FINANCIAL DESIGNS CORPORATION

CyberSecurity & Privacy Program

Created by:
Financial Designs Compliance Department
Version 2-2023

Index

Financial Designs Corporation
CYBERSECURITY & PRIVACY PROGRAM

IDENTITY THEFT PREVENTION

Financial Designs Corporation (FDC) takes the security of our client information very seriously. We have endeavored to take every preventive measure possible to insure against any security breaches.

The Department of Homeland Security defines "Sensitive Personally Identifiable Information (PII)" as: *Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.*

This is the defining standard FDC utilizes in approaching security for our clients.

Personally Identifiable Information includes:

- Social Security Number
- Driver License Number
- Passport Number
- Financial Account Number(s)
- Address of Residence
- Date of Birth
- Medical Information

Red Flags

Every staff member has been trained to recognize the red flags indicating a possible identity theft situation and the recourse action if it is found to be true.

- Any email or phone call that has a subject matter out of the ordinary and "urgency" seems to be paramount.

- Any email or phone call that is from an "unknown relative" or "friend" corresponding on behalf of the client.

Document Disposal/Retention

Identity Theft can begin with improper document disposal. Client documents are securely retained for the time limits specified for all Registered Investment Advisors (SEC Rule 204-2). When purged, documents are destroyed utilizing secure document shredding services.

Emails are retained by a secured third-party service (GlobalRelay) and only accessed by the Chief Compliance Officer and authorized FDC staff.

Minimizing Proliferation

All client information is for the sole use of FDC staff members who have a specific purpose to use that information for the facilitation of servicing the client's account(s). Information is only shared with other FDC staff members as necessary to carry out that objective and is not shared with any other entities or individuals.

Securing Sensitive PII

Awareness is always paramount when dealing with client information. To limit the potential for unauthorized disclosure, all staff has been trained to be mindful of their surroundings to protect against "shoulder surfing" or eavesdropping by unauthorized persons.

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.

Electronic Security

When at all possible, faxing PII is avoided in order to protect against unauthorized recipients. Emailing is the preferred correspondence when an email has been verified as secure and correct. Encryption is used to share PII when available by both the sender and the recipient.

As a best practice, the client is cautioned not to send any sensitive PII to FDC in an unsecure manner, including sending it to the general email address where all staff has access.

Remote/Travel Access

Sensitive PII should only be accessed or transferred by phone, laptop or flash drive when necessary, and extreme caution should maintained to keep the device secure (car, hotel room, airport, etc.)

Privacy Incident Reporting

All incidents of a privacy breach, whether suspected or confirmed, is to be reported by FDC staff to their supervisor immediately. A full detailed report of the incident is required including the content of the information at risk.

Compromised information should not be reported utilizing any method that would further compromise the data to unauthorized persons, e.g. sending it to a supervisor via email where there is a possibility of an unauthorized person reading the email.

* S*ee "Procedure for Managing a Privacy Breach" in the FDC Compliance Manual*

Summary of Protecting PII at Financial Designs Corporation

- Physically securing sensitive PII (in a locked drawer, cabinet, desk, etc.) when not in use or not otherwise under the control of a person with a need to know.

- Never leaving PII unattended on a desk, network printer, fax machine or copier.

- Utilizing a privacy screen in any unsecured area or ensuring any computer monitor is hidden from the public or unauthorized user.

- Locking any computer screen when leaving your desk for any reasonable amount of time.

- Avoiding discussing sensitive PII over the phone within earshot of anyone who does not need to know the information. If a speakerphone must be utilized, ensuring it is used in a location secure from unauthorized persons.

- When teleworking from home or travel is necessary, all the above mentioned safeguards will be utilized just as they are in the physical office.

Financial Designs Corporation
CYBERSECURITY & PRIVACY PROGRAM

PRIVACY BREACH PROCEDURE

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the federal Privacy Act of 1974 or a relevant provision of the SEC Rule 206(4)-7 [17 CFR Part 248.30]. An example of a privacy breach would be personal information becoming lost or stolen or personal information being mistakenly emailed to the wrong person.

The recommended privacy breach incident protocol has five steps. Step 1 is the responsibility of the individual or individuals who first become aware of the potential breach. The second through fifth steps are the responsibility of Financial Designs Corporation, working in cooperation with financial custodians or other financial institutions, as necessary.

Step 1: Reporting the Breach

Any client or Financial Designs employee who becomes aware of a possible breach of privacy involving personal information in the custody or control of Financial Designs (“the company”) should immediately inform the company. As soon as the breach has been confirmed to have or have not occurred, the company will inform both the client and the responsible entity. This confirmation will occur within 72 hours of the initial report.

When a breach has been confirmed, Financial Designs will implement the remaining four steps of the breach incident protocol.

Step 2: Containing the Breach

Financial Designs will take the following steps to limit the scope and effect of the breach. These steps will include:

1) recover any records affecting the clients' security
2) working with the custodian of funds to stop all unauthorized transactions
3) shutting down the system that was breached or correcting weaknesses in security

Step 3: Evaluating the Risks Associated with the Breach

To determine what other steps are immediately necessary, Financial Designs will assess the risks associated with the breach. The following factors will be among those considered in assessing the risks:

1) What personal information was involved?

2) What data elements were breached? Generally, the more sensitive the data, the higher the risk. Social security and financial information that can be used for identity theft would be considered high risk.

3) What possible use is there for the personal information? Can the information be used for fraudulent or otherwise harmful purposes?

4) Cause and extent of breach.

5) Risk of further exposure of the information.

Step 4: Notification

Notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed. Financial Designs will work with the client and/or entities involved to decide the best approach for notification.

Notification of individuals affected by the breach will occur as soon as possible following the breach. However, if law enforcement authorities have been contacted, those authorities will assist in determining whether notification will be delayed in order not to impede a criminal investigation.

The preferred method of notification is direct - by phone, letter or in person - to affected individuals. Indirect notification - website information, posted notices, media -will generally occur only where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

Notifications will include the following pieces of information:

a) Date of the breach
b) Description of the breach
c) Description of the information inappropriately accessed, collected, used or disclosed.
d) The steps taken to mitigate the harm.
e) Next steps planned and any long term plans to prevent future breaches.
f) Steps the individual can take to further mitigate the risk of harm.

Regardless of what obligations are identified with respect to notifying individuals, notifying the following authorities or organizations will also be considered:

a) Police, if theft or other crime is suspected.
b) Financial Custodian
c) Other regulatory bodies, if professional or regulatory standards require notification of these bodies.

Step 5: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, Financial Designs will investigate the cause of the breach. If necessary, this will include a security audit of physical, organizational and technological measures. As a result of this evaluation, Financial Designs will assist the responsible entities to put into effect adequate long-term safeguards against further breach. Policies will be reviewed and updated to reflect the lessons learned from the investigation and will continue to be reviewed on an on-going basis.

Financial Designs Corporation
CYBERSECURITY & PRIVACY PROGRAM

PRIVACY POLICY

Financial Designs Corporation ("FDC") believes it is essential that we maintain the privacy of the nonpublic personal information that you provide to us and that we obtain in connection with providing our products and services to you.

FDC limits the use, collection, and retention of such information to what we believe is necessary or useful to conduct our business and to provide and offer you quality products and services, as well as other opportunities that may be of interest to you. Information collected may include, but is not limited to name, address, telephone number, tax identification number, date of birth, employment status, annual income, and net worth.

In providing products and services to you, we collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms (e.g. investment/insurance applications, new account forms, and other forms and agreements);
- Information about your transactions with us, our affiliates, or others (e.g. broker/dealers, clearing firms, or other chosen investment sponsors); and
- Information we receive from consumer reporting agencies (e.g. credit bureaus), as well as other various materials we may use to put forth an appropriate recommendation, or to fill a service request.

FDC places strict limits on who receives specific information about your account(s) and other personally identifiable data. In compliance with the California Financial Information Privacy Act, Code sections 4050-4060, we require you to “opt in” before we may share any personal information with an unaffiliated third party. “Opting in” is assumed if we do receive any communication from you stating you would like to opt out.

As a rule, we do not disclose any nonpublic personal information we collect to others. However, because we rely on certain third parties for services that enable us to provide our advisory services to you, such as our attorneys, auditors, consultants, brokers, and custodians who, in the ordinary course of providing their services to us, may require access to information, we may share—upon your “opt in” approval—non-public personal information with such third parties. Additionally, we will share such information where required by legal or judicial process, such as a court order, or otherwise to the extent permitted under the federal privacy laws.

We restrict access to nonpublic personal information about you to those persons associated with FDC, who need access to such information in order to provide our products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.

If you decide to close your account(s) or become an inactive customer, we will adhere to the privacy policies and practices as described in this notice.

_____

FDC reserves the right to change these Privacy Principles, and any of the policies or procedures described above, at any time without prior notice. However, you will be promptly provided with a current copy of our privacy notice upon material changes or upon request. So long as you remain an active customer, you will receive a current copy of our privacy notice at least annually. These Privacy Principles are for general guidance and do not constitute a contract or create legal rights, and do not modify or amend any agreements we have with you.

Safeguarding of Client Records and Information

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

To protect client and personal information, including consumer report information, the Company maintains the following security measures and safeguards for the storage of, access to, and disposal of client personal information, including consumer report information, obtained and/or maintained in hard copy and/or electronically, as well as access and protections of its computer and information systems:

- limiting access to nonpublic and consumer report information to those Associated Persons who require the information in order to help us provide services;
- locking rooms and file cabinets where paper records are stored;
- protecting storage areas against destruction or potential damage from environmental hazards;
- storing electronic nonpublic and consumer report information on a secure server that is accessible only with a password;
- maintaining secure backup media;
- storing archived data off-line and/or in a physically-secure area;
- supervising the disposal of records containing nonpublic and consumer report information;
- shredding nonpublic and consumer report information recorded on paper and storing such material in a secure area until it is collected by a recycling service;
- erasing all data when disposing of computers, diskettes, magnetic tapes, hard drives, or any other electronic media containing nonpublic and consumer report information;
- disposing of outdated nonpublic and consumer report information promptly;
- using anti-virus software that updates automatically; and
- maintaining up-to-date firewalls.

If you have any questions about this Privacy Notice please call Greg Morton at (909) 626-1642 or contact the company via e-mail at fdc@fdcadvisors.com .

FINANCIAL DESIGNS CORPORATION