Our Policies That Help Protect Our Clients Against Identity Theft

OPPENHEIMER

Oppenheimer's Information Technology, Legal, Compliance and Operations departments along with our Private Client Division have created a robust, multi-layered set of policies against cyber-crime designed to help protect clients and prospective clients.

Information Technology Procedures

The Firm's network and website are monitored at all times, both by our own information technology professionals and independent consultants.

The Firm maintains anti-virus and spam software and routinely runs data loss prevention and monthly network penetration tests to help us ensure that our client's accounts are safe and secure. Additionally, the Firm has developed Cyber Security Policies and Procedures and follows the NIST (National Institute of Standards and Technology) framework recommended to mitigate any cyber risks posed to the Firm and to our clients.

Oppenheimer client information is processed and stored with a high level of security and care in accordance with our industry requirements. The Firm has proactively installed software that monitors electronic communication; this software is designed to prevent the mailing of any e-mail that contains social security numbers and Tax ID numbers, thus protecting client's personal information.

Employee/Operational Procedures

Oppenheimer employees seek to ensure the confidential and secure handling of customer information, assets and transactions. The Firm's employees and our affiliates' employees are required to report any suspected identity theft immediately. Registered employees receive additional training to help identify and respond promptly to "Red Flags," or potential threats. An employee who has reasonable belief that a client account has been accessed without authorization must notify management immediately. All reasonable attempts are made to phone the client immediately (via the number on record). The employee who noticed the Red Flag will complete and submit the "Suspected Identity Theft Incident Report" to Oppenheimer's General Counsel and Chief Compliance Officer.

How We Process Fund Disbursements

Firm procedure requires employees to obtain written instructions from a client before funds are disbursed by check unless the disbursement is (1) made payable to the account owner of record and (2) intended to be sent to the account owner's primary address of record. In addition, if we receive an e-mail request for the disbursement of funds to a third party, Oppenheimer requires a phone call to be made to the phone number we have on record. Furthermore, if funds are distributed from an account to a payee other than the account holder, or if they are to be delivered to an address other than the primary account address, the Firm's operating system automatically generates a notice detailing that disbursement and sends the notice to the account address on file.

Processing Trade Instructions

Oppenheimer will only accept orders from the account owner of record. In order for Oppenheimer to take instruction concerning trades, but not money movement, from an individual or entity other than the account owner or authorized signatory of an entity, the account owner is required to sign and have notarized either Oppenheimer's Limited Trading Authorization or provide an outside Power of Attorney executed in compliance with relevant statutes. Moreover, an authorized agent must sign and have notarized Oppenheimer's Power of Attorney Affidavit. Furthermore, before providing account information to a third party, subject to the exceptions noted in Oppenheimer's Privacy Notice, Oppenheimer requires the account owner's express written consent.

What If Your Identity Has Been Compromised?

Identity thieves have the expertise to hack into e-mail accounts and use that means to possibly request payment from Oppenheimer brokerage accounts to non-client-controlled accounts. After the suggestion of an identity theft concern, Firm policy requires that a Financial Advisor or his or her Client Service Associate contact the client by phone to investigate whether there have been other attempts at identity theft. His or her accounts will go on heightened supervision and trades may be temporarily blocked for the client's protection.

Oppenheimer is also minimizing the impact of identity theft for clients by:

- Offering to change the account's password or other means of access;
- Offering to close the account and reopen it with a new account number;
- Assisting the client to work with the FTC Identity Theft Web Site to minimize the effects of identity theft.

Oppenheimer will only release account information to authorized third parties such as government agencies.