed "nonpublic personal information." This is information obtained by Brown & Brown that is not deemed "public information" which is defined as information that may be obtained from three sources: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law.
3. At the time an account is opened the customer is provided with Brown & Brown 's privacy policy and is given the opportunity to opt out of arrangements to share non-public information with nonaffiliated third parties. The privacy policy is also provided to customers on an annual basis.
4. Employees are prohibited from sharing or releasing nonpublic personal information other than to authorized parties. This includes a prohibition against:

    - Sending internal reports or other information about firm customers to a non-affiliated 3rd party (unless authorized).
    - Sending internal or other documents which include customer non-public information to your personal e-mail address.

Brown & Brown has adopted a Privacy Policy which is provided to customers at the time a new account is opened. The Privacy Policy explains the firm's policies regarding safeguarding of customer information and records and whether Brown shares information with outside parties. Brown & Brown also publishes its Privacy Policy on its web site. Customers will receive notice of revisions to the Privacy Policy when they occur.

SEC Regulation S-P ("Privacy of Consumer Financial Information") applies only to accounts for individuals (*i.e.,* institutional accounts are not affected) and differentiate between "customers," where Brown & Brown has an established relationship with the individual, and "consumers," where there is no pre-established relationship. For purposes of this section, any individual from whom information is obtained (and their legal representative acting on their behalf) to open an account or to obtain services or

products from the firm is considered a "customer." The term "consumer" will be considered synonymous with "customer" for purposes of this section. The safeguards and disposal requirements cover both the non-public personal information collected by the Firm about its own customers and non-public personal information the Firm receives from another financial institution about customers of that financial institution.

The Privacy Policy applies to all individual customers of Brown & Brown, whether U.S. residents or foreign residents.

Questions about providing customer information should be referred to Compliance.

Responsibility	• Designated Supervisor
Resources	• The Firm's Privacy Policy • Customer opt-out requests (if applicable) • Available reports and/or data • Third-party vendor contracts
Frequency	• When accounts are opened - provide copy of Privacy Policy and opt-out form (if opt-out is applicable) • As required- send notice of revised Privacy Policy to all customers • As determined by the designated supervisor: training for employees • As necessary - establish procedures for protecting customer information and ensuring information is only shared when it is allowed • As necessary - when new technologies are adopted • When third-party vendors are engaged to handle customer information • Periodically - audit/test internal systems
Action	• Establish procedures to protect customer information against unauthorized access or use, regardless of where data is stored, including (but not necessarily limited to): o Validation of customer online access o Limiting access to only authorized personnel o Reviewing third party access to sensitive information and third-party establishment of sound safeguards o Remove access to customer information for departing employees o Limit employee access only to required information • Provide the privacy policy to customers: o At time of account opening o Annually o When revisions are made o On the Firm's web site • Code accounts for customers opting out (if applicable) • When a breach occurs: o Send breach notification to affected customers as soon as practicable but no later than 30 days of a breach o Notify key personnel as necessary o Review systems for cause of breach and take corrective action

	○ If the breach is through a third-party vendor, obtain information about the scope of the breach, corrective action taken, and timeframe for correction • If "eligibility information" is received from affiliates, determine that Regulation S-AM requirements are satisfied • Test internal computer systems periodically • Oversee third-party service providers with access to customer information: ○ Ensure agreements with third parties receiving customer information reflect the third-party provider's safeguards; confidentiality agreement; and agreement to notify the Firm of breaches and corrective action ○ When new technologies involving customer information are adopted: ○ Contact the Firm's technology officer to: ▪ Determine whether appropriate technological precautions have been taken to protect customer information ▪ Determine whether existing testing/audits will include the new technology and, if not, adjust testing program ○ Review existing policies and procedures to determine if changes/additions are required ○ Determine whether added training of employees is necessary and implement, if required ○ Provide training for employees
Record	• Current Privacy Policy • Customer opt-out requests (if applicable) • Record of providing notices to customers annually, when revised, and on the Firm's web site • Records of breach of sensitive customer information • Records of customer breach notifications including date of providing • Determination that Regulation S-AM requirements are satisfied, if information from affiliates will be used for marketing purposes • Copies of signed agreements with third parties receiving customer information and review of third-party's program to prevent breaches • Records of periodic privacy audits or other reviews conducted of the Firm's computer system that retains customer information • Records of reviews of outsourced services involving the privacy of customer information • Records of review of new technology involving customer information • Employee training

Responsibility For Privacy Policy

The firm's chief compliance officer, Colon Brown Jr., is the firm's designated supervisor responsible for the firm's Privacy Policy system. Where appropriate, responsibilities will be segregated and/or supervised to prevent unauthorized activities.

"Public" vs. "Nonpublic" Personal Information About Customers

Generally, information provided to Brown & Brown by a customer or potential customer in the normal course of the firm offering a product or service is considered "nonpublic personal information." Identifying whether information is "public" or "nonpublic" is important as to Brown & Brown 's obligations if our firm shares information with nonaffiliated third parties. Public information is information that one reasonably believes may be obtained from three sources:

- federal state or local government records;
- widely distributed media; or,
- disclosures to the general public that are required to be made by federal, state, or local law.

Nonpublic personal information also includes any list, description, or other grouping of customers (and publicly available information about them) that is derived from financial information that is not publicly available.

Sharing Nonpublic Personal Information

In the normal course of business, Brown & Brown may share customer nonpublic personal information with service providers such as clearing firms or service bureaus. Agreements with such third parties include assurances regarding the protection of customer records and information. Information sharing with affiliated companies may also occur, and if applicable, is disclosed in the firm's Privacy Policy.

Brown & Brown does not share customer nonpublic personal information with non-affiliated companies or non-exempt service providers.

Customer Opt-Out

At the time an account is opened, the customer is given the opportunity to opt out of the Firm's arrangement to share nonpublic personal information with affiliates and nonaffiliated third parties other than clearing firms and other service providers. For accounts that choose to opt out, the accounts will be blocked from such information sharing arrangements.

Customer Notice

[12 CFR Federal Reserve System Regulation P; Federal Reserve Privacy of Consumer Financial Information (Regulation P): http://www.federalreserve.gov/boarddocs/supmanual/cch/consumer.pdf; Gramm-Leach-Bliley Act Title V Section 503]

Covered institutions are required to notify those whose sensitive information was, or was reasonably likely to have been, accessed or used, within 30 days of an incident. The firm will provide notice to customers about our Privacy Policy. The notice is provided as follows:

- At the time an account is opened.
- On our web site.
- Annually, unless the firm meets the following two conditions:
    - The firm does not disclose personal nonpublic information to third parties (*e.g.,* sharing in connection with marketing activities vs. sharing solely to service customer accounts), other than disclosure permitted under exemptions available under the Gramm-Leach-Bliley Act; and
    - There has been no change in policies regarding disclosing nonpublic personal information from the last notice sent to customers
- When there is a revision to the Privacy Policy.

Third-Party Provider Oversight and Vendor Management

The Firm recognizes that service providers play a critical role in safeguarding customer information. The Firm exercises oversight—including due diligence and monitoring—over all service providers who receive, maintain, process, or otherwise access customer information on behalf of the Firm.

The Firm's service provider oversight program is governed by written policies and procedures reasonably designed to ensure service providers take appropriate measures to protect customer information and notify the Firm within 72 hours of becoming aware of a breach in security involving unauthorized access to customer information systems. The Firm initiates its incident response program immediately upon receiving such notice.

The Firm may, where appropriate, contractually delegate customer notification responsibilities to a service provider, provided that the Firm retains ultimate responsibility for ensuring compliance with all notification obligations.

The amendments to the regulation formally establish requirements for covered institutions to adopt policies and procedures regarding due diligence and monitoring of service providers. Under Amended Regulation S-P, policies must be reasonably designed to ensure service providers take appropriate measures to:

- Protect against unauthorized access or use of customer information; and
- Provide notification to covered institution clients within 72 hours of becoming aware of a breach resulting in unauthorized access to a customer information system maintained by the service provider. Upon receipt of notification, a covered institution must initiate its incident response program.

When third-party providers have access to customer non-public personal information, the Firm will:

- Include review of the provider's procedures for protecting information and preventing breaches
- Confirm provider breach procedures

Recordkeeping and the Disposal of Customer Information

The firm will ensure to take appropriate steps to maintain written records evidencing compliance with the amended rules. The rules were expanded to include any information maintained by transfer agents. The Books and Records Rule were amended in conjunction with Regulation S-P to include:

- Records of written policies and procedures;
- Written documentation of any detected unauthorized access, any response to, and recovery from such access;
- Written documentation of any investigation and determination made regarding whether notification is required, including the basis for such determination, as well as any notice transmitted; and
- Any written contracts or agreements entered into pursuant to the rule. For RIAs, these records must be maintained for five years, the first two in an easily accessible place.

The Disposal Rule, a component of Regulation S-P, requires firms to securely dispose of customer and consumer report information once it's no longer needed for business or regulatory purposes. Disposal of customer information will follow procedures to prevent unauthorized access or use in accordance with the disposal policy.

Acceptable disposal methods include:

- Shredding or pulverizing paper records

- Permanently deleting or wiping digital files from storage devices
- Using certified vendors for the destruction of electronic media

Disposal of Consumer Report and Customer Information and Records

Consumer report and customer information and records will be disposed of in a manner to prevent unauthorized access or use. Procedures may include the following:

- Responsible employees will be identified and trained in proper disposal procedures.
- Information subject to these procedures will be identified in a written memo maintained and updated by the designated supervisor.
- There will be secure removal of trash involving consumer report and customer information.
- Paper information will be burned, pulverized, or shredded so that it cannot be practicably read or reconstructed.
- Electronic information will be destroyed or erased so the information cannot be practicably read or reconstructed.

Outsourcing (Third-Party Vendors)

Responsibility	• Designated Supervisor
Resources	• Third-party vendors • Reviews of vendor performance • Customer complaints
Frequency	• At initial identification of need for outsourcing: identify candidate vendors • Upon engagement: Obtain written agreement • Annually: Obtain attestation or certification • Ongoing: monitor and periodically audit vendor activities
Action	• Identify areas of the Firm's business where outsourcing is appropriate • Identify third-party vendors that provide the needed services • Evaluate potential third parties and determine whether to engage using the Service Provider Due Diligence Spreadsheet • Execute an agreement to include, among other items: o validating data protection controls in contracts o representations that they are conducting self-assessments o recordkeeping will comply with regulatory rules o the vendor and/or its employees are appropriately registered where required o authorized access to the Firm's systems and customer information o disposition of records upon termination of agreement o existence of a Business Continuity Plan covering the Firm's records o the vendor's use of vendors (fourth-party vendors) that may handle firm data o a prohibition against firm or customer information being ingested into the vendor's open-source generative AI tool • Maintain a list of all third-party vendor-provided services • Determine vendor access to sensitive firm or customer non-public information and critical firm systems granting access only when required and revoking when no longer needed and upon termination

	• For third-party technology, consider business impact including assessment and contingency plans • Evaluate the impact of the Firm's ability to meet its regulatory obligations if the third-party vendor fails to perform the outsourced activity or function • Review and adjust, as needed, third-party vendor tool default features and settings (*e.g.,* disabling a chat feature, reviewing whether communications are being captured for supervisory review) • Require periodic attestations or certifications the vendor has fulfilled certain reviews or obligations under the agreement • Include vendor activities in periodic audits for compliance with the agreement and regulatory requirements • Involve third-party vendors that support key systems in the testing of the Firm's Incident Response Plan • When problems are identified through customer complaints, monitoring of services, reports from employees, or from the vendor itself, take corrective action which may include: o Review the problem to determine whether the source is the vendor or is internal o Take corrective action which may include the following: ▪ Contact the vendor and determine what corrective action will be taken and follow-up to determine corrective action has been taken ▪ If the problem continues or is significant, determine whether vendor agreement should be continued ▪ If the problem is internal, contact the appropriate supervisor to determine corrective action ▪ Report issues to regulators if required o Consult with Compliance when necessary to determine action to be taken
Record	• Service Provider Due Diligence Spreadsheet • Contracts/agreements with third parties • Annual attestation • Records of third-party vendor reviews including periodic audit reviews • Records of corrective action taken including reports to regulators, if applicable\

Some services may be outsourced to third parties (vendors). While third parties are responsible for providing agreed-upon services in an accurate manner, regulators have stated that firms remain responsible for ultimate compliance with rules governing the outsourced activity (covered activities) that, if performed by a firm, would be required to be the subject of a supervisory system and written supervisory procedures.

When choosing an outside vendor, a number of factors will be considered depending on the type of service provided. Factors that may be considered when engaging a third party include:

- Length of time in business
- Financial stability
- Prior knowledge of the vendor
- Other users of the vendor's services
- Technology and ability to deliver services
- Security of customer or other financial information, if applicable

- Vendor's cybersecurity controls
- Vendor's ability to retain firm records in accordance with regulatory requirements
- Who at the Firm is responsible for oversight and monitoring the vendor's services

A Service Provider Due Diligence Spreadsheet will be completed when a new vendor is considered.

Reporting Possible Law or Rule Violations

[SEC Securities Exchange Act of 1934 Section 21F; SEC Rule 21F; FINRA Rule 4530(b)]

Responsibility	• Chief Compliance Officer (or, if the CCO is involved in the potential wrongdoing, an alternate senior manager)
Resources	• Reports of possible law or rule violations from employees • Referrals from outside sources such as regulators
Frequency	• Investigate reports: As required • Employee education: At least annually
Action	• Acknowledge the employee's report and advise confidentiality will be maintained and there will be no retaliation for reporting • Determine who will be involved in the investigation and notify those persons of the confidentiality of the investigation • Conduct the investigation using tools appropriate to the issue (interviewing employees, reviewing internal/external reports, engaging counsel, etc.) • Determine whether there was potential wrongdoing and decide whether a report should be made to regulators • Take internal corrective action, as appropriate • Advise the reporting employee of the status of the investigation • Include reporting of possible law or rule violations and the firm's process for internal investigations as part of regular employee education
Record	• Report from employee • Information regarding the investigation including records reviewed, who is involved, what steps taken, reports to regulators (if appropriate), conclusion of investigation • Records of employee education including how education is conducted (classes, online education, compliance memos, etc.), who participates, subjects included, and when it occurs

It is the intent of the firm to adhere to all laws and regulations that apply to the organization; the underlying purpose of this policy is to support the organization's goal of legal compliance. The support of all employees is necessary to achieve compliance with various laws and regulations.

Reporting

Employees should report possible crimes or rule violations involving the brokerage, a department, or an employee or employees as well as outside vendors or service providers. Reporting may be made to any or

all of the following, particularly where the employee's supervisor may be involved in the possible wrongdoing.

1. Compliance Officer
2. Your supervisor
3. Your supervisor's supervisor
4. Chief Compliance Officer
5. General Counsel
6. Chief Executive Officer

Confidentiality of Employee Reporting

All reports will be treated as confidential. The employee's identification will be kept confidential other than those who need to know such as the compliance officer or counsel or someone else conducting an investigation. Any person identified in the report as a potential wrongdoer will not be provided the name of the person who has filed a report.

Notification of Chief Compliance Officer

A supervisor or other manager who receives a report of possible violations should immediately refer the matter to the Chief Compliance Officer who is responsible for conducting an investigation and overseeing the review until its conclusion, including potential reporting to a regulator. If the Chief Compliance Officer is involved in the potential wrongdoing, the member of management to whom the issue is reported will be responsible for conducting the investigation.

Investigation

The firm will promptly investigate the reported possible wrongdoing and determine what action is required. Outside counsel may be engaged as part of the investigation. The reporting employee will be advised of the conclusion or resolution of the investigation.

Anti-Retaliation

The firm will not retaliate against an employee who reports some practice of the brokerage, a department, or employee(s) or of another individual or entity with whom the firm has a business relationship that may represent a rule or law violation. Brown will not retaliate against employees who disclose or threaten to disclose (to Brown or a public body such as a regulator) any activity, policy, or practice of the brokerage that the employee believes is in violation of a law, or a rule, or regulation mandated pursuant to law.

Supervisors and others are prohibited from engaging in discipline, threats, or discriminatory actions against employees for engaging in whistleblowing activities.

Federal Whistleblower Laws and Rules

The Securities Exchange Act includes Sec. 21F and the SEC has adopted Rule 21F to implement Sec. 21F that provides for reporting possible violation of federal securities laws and potential rewards for information that leads to successful enforcement of a covered judicial or administrative action where monetary sanctions equal $1,000,000 or more. The Sarbanes-Oxley Act of 2002 (which governs public companies) and the Foreign Corrupt Practices Act (FCPA) also have whistleblower provisions.

Annual Review and Periodic Testing

The CCO conducts at least annual reviews of the Safeguards Program, including the incident response procedures, service provider oversight, and disposal practices. The review includes assessing the adequacy of controls, the effectiveness of the Firm's technologies, the results of any testing, and the Firm's compliance with its notification obligations.

The Firm updates its procedures as necessary to reflect technological developments, regulatory changes, identified risks, or lessons learned from the security event.

Opt-Out Notice

If we arrange a joint marketing arrangement with another financial institution or non-affiliated third parties, we will notify the customer in writing and allow them to Opt-Out of the sharing of their personal, non-public financial information. If they decide to Opt-Out, the request may be made in writing addressed and mailed to: Brown & Brown Securities Inc., 6440 North Central Expressway, Suite 107 Dallas, TX 75206 or may call our main office and request that we send our Opt-Out Request Form.

Updating/Correcting Customer Personal Data

If your personal data or account information is incomplete, inaccurate, or outdated, please contact registered representative or our main office by calling (214) 696-1768.