REVOLVE
WEALTH PARTNERS

At Revolve Wealth Partners (Revolve), we value your privacy and take seriously our obligation to use and protect your personal information in accordance with applicable laws and regulations, whether you are a prospective client or a client.

Specifically, as a registered investment adviser, we are subject to certain privacy rules promulgated pursuant to the Gramm-Leach-Bliley Act. These rules are highlighted in our Privacy Policy Notice which require Revolve to keep your personal information private.

Accordingly, Revolve agrees not to intentionally share personal information of clients or prospective clients with third parties except for our own business purposes, such as processing your transactions, maintaining your accounts or for our own marketing purposes. Revolve has advised all of its employees who are given access to personal information of prospective clients and clients of the requirements and provisions of this document and of our Privacy Policy Notice.

Please find our Privacy Policy Notice enclosed with this letter. We encourage you to review this notice closely and let us know if you have any questions.

Sincerely,

Michael Israel & Daniel Katz
Managing Partners

Enclosures: Privacy Policy Notice

Privacy Policy Notice

Rev. [April, 2017]

FACTS	WHAT DOES REVOLVE WEALTH PARTNERS, LLC DO WITH YOUR FINANCIAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depends on the product or service you have with us. This information can include: ▪ Social Security number and income ▪ Account balances and assets ▪ Transaction history
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Revolve Wealth Partners, LLC chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Revolve Wealth Partners, LLC share?	Can you limit this sharing?
For our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes – to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	Not Applicable
For our affiliates' everyday business purposes – information about your transactions and experiences	No	Not Applicable
For our affiliates' everyday business purposes – information about your creditworthiness	No	Not Applicable
For our affiliates to market to you	No	Not Applicable
For nonaffiliates to market to you	No	Not Applicable

Questions?	Call (201) 373-2163 or go to www.revolvewealth.com

REVOLVE WEALTH PARTNERS

Who we are	
Who is providing this notice?	Revolve Wealth Partners, LLC

What we do	
How does Revolve Wealth Partners, LLC protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and building.
How does Revolve Wealth Partners, LLC collect my personal information?	We collect your personal information, for example, when you: ▪ Open an account ▪ Deposit money ▪ Seek advice about your investments ▪ Enter into an investment advisory contract ▪ Tell us about your investment or retirement portfolio or earnings We also collect your personal information from other companies.

Definitions	
Affiliates	Companies related by common ownership and control. They can be financial and nonfinancial companies. ▪ *We have no affiliates.*
Nonaffiliates	Companies not related by common ownership and control. They can be financial or nonfinancial companies. ▪ *We do not share with nonaffiliates so that they can market to you.*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or service to you. ▪ *We do not jointly market.*

SECURITY

Information Security Controls Overview

At eMoney, it's our mission to revolutionize the way trusted advisors serve the needs of their clients and enable them to succeed by providing knowledge, systems and tools to support the "next generation" of trusted advisors. We realize that fulfilling this mission requires constant attention to the security of our clients' information. eMoney has designed and implemented a robust information security program intended to ensure the confidentiality, integrity and availability of this information.

This overview provides information regarding security practices and controls we use to ensure that data is safe and secure.

CORPORATE GOVERNANCE, OVERSIGHT & POLICIES

We maintain a robust and comprehensive set of Formal Security policies including, but not limited to:

- Access control
- Privacy and confidential information handling
- Encryption
- Security incident management
- Secure development life-cycle
- Awareness and education
- Vendor oversight
- Business continuity and disaster recovery

These policies are reviewed by the eMoney Executive Team on a regular basis to ensure that they are responsive to technological advances, trends and changes in the threat landscape.

SECURE DEVELOPMENT PRACTICES

The eMoney platform was developed and is administrated internally. We maintain a robust set of practices around our application development process and various data environments. Important elements of our development process include:

- Physical and logical separation of development, testing, and production environment
- Manual and automated code analysis
- Restricted physical and logical access to the production environment
- Internally and externally conducted penetration and code analysis scans
- A formal change management process to effectively manage any platform changes
- All access to production servers and databases audited and reviewed by management on a regular basis
- No use of shared or generic IDs. Each individual is uniquely identified and accountable for actions that occur within their ID.

HUMAN RESOURCES & ACCESS CONTROL

Information Security and Human Resources coordinate to ensure that security processes related to both areas work together effectively and efficiently.

- As a requirement for employment, all employees submit to a background check. This process includes employment verification, criminal and credit checks, and drug screening.
- Every employee is required to participate in security awareness training upon hire and annually thereafter.
- All eMoney employees are required to confirm their understanding and acceptance of a Non-disclosure agreement and eMoney's formal policies.
- eMoney has implemented a formal security incident response plan to respond appropriately to any suspected incidents. All eMoney staff are provided training in how to identify and properly report any suspected breach of confidential information.

DATA LEAKAGE CONTROL

eMoney has several controls in place to mitigate the potential for sensitive data leakage from the corporate environment. These include:

- Solutions to control and prevent unauthorized access, enforce restriction of removable media such as USBs, and to detect or prevent the transmission of sensitive data.
- Data is encrypted at rest and in transit, as well as encryption of all end-point devices using the AES 256-bit standard encryption.

Effective information security controls naturally evolve over time. With the layers of controls discussed in this document, we feel confident that we successfully address today's threat landscape.

Good security is a shared responsibility and often involves coordination and cooperation among organizations. We look forward to working with other organizations and customers as we strive to grow our business and fulfill our mission.

INFRASTRUCTURE CONTROLS

Infrastructure devices are the backbone of any corporate network, and we have controls in place to help protect this vital part of our network.

- We co-locate our infrastructure in geographically dispersed data centers in Valley Forge, PA & Las Vegas, NV.
- Physical access at the hosting data centers is limited to authorized personnel and requires multiple levels of authorization.
- The eMoney platform offers a 99.5% availability with a 24 hour Recovery Time Objective (RTO) and a 4 hour Recovery Point Objective (RPO).
- eMoney maintains a formal Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP). eMoney's DRP and BCP are validated by management and tested annually.
- The eMoney platform is continuously monitored for security and availability.
- eMoney's infrastructure at the primary and secondary data centers are fully redundant. Disk-to-disk data backups are completed electronically and stored at our secondary data centers in encrypted format.

VENDOR OVERSIGHT

We conduct Security due diligence on all third-parties. Third Parties that have access to sensitive information are considered high-risk and are assessed annually.

THIRD-PARTY VALIDATION

- We use third-party providers to validate security controls. eMoney Advisor conducts annual penetration testing as well as annual Web/Application Security Assessments.
- eMoney completes an annual SOC2:Type2 Assessment and received a clean opinion for this testing period (since 2014).

Black Diamond®

Corporate security, privacy, and business continuity

Corporate privacy

SS&C Technologies and its Advent and Black Diamond business units understand the importance of preserving the privacy and confidentiality of client and partner data. This bulletin provides notice and guidance to Black Diamond clients about the practices and principles used in the collection, use, maintenance, and release of client information.

Privacy statement for SS&C:
https://www.ssctech.com/about-us/privacy

Privacy statement for SS&C Advent and Black Diamond:
https://www.advent.com/about-us/privacy-policy

Privacy principles at Black Diamond

To support its privacy goals, Black Diamond has implemented company programs and policies covering privacy, security, conduct, and ethics. Black Diamond's privacy goals also include implementing agreements with vendors, customers, and employees that are designed to protect non-public personal information including non-disclosure agreements, protective commercial agreements, and data sharing authorizations.

Black Diamond has also implemented administrative, technical, and physical safeguards to help protect private data against anticipated threats and hazards, and unauthorized access. Black Diamond has procedures in place to help support these privacy objectives and protect non-public personal information and private employee data. These procedures are designed to be consistent with applicable state and federal regulations, such as the Gramm-Leach-Bliley Act and MA-201-CMR-17, and applicable European Union privacy regulations and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

Black Diamond takes reasonable steps to retain vendors and service providers that are capable of reasonably maintaining appropriate security measures to protect non-public personal information. Such steps may include reference checks and using our internal audit and security teams to conduct reviews of operations to verify that reasonable design and security principles have been included.

Information collected

In the normal course of operations, Black Diamond collects confidential and non-public information about our clients that is necessary to understand, meet and support the needs, requests, and administration of client accounts. Black Diamond collects the following data:

- Information received from clients through Black Diamond's web-based application and related agreements, applications, or other documentation
- Information transmitted to and received by Black Diamond from any interface source, on the client's behalf, through applications or other forms
- Information received from third-parties, such as custodians, financial advisors, financial institutions, and credit or service bureaus
- Other information including, without limitation, account numbers, names, and balances, as well as names and addresses, depending on the services for which Black Diamond is engaged

Disclosure of client information

Black Diamond provides client Information, including non-public personal information, to outside parties and service providers only as necessary to provide products and services to clients and to complete requested transactions or services. Black Diamond does not sell or otherwise intentionally disclose any client information to third parties for their independent use.

- Black Diamond may disclose client Information under, but not limited to, the following circumstances:
- When requested by a client
- When necessary, in the opinion of Black Diamond, to verify or complete a client-initiated transaction
- When complying with law, regulation, or a court or government order or request
- In connection with obtaining technical or functional assistance from Black Diamond's affiliates

Information security

On a daily basis, Black Diamond receives confidential information associated with the investments and strategies of our clients and the accounts, investments, positions, and transactions of the clients of our clients.

Access control

- Black Diamond incorporates the principle of least-privilege to limit access to client information only to personnel who need it to provide services to our clients.
- Based on Black Diamond's functional design, Black Diamond assigns its employees who have access to client data to one of the following roles:
  (1) Read-Only, (2) Operational, and (3) Administrative.
  A. **Read-Only access** is granted to employees who need information from the website, but are constrained from editing its content.
  B. **Operational access** is granted to employees involved with the daily receipt and reconciliation of data and the calculation and publication of associated performance returns. Operational employees also have limited access to manage data pursuant to their functional area.
  C. **Administrative access** is limited to designated Black Diamond Technology staff, and supporting product specialists, and provides access to all functional areas of Black Diamond's application and its supporting platforms.
- Black Diamond applies a group of policies to protect against unauthorized changes to the production environment.
- The use of privileged accounts to access the production environment is limited to a small number of Black Diamond staff. Inactive accounts are disabled and require Administrative intervention for reactivation.

Authentication

Black Diamond offers customers the ability to use multi-factor authentication (MFA) when accessing the latest release of the Black Diamond web platform.

Multi-factor authentication is required for all Black Diamond staff when connecting remotely to the production environment.

By default, user accounts will be logged out of their web platform session after a specified period of inactivity.

Passwords are stored using a one-way uniquely salted hash and complexity requirements are configurable by the customer, including length, age, history and character limits.

Single sign-on can be supported to offer clients a seamless sign-on experience.

Firm administration

- The Black Diamond platform allows designated firm administrators granular control over user account management and access for their users.
- **Investor communications:** The Black Diamond Investor Experience provides functionality to assist with the distribution of end-client communications. Black Diamond's systems can automatically send copies of emails to designated email addresses such as a client's compliance department. Black Diamond does not currently provide a stand-alone regulation-compliant archiving system.
- **Document vault:** Clients may restrict their own firm's team member's access to their files in the Black Diamond Document Vault and control the downloading or uploading of content. For support purposes, only designated Black Diamond technology staff with administrative access can review file content, if needed.

Personnel security

- Black Diamond employees are obliged to comply with corporate policies and procedures regarding client confidential information.
- Employees are periodically reminded about the importance of maintaining the confidentiality of data received from clients, including a signed confidentiality agreement that prohibits unauthorized disclosures of confidential information.
- SS&C delivers periodic security awareness communications with material covering privacy and security topics that include physical security, data security, phishing attempts, malware prevention, data handling, and device security.

Application development security

- Black Diamond follows a secure Software Development Lifecycle (SDLC) to identify and fix vulnerabilities found within its web applications and APIs.
- As part of the build process for major releases, static code analysis is conducted with the results reviewed by Development and Security personnel.
- Black Diamond secures its source code through a version-controlled repository that is physically and logically isolated from other infrastructure networks.

Vulnerability and penetration testing

- Black Diamond utilizes internal staff and external specialists to conduct application-level security testing, which includes penetration testing and network vulnerability tests at least annually. Management ensures test results and remediation plans are tracked to resolution.

Change management

- Change Management Process: Black Diamond enforces a change management process to track and control changes to the production environment. Although the elements of the process are applicable to any requested changes, the implementation steps vary depending upon whether the requested changes are related to product functionality or to data:

  A. **Departmental approval:** All changes must be approved by the supervisor of the requesting employee.

  B. **Development/product approval:** Requests for new development and changes to the existing product are presented to Product Development senior management for approval.

  C. **Testing:** Changes are validated in a testing environment before being released to production. The Product Manager is responsible for overseeing the testing and release.

  D. **Documentation:** Changes are tracked by Black Diamond's internal, web-based workflow management system. Required information includes a description of the change, associated stakeholders, and pertinent operational information. A number is assigned to the request and it is tracked until released.

  E. **Review:** Change requests are reviewed at regular product meetings involving the appropriate levels of management.

Encryption

- Black Diamond uses encryption-in-transit to help secure the communication between the user's browser and Black Diamond's servers. A combination of Transport Layer Security (TLS) with 2048-bit encryption keys and SHA256 signed certificates facilitate these connections.
- Black Diamond uses encryption-at-rest to help secure data stored directly on Black Diamond's servers with key management technology incorporating AES-256.
- Developments in cryptography are monitored to keep Black Diamond's encryption practices in line with industry guidance to help maintain the confidentiality and integrity of data access and connections.

Network security

- The Black Diamond systems at the data center utilize firewalls and load balancers in a redundant environment with intrusion detection systems (IDS) that are monitored automatically 24/7/365.
- Firewalls are configured to deny all traffic unless explicitly required by the application. Firewall configurations proceed through the Change Management Process and are reviewed by the Infrastructure team.
- Firewalls are configured to log unauthorized access attempts and the logs are periodically reviewed by the Network Team.
- Physical and logical network segmentation is implemented to separate Production data from Development and QA environments as well as Internet and non-Internet facing servers to minimize external exposure.
- Computers are outfitted with centrally managed endpoint protection technology.
- Black Diamond, in association with SS&C's security team, periodically review the existing security infrastructure to recommend and implement improvements.

Data integrity

- Black Diamond takes multiple steps to protect the integrity and confidentiality of the custodial data it receives from its trusted partners.
- Data transmissions from custodians use encrypted files or encrypted communications channels.
- An automatic daily reconciliation process checks for corrupt/incorrect custodian data. Manual checks are performed prior to custodian data being reconciled.

Security incident process

Black Diamond enforces policies and procedures reasonably designed to address and mitigate the potential impact of any compromise of confidential information.

- **Reporting:** In the event of a confirmed compromise or a threat to compromise Confidential Information, the matter will be reported promptly to the security team and management.
- **Response:** Upon notice, the security team and management will research the situation to understand its potential impact, and then promptly implement incident response actions to address the threat and mitigate its effects. Simultaneous with the implementation of action items, the incident response team will assess the appropriate communication protocols.
- **Communication:** At the earliest reasonable opportunity (and after sufficient information has been obtained regarding the cause of the threat, the extent of its effects, and the appropriate response), the incident response team will provide necessary personnel with an appropriate communication.
- **Post-event assessment and prevention planning:** Upon resolution and completion, the incident response team will assess the threat and its effects on clients and Black Diamond operations, evaluate measures to avoid similar threats, and implement a prevention plan.

Former customers

- If a service relationship between Black Diamond and a client is discontinued, Black Diamond will continue to adhere to the policies and practices described in our current Privacy Policy and will retain all collected client information in accordance with the terms of the client's contract.

Office facility security

- The Black Diamond corporate office suite in Jacksonville is equipped with an access control system that logs door entry activity and an alarm system that is monitored 24/7/365.
- The Jacksonville office property management provides building guards, secure perimeter doors and elevators, and controlled after-hours access.
- Sensitive and confidential paper documents awaiting destruction are stored in secure locked boxes until shredded.
- Time-based screen lockouts are configured on employee desktop computers and laptops to activate automatically after a prescribed period of inactivity.

Data center security

Black Diamond's IT infrastructure and business applications are currently being hosted in two geographically separate data centers. SS&C's Yorktown Heights data center in New York State provides hosting services for the production environment while Flexential in Jacksonville, Florida supports the disaster recovery systems. Both data centers use resilient infrastructure that is intended to be reliable and secure in the event of a survivable local natural disaster or other comparable catastrophic event. SS&C and Flexential periodically engage an independent audit firm to review their operating controls.

SS&C Yorktown Heights

Yorktown Heights: General facility features

- Closed circuit television ("CCTV")
- NYSEG power grid
- N+1 Generators with multi-day fuel capacity
- Enterprise class N+1 UPS & N+1 PDU electricity distribution
- Redundant heating, ventilation and air-conditioning (HVAC) systems
- Onsite technical support services

Yorktown Heights: Network infrastructure

- Network monitoring that includes 24×7 support from multiple office locations
- Network configuration changes are subject to a Change Management and System Review process
- Utilizes a network-based IDS
- Redundant network design supports failover and load balancing to minimize any downtime

Yorktown Heights: Physical security

- Physical access is limited, requires approval from Management, and is periodically reviewed
- A centralized computer keycard system which includes biometric checks is used to control access to the data center
- Vendors, contractors, and other authorized visitors require prior approval and an escort
- 24×7 on-site security guards

Flexential Jacksonville data center

Flexential: General facility features

- 24/7/365 Network Operations Center
- Customer Access with 24-hour staff and security
- Controlled Temperature and Humidity
- Enhanced Storm Protection

Flexential: Redundant network infrastructure

- Onsite backup power generator
- Comprehensive fire suppression systems
- Multiple Internet/Network Access Options
- Redundant Internet access

Flexential: Facility security

Each Flexential facility is engineered with five levels of security:

Level 1: Proximity card access with PIN is required to enter the building (but not the data center secured floor area)

Level 2: Proximity card access with Biometric (fingerprint) scan is required to enter the data center secured floor area

Level 3: All hardware is secured in a locked cage or steel mesh cabinet fitted with combination locks

Level 4: Video surveillance cameras are placed throughout the facility

Level 5: Staffed 24/7/365

Business continuity and disaster recovery

Black Diamond maintains a business continuity and disaster recovery program to establish the processes, procedures, and protocols to follow in the event of a natural disaster or other catastrophic event, and to help reestablish critical operations and support functions. The program is guided by documented plans such that in the event of a disaster, teams will be in place to coordinate personnel and enable sufficient level of functional recovery.

Black Diamond operations

Black Diamond has developed contingency plans to address the impacts that natural disasters and other catastrophic events can have on our office environment. Since Black Diamond services are web-based, the goal is for key personnel to have access outside of our office to the network through VPN so they can resume normal operations from alternate locations to minimize service disruption. The primary remote VPN access point for Black Diamond is Yorktown Heights with San Francisco acting as a redundant west coast access point.

It is Black Diamond's goal to have the network infrastructure, including VPN remote services, be one of the early IT elements to be restored. However, several important SaaS and TLS-secured systems are expected to be available without a dependency on the state of the VPN. To the extent possible, personnel will be encouraged to work out of a home office for the time needed to repair or replace an impaired local office.

If a scenario occurs that would disrupt ongoing office functions for an extended period of time, Black Diamond will relocate key personnel (client advocates, operations analysts, implementation managers, and others) to an alternate location. This allows these resources to be fully operational with access to Black Diamond's proprietary systems, the Internet, email, and telephone.

As a generally accepted good practice, Black Diamond tests its Business Continuity and Disaster Recovery plan on at least an annual basis.

Recovery objectives

Black Diamond's goal is to achieve a 24-hour Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for all services considered business-critical. This includes the Black Diamond Production Web Presence, hosted at the SS&C Yorktown Heights Data Center in New York as well as its redundant facilities at Flexential in Jacksonville, Fl. All services hosted that are delivered from Black Diamond's corporate office are supported by routine backups, completed and stored offsite, and available for use at a recovery facility. The Recovery Point Objective is the last recoverable backup with a focus on the most critical functions first. For example, recovering the ability to transact might require 24 hours but reloading historical data may need 72 hours. Black Diamond's Continuity Plan also includes methods for timely and continual communications to clients, employees, and vendors regarding Black Diamond's operations.

Attainment of Service Organization Controls Report (SOC-1)

Since October 2013, Black Diamond has conducted an annual examination process with an independent audit firm to obtain a SOC-1 report.

The SOC-1 report evaluates Black Diamond as a service organization and provides supporting documentation for our clients' internal and external audits, risk assessments, and regulator examinations. The report includes information on Black Diamond's product development, data and client privacy practices, operational processes, business continuity approach, personnel management, and other vendor viability information. The report is available upon request.

About Black Diamond

Black Diamond provides investment advisors and wealth managers with a cloud-based portfolio management platform offering aggregation, customizable reporting and rebalancing combined with fully outsourced daily reconciliation and data management service. With innovative technology backed by exceptional service, Black Diamond frees advisors to focus on serving clients and growing their business. Over 1400 advisory firms have chosen Black Diamond to help manage over one trillion dollars in assets. Learn more at blackdiamond.advent.com.