FINANCIAL DESIGNS CORPORATION

CyberSecurity and Incident Response Program

SEC REGULATION S-P
PRIVACY OF CONSUMER FINANCIAL INFORMATION

Created by:
Financial Designs Compliance Department
Version August 31, 2026

Index

Table of Contents

IDENTITY THEFT PREVENTION PROGRAM

Introduction

FDC has adopted a program intended to detect red flags and prevent identity theft. As part of its Identity Theft Prevention Program ("ID Program"), the Company will identify red flags and specific risks facing the Company. A red flag is a warning sign that identity theft may be occurring. The Company's ID Program is designed to detect, prevent, and mitigate identity theft in connection with the opening of an advisory account or the management of an existing one.

Associated Persons could be responsible for identity theft through more direct means. Insider access to information could permit a dishonest Associated Person to sell clients' personal information or to use it for fraudulent purposes. Such action is cause for disciplinary action at the Company's discretion, up to and including termination of employment as well as referral to the appropriate civil and/or criminal legal authorities.

Prevention of Identity Theft

As part of their fiduciary obligations to clients, Associated Persons shall work diligently to prevent identity theft. Specifically, Associated Persons should take the following preventive measures:

- When providing copies of documents to others who are authorized to view them, Associated Persons shall make sure that non-essential and non-public personal information is either removed or redacted.
- Associated Persons shall shred or otherwise destroy all paperwork containing non-public personal information when disposing of documents.
- Requests for address changes must be verified before sending mail to the new address. Even after a change of address has been verified, Associated Persons shall send confirmation notices to both the new address and the old address. This address change procedure applies to traditional and electronic mailings.
- Associated Persons should be on the lookout for pretext calling. These calls are an attempt to elicit personal information about a client by phone, such as the individual's Social Security number. Associated Persons shall take reasonable steps to confirm the identity of the caller before divulging non-public personal information.
- All written (or emailed) wire transfer requests must be verified by calling the client first and getting their verbal approval. Verbal wire transfer requests must be confirmed by verifying the identity of the client.
- Associated Persons shall zealously guard clients' Social Security numbers and other personal information.
- Files and computers should be secured before Associated Persons leave their work areas.
- Hard drives should be scrubbed or destroyed before computers are discarded.

The Company has also implemented a written information security program. See the Information Security Program section of FDC's Compliance Manual.

Red Flags That May Indicate Identity Theft

Associated Persons should be vigilant for identity theft red flags, which fall into five broad categories:

- Alerts, notifications, or other warnings received from consumer reporting agencies and service providers, including fraud detection services
- Presentation of suspicious documents that appear to be altered or forged
- Presentation of suspicious personal identifying information
- Unusual activity in a covered account or other suspicious activity
- Notification from customers, identity theft victims, law enforcement, or other persons related to covered accounts held by the Company

In addition, Associated Persons should always be on the alert for specific red flags such as:

- Identification documents appear to have been altered or forged.
- An individual falsely claims to be a person who is known to an Associated Person.
- Photo IDs are inconsistent with the person's appearance.
- Other identification is not consistent with the information provided by the person who opened the account.
- Other information on the identification is not consistent with readily available information in the Company's files, such as a signature on a recent check.
- The identification does not look genuine.
- The individual's address and/or phone number have changed suddenly.
- The new address is a post office box.
- There is unusual account activity, such as larger than normal withdrawals.
- The person begins communicating in a new manner, such as an elderly client who begins sending emails instead of calling.

This list of red flags is not exhaustive. FDC will identify other red flags as it learns of new identity theft risks.

Associated Persons should be especially alert if a client has notified the Company of a previous identity theft occurrence, or there has been a prior attempt to infiltrate the person's online accounts.

Response When Red Flags are Detected

Associated Persons should be proactive in response to the detection of red flags. Depending upon the facts and circumstances, including the level of identity theft risk, Associated Persons may respond accordingly with measures such as:

- Monitoring a covered account for evidence of identity theft
- Contacting the customer
- Changing any passwords, security codes, or other security devices that permit access to a covered account
- Closing an existing covered account and reopening with a new account number

- Not opening a new covered account
- Notifying law enforcement

No further action is necessary if an Associated Person has confirmed that a red flag was not indicative of identity theft. Whether or not a red flag is indicative of identity theft, Associated Persons are required to document how they responded to the perceived risk. Associated Persons who encounter red flags should report the incidents to FDC's CCO.

Communicating and Updating the ID Program

FDC will review its ID Program at least annually and update it on an as-needed basis or in response to changes in the kinds of risks facing clients. Identity theft occurrences and security breaches should prompt enhancements and revisions in the Company's policies and procedures. The CCO will approve all revisions to FDC's ID Program.

FDC will conduct a training session at least once per year to educate Associated Persons about identity theft. Associated persons may be subject to disciplinary action for violating the Company's ID Program.

CYBERSECURITY PROGRAM

General

The Company's cybersecurity policies and procedures are designed to

- Identify and control cybersecurity risks;
- Protect the Company's networks and client information;
- Curb risks arising from remote customer access and funds transfer requests;
- Mitigate risks related to vendors and other third parties; and
- Detect and report unauthorized activity on our network.

The Company's CCO serves as Chief Information Security Officer and is responsible for oversight, development, implementation, and administration of this cybersecurity policy.

Relationship to Other Compliance Policies

This policy incorporates by reference other policies intended to protect the firm and its clients from cyber threats, including: Identity Theft Prevention Program; Privacy Policies; Business Continuity Plan; and Written Information Security Program.

Procedures to Prevent Cybersecurity Breaches

Identification of Risks/Cybersecurity Governance

The Company conducts periodic reviews to identify cybersecurity threats, vulnerabilities, and potential business consequences and documents such reviews in its compliance files. The Company has taken the following steps to identify and control risks:

- The Company has prepared a list of all computers, devices and software connected to, or supported through, its internal network. Maintenance of our information technology system is the responsibility of the CCO or his designee.
- Connections to the Company's network from external sources are tracked.
- Log-in and log-out practices are assessed for adequacy, appropriate retention and secure maintenance.

E-mail and Fax Requests to Transfer Funds and/or Securities

The Company verifies e-mail and fax requests to transfer funds and/or securities through the following means:

- An associated person will attempt to contact the client by phone.
- If the associated person cannot contact the client by phone, he/she will attempt to communicate with the client's emergency contact.
- If the request still cannot be verified, the investment adviser representative handling the client's account will review the account history to determine if the circumstances surrounding the transfer are suspicious in view of the client's profile, personal situation, and historical transactions.

If the request cannot be verified and is inconsistent with the client's profile, personal situation, and historical transactions, it will not be honored.

Client Education Program

The Company takes the following steps to educate clients regarding the risks posed by cyber threats:

- Encourages clients to develop more complicated passwords and to change them frequently;
- Warns clients regarding *phishing* e-mails to obtain personal information;
- Alerts clients to be on the lookout for fake wireless hot spots; and
- Notifies clients about the importance of monitoring their accounts for suspicious activity.

The Company retains books and records to demonstrate that these educational efforts were undertaken.

Employee Education Program

The Company provides written guidance and periodic training to employees relating to information security risks and their responsibilities. The Company retains books and records to document the agenda of those training sessions and the topics covered. The Company also retains a list of the employees who attended these training sessions.

Employees are educated on safeguarding resources used for business purposes, such as smart phones and laptop computers.

Smart phones and other electronic devices may not be used to contact clients and prospects without express written authorization from the Company and the communications must be preserved on the Company's server. Encryption software must be enabled when a representative is communicating confidential information.

Antivirus and Antispam Software

The Company utilizes antivirus and antispam software on all fixed workstations and portable electronic devices. Updates are downloaded to the antivirus antispam software on a periodic basis.

The Company regularly updates firewalls. Patches to fix security vulnerabilities are applied in a timely fashion.

Physical Security

All client documents are retained and locked in fire-proof cabinets at the end of each day in the appropriate client file. If there is a reason any additional documents, or copies thereof, having client information on them, are being utilized for worksheet calculations, annual appointments, etc. they must be treated as all other confidential documents. If they are copies, then they must be shredded on-site after they have served their purpose. Simply throwing them away is not acceptable.

Protection of Company Networks and Information

FDC has developed and implemented appropriate safeguards to protect the Company's networks, network storage solutions and data information. To ensure secure delivery of critical infrastructure services and

maintain information security architecture and processes, security procedures are maintained and used to manage protection of information systems and assets. The Company believes these practices will support the ability to limit or contain the impact of a potential cybersecurity event.

The Company restricts access to network resources to the extent necessary to accomplish their business functions. We detect unauthorized access to the firm's network through the following means:

- Utilization of software to detect malicious code on the Company's networks and mobile devices;
- Maintaining statistical baseline information about anticipated events on the Company's network;
- Aggregating and correlating event data from multiple sources;
- Establishing written incident alert thresholds;
- Monitoring the Company's network environment to detect potential cybersecurity events;
- Monitoring the Company's physical environment to detect potential cybersecurity events;
- Monitoring the activity of third party service providers with access to the Company's networks;
- Monitoring the presence of unauthorized users, devices, connections, and software on the Company's networks;
- Evaluating requests initiated remotely to identify potentially fraudulent requests;
- Utilization of data loss prevention software;
- Conducting penetration tests and vulnerability scans; and
- Testing the reliability of event detection processes.

The Company retains books and records to document that what tests were performed and the date on which they occurred.

Specific Safeguard Practices

Access Control

Access to FDC's network, systems and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. User restrictions are applied to network resources as necessary for business functions. At the application and database level, other access control methods may be implemented to further restrict access. The application and database systems limit the number of applications and databases available to users based on their job requirements. All authorized users of the Company's network, applications, and database functions are cataloged. All requests for access are tracked.

Data Classification and Risk Based Controls

Unless it is marked otherwise or clearly intended to be Public Information (defined below), Employees must treat all Company, client and internal information as if it is at least Sensitive Information, regardless of its source or form, including electronic, paper, verbal, or other information.

Highly Confidential: This refers to any data used by FDC or given to FDC by its clients where any breach in confidentiality, integrity or availability could present a serious amount of risk to FDC, its clients, and its clients' affiliates. This includes sensitive customer information, trading data, investment research and financial statements. This data should be treated with the highest level of security. You must protect Highly Confidential Information with specific administrative, physical, and technical safeguards implemented according to risks, including (but not necessarily limited to): (i) only discussing Highly Confidential Information in non-public places, (ii) encryption of Highly Confidential Information, and (iii) only sharing Highly Confidential Information when there is a business purpose.

> *Examples include: Client and employee sensitive customer information, trading strategies, files containing important documents, agreements, statements, and databases containing all trades and accounting details for past several years.*

Sensitive: This refers to all other data that could harm a person's right to privacy or negatively impact FDC in any way. This includes all data that is not made readily available to the public but is not considered confidential.

> *Examples include: Market data research, trading server information, web server data, communications or records regarding internal Company matters and assets, including operational details and audits.*

Public: Any data that does not present any form of harm to the party it belongs to and is not considered classified or restricted.

User System and Network Access – Normal User Identification

All users will be required to have a unique logon ID and password for access to systems. All user passwords and applicable security credentials should be kept confidential and MUST NOT be shared with management and supervisory personnel and/or any other employee at any time. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password must be unique. Do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
- Password should be changed every 120 days.
- User accounts will be frozen after five (5) failed logon attempts.
- Logon IDs and passwords will be suspended after thirty (30) days without use.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting, or modifying a password file on any computer system is prohibited.

Employees who forget their password must call the IT administrator, VC3, to get a new password assigned to their account.

Employees will be responsible for all transactions occurring during logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined below.

Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of FDC.

A terminated employee's physical and electronic access to personal information must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes, or badges, business cards, and the like, that permit access to the Company's premises or information. Moreover, such terminated employee's remote electronic access to personal information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated. The CCO, or CCO designee, shall maintain a highly secured master list of all lock combinations, passwords, and keys.

Network Security

The Company is required to protect and ensure the confidentiality, integrity, and availability of its networks, data and information systems. Security controls are designed and maintained to ensure compliance with all legal and regulatory requirements.

Maintenance

FDC ensures that regular system maintenance and repairs are performed, including timely installation of software patches and updates that address security vulnerabilities.

INCIDENT RESPONSE PROGRAM FOR UNAUTHORIZED ACCESS TO OR USE OF CUSTOMER INFORMATION

Regulation S-P requires investment advisers to adopt programs that are reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including customer notification procedures.

An Associated Person must immediately notify the CCO if he or she becomes aware of an actual or suspected privacy breach, including any improper disclosure of client non-public personal information and/or of the Company's proprietary information. As appropriate, the CCO will:

- Ascertain, with the assistance of service providers as needed, whether an incident occurred;
- If an incident did occur, assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization;
- To the extent possible, categorize the incident based on the sensitivity of the information involved and operational impact;
- Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, the appropriateness of which is dependent on the type of incident and may include isolating compromised systems or enhancing the monitoring of intruder activities, searching for additional compromised systems, changing system administrator passwords, rotating private keys, and changing or disabling default user accounts and passwords, among other interventions;
- Take actions necessary to reduce the potential harm from improper disclosures that have already occurred;
- Discuss the issue with counsel and evaluate individual state reporting requirements;
- Contact regulatory authorities and/or law enforcement officials, where required;
- Notify each affected individual whose "sensitive customer information" was, or is reasonably likely to have been, accessed or used without authorization, unless it is determined, after a reasonable investigation of the facts and circumstances of the incident that occurred that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience;
- Collect, prepare, and retain documentation associated with the breach and the Company's responses, including information about the type of access, the extent to which systems or other assets have been affected, the level of privilege attained by any unauthorized persons, the operational or informational impact of the breach, and whether any data has been lost or exfiltrated along with a post-incident review of events and actions taken, if any; and
- Evaluate the Company's existing privacy protection policies and procedures in light of the breach and make any needed changes accordingly.

Notification to Affected Individuals of Unauthorized Access or Use

The Company will provide a clear and conspicuous notice to each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization,

unless the Company determines, after a reasonable investigation of the facts and circumstances of the incident that occurred that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. The CCO shall determine the scope of the investigation, taking into account (i) whether the incident is the result of internal unauthorized access or an external intrusion, (ii) the duration of the incident, (iii) what accounts have been compromised and at what privilege level and (iv) whether and what type of customer information may have been copied, transferred, or retrieved without authorization. The CCO shall document their findings, including a record of the investigation and the basis for the notification determination.

The notice must be transmitted by a means designed to ensure that each affected individual can reasonably be expected to receive actual notice in writing. The notice and the method of transmission must be pre-approved by the CCO before utilization. Should the Company become aware of new facts regarding the incident, it shall reassess its notification determinations.

The written notice must:

1. describe in general terms the incident and the type of sensitive customer information that was or is reasonably believed to have been accessed or used without authorization;
2. include, if the information is reasonably possible to determine at the time the notice is provided, any of the following: the date of the incident, the estimated date of the incident, or the date range within which the incident occurred;
3. include contact information sufficient to permit an affected individual to contact the covered institution to inquire about the incident, including the following: a telephone number, an email address, a postal address, and the name of a specific office to contact for further information and assistance;
4. recommend that the customer review account statements and immediately report any suspicious activity to the covered institution;
5. explain what a fraud alert is and how an individual may place a fraud alert in the individual's credit reports to put the individual's creditors on notice that the individual may be a victim of fraud, including identity theft;
6. recommend that the individual periodically obtain credit reports from each nationwide credit reporting company and that the individual have information relating to fraudulent transactions deleted;
7. explain how the individual may obtain a credit report free of charge; and
8. include information about the availability of online guidance from the Federal Trade Commission (FTC) and usa.gov regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the FTC and include the FTC's website address (https://www.ftc.gov/) where individuals may obtain government information about identity theft and report suspected incidents of identity theft.

The notice must be sent as soon as practicable, but not later than 30 days, after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred. Upon determination by the CCO, the Company may delay providing notice if the US Attorney General determines that the notice required poses a substantial risk to national security or public safety.

Response Program Requirements Related to Service Providers

Under Regulation S-P, investment advisers are required to maintain oversight of service providers through due diligence and monitoring. The Company requires its service providers who have access to customer information to (i) take appropriate measures to protect against unauthorized access to or use of customer information and (ii) provide notification to the investment adviser as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred resulting in unauthorized access to a customer information system maintained by the service provider. Upon notification, the Company will initiate its incident response program. The CCO is responsible for ensuring that provisions addressing these responsibilities are included in contracts with service providers with access to customer information. The CCO shall also review such service providers on a periodic basis to ensure that they continue to fulfill these obligations.

Training

The Company will provide guidance and periodic training to employees relating to information security risks and responsibilities no less than annually. The Company will retain documentation of the agenda of those training sessions and the topics covered. The Company will also retain a dated list of the employees who received such training.