Identity Theft Prevention / Red Flag Policy

Policy Objectives

The purpose of the Strong Investment Management's Identity Theft Prevention/Red Flag Policy is to define Strong's responsibilities in detecting, preventing, and mitigating identity theft as required by the Federal Trade Commission (FTC) under the Fair and Accurate Credit Transactions (FACT) Act. The rule adopted by the FTC is referred to as the "Red Flag Rule."

Policy Scope

All employees, temporary workers, and contractors of Strong Investment Management and its affiliates are responsible for adhering to this policy.

Policy Owner

The Strong Investment Management chief security and privacy officer is responsible for administering this policy.

Responsibilities

Strong Investment Management takes seriously its regulatory responsibilities and all reports of identity theft will be investigated and acted upon, up to and including the involvement of law enforcement agencies, when needed.

All employees are required to receive regular training in identity theft prevention and red flag procedures. This training includes but is not limited to the new-hire training process.

Business units are responsible for maintaining procedures to identify red flags and monitor accounts that have been flagged as being potentially linked to instances of identity theft. Department management is responsible for performing regular identity theft risk assessments and updating related procedures, as necessary.

Examples of identity theft prevention procedures:

- Obtaining identifying documents from new clients
- Monitoring account transactions
- Verifying the validity of address changes

The executive risk committee assigns specific responsibility for implementation of the red flag program, approves material changes, and reviews staff reports of identity theft. The executive risk committee reports no less frequently than annually on status to the firm's Board of Directors.

Reporting Procedures

If you are a client of Strong Investment Management, and feel you may be a victim of identity theft, please contact your financial advisor.

Any suspicion or incident of identity theft discovered by Strong Investment Management staff or advisors must be promptly reported to the ERM department via the security incident hotline at (949) 759-9686.

How Strong Investment Management Secures Your Information

To protect your information and assets, Strong Investment Management employs extensive physical, technical, and procedural security controls at all of our facilities. We actively monitor and enforce compliance to our security policy and its related procedures. We regularly review, update, and modify our policies and procedures to respond to new threats and to adapt to changes in technology.

Strong employees and customers receive thorough training in our security policy and are held accountable for adhering to the policy. Employees who work directly with customers also receive training in other related risks, such as identity theft.

Although we cannot fully disclose all that we do to protect the personally identifiable information of our customers, here are just a few measures we take:

- We employ strong authentication and password protocols.
- We enforce inactivity timeouts on our computers.
- We maintain and regularly test our firewalls.
- We continuously update our anti-virus and anti-malware protection.
- We employ threat monitoring/intrusion detection.
- We have mandatory training for employees, customers, and managed representatives.

Anyone who has questions should contact us at the number above.