Additional 21713

FISHER FIDUCIARY SERVICES

793 S. Tracy Blvd., Suite 286
Tracy, CA 95376

Telephone (209) 629-8518
Fax (209) 830-0500

June 30, 2021

NAME
ADDRESS

RE: Notice of Data Breach

Dear NAME:

I am writing to inform you about a data security incident affecting personal information about you in our office's records, which I refer to as the "Incident" in this letter. A fire occurred in our office building on March 16, 2021. The fire was catastrophic, and it was determined by the fire department that it was unsafe to re-enter the building until such time as the building could be inspected and secured. On April 20, we received notification from the owner of the building that we were cleared to enter the building to retrieve our belongings but were informed that that the Incident occurred. Your personal information was exposed to one or more unauthorized third parties as a result of the Incident.

We sincerely apologize for this Incident occurring and for any inconvenience you have experienced or may experience in the future. We want you to know that we take the security of our client data seriously and therefore want to inform you of the immediate steps we started to respond to this Incident.

What Happened?

The Incident occurred sometime on or after March 16, 2021. On that date, a tenant in an adjacent suite in our office building accidentally spilled epoxy on a surge protector, sparking a fire. The fire spread quickly to the roof, and we had to evacuate our office. The fire department was able to extinguish the fire before our space burned. However, there was significant smoke and water damage to the entire building. Due to heavy air conditioning units that were dangling from the roof and asbestos concerns, the fire department considered the building too hazardous to enter, and we were instructed not to reenter the building until the fire department could complete the necessary inspections, including hazmat inspections, until removal of the air conditioning, and until a determination that the building was safe.

For over a month, we were unable to reenter our office space. Finally, on April 20, the building owner informed us that the fire department was permitting tenants to reenter the building. At the same time, we learned about the Incident. We do not know the

exact date of the Incident, but believe it occurred sometime between March 16 and April 20.

Under Massachusetts law, a notice of a security incident such as the Incident "shall not include the nature of the breach of security or unauthorized acquisition or use" or your personal information. Accordingly, this notice does not include more details about how the Incident occurred.

What Information Was Involved?

Based on our investigation to date, the compromised data included the following categories of information about our clients and other non-client individuals that had some relationship with Fisher Fiduciary Services, Inc., including potential clients, family members of clients, beneficiaries of estates, and vendors:

- Social security numbers
- Driver's license numbers
- Naturalization documents
- Birth certificates
- Payment card accounts, brokerage/retirement accounts, and bank accounts with username and password information to access such accounts
- Medical information about the client's medical condition and treatment
- Health insurance card information from Medicare or private insurers

Our records did not necessarily include all of these categories of information on every individual. Investigation is continuing to confirm what kinds of personal information of each client was exposed. If you have questions about what information of yours might have been exposed, please contact me, and I will provide you with the latest information about your personal information that is available to me at that time.

What We are Doing

First, we promptly filed a police report to inform law enforcement of the Incident.

Second, we immediately contacted card issuers for certain payment card accounts and ordered new cards for all of our clients who had one.

Third, we called and talked with some of you that have been impacted by the incident.

Fourth, for clients who had credit profiles and could not respond on their own, we placed fraud alerts on their credit profiles with the three credit bureaus. For those that did not assistance from us, we notified you of the breach and recommended that you place a fraud alert on your credit profile.

Fifth, we have launched an investigation with the assistance of a computer forensic expert to make sure we have a complete understanding of the kinds of personal information that might have been exposed. That investigation remains ongoing and, if appropriate, we will follow up with further notifications.

Sixth, we are offering identity theft protection services through IdentityForce, Inc. to provide you with RapidResponse Plus identity monitoring services. Our office is providing these services to you without cost. IdentityForce's services include:

- 18 months of credit monitoring and recovery services,

- Medical identity theft coverage,
- Educational materials to reduce the risk of identity theft,
- $1 million in identity theft insurance, and
- Access to identity theft resolution representatives that can provide advice to you on ways to prevent and recover from identity theft.

What You Can Do

You have the right to obtain a police report about the Incident.

Also, you can obtain free credit reports from the nationwide credit reporting agencies. The three nationwide agencies and their contact information, including toll-free telephone numbers, are:

Equifax	Experian	TransUnion
888-766-0008	888-397-3742	800-680-7289
PO Box 740241	PO Box 9554	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

A fraud alert helps to prevent someone from establishing credit in your name, because businesses must verify your identity before offering new credit in your name. A security freeze restricts access to your credit report, making it more difficult for someone to open credit in your name. Fraud alerts and security freezes, however, may delay your own ability to apply for credit.

If you don't yet have a fraud alert or credit freeze on your accounts, Transunion representatives can advise you about using fraud alerts and credit freezes to reduce the risk of identity theft. There is no charge for using a fraud alert or credit freeze. The number to call is 1-800-916-8800. You may use this number to place a fraud alert on your credit file for up to one year through their automated system, or up to seven years if you speak to a representative. Also, by placing the fraud alert through Transunion, the alert automatically spreads to all three credit reporting agencies. If you sign up for IdentityForce services, its representatives can also assist you with fraud alerts and credit freezes.

You can also receive information from the three credit reporting agencies at the above contact information or the Federal Trade Commission about fraud alerts and security freezes (https://www.consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts).

To enroll in IdentityForce's credit monitoring and identity theft service, please call our office at the number at the top of this letter or email me at hfisherfs@yahoo.com to receive an enrollment code. You must have an enrollment code to enroll. Once you have a code, go to https://secure.identityforce.com/benefit/fisher , fill in your name, email address, and enrollment, and click "Activate My Account".

You have until June 30, 2022 to enroll in the IdentityForce program.

We also recommend that you review statements about your financial accounts for possible identity theft and monitor free credit reports. You should report any suspicious transactions or other activity to your financial institution. You may also want to report the

activity to law enforcement. In addition, you may want to report the activity to the Federal Trade Commission at www.ftc.gov/idtheft or (877) IDTHEFT (438-4338). You can also view tips and information about preventing identity theft from the Massachusetts Office of Consumer Affairs and Business Regulation at the following contact information:

- Web: https://www.mass.gov/service-details/identity-theft
- Phone: (617) 973-8787
- Write: Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116

For More Information

If you have any questions or concerns about this incident, please contact me directly. My contact information is at the top of this letter.

* * * *

We deeply regret that this Incident occurred and want to assure you we are taking every necessary step to minimize any impact to you. Also, we want to assure you that we are taking steps to prevent future incidents of this kind and are reviewing our data security practices and will implement additional steps to enhance our business's security to minimize the likelihood and impact of any future security incident. While we cannot guarantee that security incidents will not occur in the future, what we can do is again express our apology for this incident and any inconvenience to you. We view it as a privilege to serve you and are committed to cooperate with you to respond to this incident. Thank you.

Should you have any questions or concerns, please feel free to call, email, or write me directly.

Regards,

Heather Fisher, CLPF# 763