Privacy Policy / Regulation S-P

GWM views protecting its customers' private information as a top priority and, pursuant to the requirements of the Gramm-Leach-Bliley Act (the "GLBA"), GWM has instituted the following policies and procedures to ensure that customer information is kept private and secure.

This policy serves as formal documentation of GWM's ongoing commitment to the privacy of its customers. All employees will be expected to read, understand, and abide by this policy and to follow all related procedures to uphold the standards of privacy and security set forth by GWM. This Policy, and the related procedures contained herein, is designed to comply with applicable privacy laws, including the GLBA, and to protect nonpublic personal information of GWM's customers. Appendix A addresses specific policies in regard to Information Security protocols.

In the event of new privacy-related laws or regulations affecting the information practices of GWM, this Privacy Policy will be revised as necessary and any changes will be disseminated and explained to all personnel.

Scope of Policy
This Privacy Policy covers the practices of GWM and applies to all non public personally identifiable information (PII) of our current and former customers.

Overview of the Guidelines for Protecting Customer Information
In Regulation S-P, the Securities and Exchange Commission (the "SEC") published guidelines, pursuant to section 501(b) of the GLBA, which address the steps a financial institution should take in order to protect customer information. The overall security standards that must be upheld are:

- Ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Employee Responsibility

- Each employee has a duty to protect the nonpublic personal information of customers collected by GWM.

- No employee is authorized to disclose or use the nonpublic information of customers on behalf of GWM.
- Each employee has a duty to ensure that nonpublic personal information of GWM's customers is shared only with employees and others in a way that is consistent with GWM's Privacy Notice and the procedures contained in this Policy.
- Each employee has a duty to ensure that access to nonpublic personal information of GWM's customers is limited as provided in the Privacy Notice and this Policy.
- No employee is authorized to sell, on behalf of GWM or otherwise, nonpublic information of GWM's customers.
- Employees with questions concerning the collection and sharing of, or access to, nonpublic personal information of GWM's customers must look to GWM's CCO for guidance.

Violations of these policies and procedures will be addressed in a manner consistent with other Company disciplinary guidelines.

Types of Permitted Disclosures – The Exceptions

Regulation S-P contains several exceptions, which permit GWM to disclose customer information (the "Exceptions"). For example, GWM is permitted under certain circumstances to provide information to non-affiliated third parties to perform services on GWM's behalf. In addition, there are several "ordinary course" exceptions, which allow GWM to disclose information that is necessary to effect, administer, or enforce a transaction that a customer has requested or authorized. A more detailed description of these Exceptions is set forth below.

- Service Providers. GWM may from time to time have relationships with nonaffiliated third parties that require it to share customer information in order for the third party to carry out services for GWM. These nonaffiliated third parties would typically represent situations where GWM or its employees offer products or services jointly with another financial institution, thereby requiring GWM to disclose customer information to that third party. Every nonaffiliated third party that falls under this exception is required to enter into an agreement that will include the confidentiality provisions required by Regulation S-P, which ensure that each such

nonaffiliated third party uses and re-discloses customer nonpublic personal information only for the purpose(s) for which it was originally disclosed.

- Processing and Servicing Transactions. GWM may also share information when it is necessary to effect, administer, or enforce a transaction for our customers or pursuant to written customer requests. In this context, "Necessary to effect, administer, or enforce a transaction" means that the disclosure is required, or is a usual, appropriate, or acceptable method.
- To carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the consumer's account in the ordinary course of providing the financial service or financial product.
- To administer or service benefits or claims relating to the transaction or the product or service of which it is a part.
- To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the consumer or the consumer's agent or broker; or
- To accrue or recognize incentives or bonuses associated with the transaction that is provided by GWM or any other party.

Sharing as Permitted or Required by Law

GWM may disclose information to nonaffiliated third parties as required or allowed by law. This may include, for example, disclosures in connection with a subpoena or similar legal process, a fraud investigation, recording of deeds of trust and mortgages in public records, an audit, or examination, or the sale of an account to another financial institution.

GWM has taken the appropriate steps to ensure that it is sharing customer data only within the above noted Exceptions. GWM has achieved this by understanding how GWM shares data with its customers, their agents, service providers, parties related to transactions in the ordinary course or joint marketers.

Safeguarding of Client Records and Information

GWM has implemented internal controls and procedures designed to maintain accurate records concerning customers' personal information. GWM's customers have the right to contact GWM if they believe that Company records contain inaccurate, incomplete, or stale information about them. GWM will respond in a timely manner to requests to correct information. To protect this information, GWM

maintains appropriate security measures for its computer and information systems, including the use of passwords and firewalls.

Additionally, GWM will use shredding machines, locks and other appropriate physical security measures to safeguard client information stored in paper format. For example, employees are expected to discard documents not required to be kept by placing them in the appropriate bin for shredding.

GWM protects confidential client information including but not limited to consumer report or any compilation of consumer report information derived from a consumer report by maintaining some information in locked areas and shredding such information when information is no longer needed by GWM.

Security Standards

GWM maintains physical, electronic, and procedural safeguards to protect the integrity and confidentiality of customer information. Internally, GWM limits access to customers' nonpublic personal information to those employees who need to know such information in order to provide products and services to customers. All employees are trained to understand and comply with these information principles.

Privacy Notice

GWM has developed a Privacy Notice, as required under Regulation S-P, to be delivered to customers initially and on an annual basis. The notice discloses GWM's information collection and sharing practices and other required information and has been formatted and drafted to be clear and conspicuous. The notice will be revised as necessary any time information practices change. A copy of GWM's Privacy Notice is available on GWM's website in PDF format.

- Privacy Notice Delivery
- Initial Privacy Notice – As regulations require, all new customers receive an initial Privacy Notice at the time when the customer relationship is established, for example on execution of the agreement for services.
- Annual Privacy Notice – The GLBA regulations require that disclosure of the Privacy Policy be made on an annual basis. GWM will deliver its annual Privacy Notice in conjunction with the annual offer summary of material changes of its Form ADV Part 2.

Revised Privacy Notice – Regulation S-P requires that GWM amend its Privacy Policy and distribute a revised disclosure to customers if there is a change in GWM's collection, sharing, or security practices.

Appendix A: Information Security Policy

The SEC has adopted amendments to the rule under Regulation S-P requiring Registered Investment Advisers adopt policies and procedures to address administrative, technical, and physical safeguards (the "Safeguard Rule") for the data security, integrity and confidentiality of customer records and information. The SEC has further required that policies and procedures take reasonable measures to protect against unauthorized access or use of the information in connection with its collection, storage, transmission and disposal (the "Disposal Rule").

To meet the standards of both the Safeguard and Disposal Rule, the Advisor has developed policies and procedures to apply security measures to reasonably safeguard its private client information during its course of ownership and through its disposal, such as shredding physical documents and coordinating with their technology service provider to destroy digital storage devices.

Primary Systems Overview

System	Dual Authentication	Password Requirements (change/reset)	Administrator Remote Control
eMoney	Yes	Yes Policy: 60 days Maximum	Yes
TD Ameritrade	No	No Policy: GWM periodically changes passwords.	No
Salesforce	Yes	Yes Policy: 60 days Maximum	Yes
Dropbox	Yes	Yes Policy: 60 days	Yes
Orion	Yes	Yes Policy: 60 days	Yes

CCO requests all of the above provide their respective privacy policy, as well as a confirmation that they have a cyber security (information protection) policy and Business Continuity policy and that it has been tested (many firms will not provide such policy, but will confirm they have one and it is tested).

Guide Wealth Management – Router and Wi-Fi / Guest Wi-Fi

Guide Wealth Management, LLC employees are permitted to work in the cloud environment from remote locations, provided they are secure in nature. At no time should data be downloaded on to a non-Guide Wealth Management, LLC system, without permission in advance. The following are also required from all employees:

Router requirements

- **Change your router's preset passwords.** Your router also usually comes with a default password. Hackers know these default passwords. So, change yours to something unique, long and complex – think at least 12 characters, with a mix of numbers, symbols and upper and lower case letters.
- **Turn off any "remote management" features.** Some routers offer remote management for tech support. Don't leave these features enabled. Hackers can use them to get into your home network.

Wi-Fi and Hot-Spot Requirements

- **Change your Wi-Fi's preset passwords.** Your Wi-Fi also usually comes with a default password. Hackers know these default passwords. So, change yours to something unique, long and complex – think at least 12 characters, with a mix of numbers, symbols and upper and lower case letters.

Public Wi-Fi

Use of public Wi-Fi should be minimized. When transmitting data over such a network the company provided VPN must be engaged to prevent Man in the Middle attacks and data loss.

Passwords

Passwords should be complex, and generated and stored within the company provided Password Management Systems. GWM uses 1Password for this.

Computer Systems

All Computer Devices should be updated promptly for security patches to operating systems and applications. They should be logged off when an employee walks away; in addition, auto-lock should be set up on the system for no more than 30 minutes. Laptop devices will have remote locator, lock, and wipe software activated.

Mobile Devices

With the permission of the CCO, mobile devices may be used if necessary. If approval is received the following is required:

- **Auto-lock**. The security mode must be set to auto-lock the device.
- **Remote Locator**. You must be able to remotely freeze the device.
- **Pop-ups.** Your device should be set so that confidential information does not pop up on the screen of the device at any time.

Email Protection and File Sharing

Wherever possible, file sharing will be used to share documents that contain confidential information. Employees will share files using a secured file sharing system. We ask our employees to remind clients to use similar measures when they send sensitive data to us. We use G-Suite Drive and Dropbox for file sharing, and some third party vendors such as eMoney, providing that they meet our security standards. In the rare event that a file must be sent via email attachment we insist that GWM employees apply password protection to the attachments.

We ask that employees be watchful when clicking on links and from clients that they are not expecting. If an employee receives a file or link from a client that is unexpected, then the employee should call the client to confirm prior to opening the file.

USB Devices

Use of USB Devices are prohibited unless approved by the CCO and proof of virus scan has been provided.

If approved and confidential information is placed on a USB drive, then the device must be password protected.

Paper Documents

Although Guide Wealth Management, LLC is a paperless office, often clients provide paper documents for us to scan and use in our analysis, those documents should be locked up each night in a drawer to protect the information.

What if a Breach Occurs?

- Notify the CCO immediately.
- Determine what data was breached and if clients were harmed.
- Contact firm attorney. Attorney-client privilege can protect the advisor from sharing too much while determining what happened and how to respond.
- Clearly define that all members of the team, legal and technical, understand their roles and responsibilities.
- Determine if breach needs to be reported to the SEC.

AFFIRMATION: I have reviewed and agree to abide by the above policies and procedures:

Signature: 

Printed Name: Matthew Hague CCO Date: 04/20/2020