

16065

[EMPLOYEE FIDUCIARY LETTERHEAD]

[EMPLOYEE NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]
[CREDIT MONITORING PROMOTION CODE]
[DATE]

NOTICE OF DATA BREACH

Confidential – for Intended Recipient Only

Dear [EMPLOYEE NAME]:

We are contacting you regarding an inadvertent disclosure of personal information discovered on October 9, 2019 at Employee Fiduciary, LLC (“Employee Fiduciary,” “we,” “us”). You are receiving this notice because your current or prior employer, Lucid Software, Inc. (“Lucid”), used Employee Fiduciary for 401(k) processing services and your personal information was involved.

WHAT INFORMATION WAS INVOLVED?

On October 9, 2019, an individual at one of Employee Fiduciary’s customers inadvertently received a copy of an employee report intended for Lucid. The report included: first names, last names, social security numbers, 401(k) deferral information and safe harbor match information, and certain transaction information related to applicable 401(k) plans.

Please note that we believe that this situation has been addressed and that the disclosed information was promptly deleted. We have no reason to believe that there has been any further use or disclosure of your employee information, or that you are at risk of identity theft or other harm from this disclosure. That said, certain state laws require disclosure in this type of event, and we are notifying employees as required by applicable law. Due to the limited nature of the disclosure, neither we nor Lucid have not engaged law enforcement in the investigation of this incident.

WHAT WE ARE DOING

Employee Fiduciary and Lucid value your privacy and regret that this incident occurred. Lucid has worked with Employee Fiduciary to ensure that the disclosed information was deleted by Employee Fiduciary’s customer, and Employee Fiduciary will be providing any affected employees with twelve (12) months of credit monitoring services, as described below, should you choose to accept it.

WHAT YOU CAN DO

Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information as well as how to receive free credit monitoring services for twelve (12) months.

FOR MORE INFORMATION

For further information and assistance, please contact Eric Droblyen at (727) 324-4004 or eric@employeefiduciary.com during our regular business hours.

Sincerely,

Eric C. Droblyen
President & CEO

Steps You Can Take to Further Protect Your Information

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). You have the right to obtain a police report from your local law enforcement, should you so desire.

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 4500	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

- **Credit Report Monitoring Services**

To help protect your identity, we are offering a complimentary one-year membership of Experian's IdentityWorksSM. This product provides you with superior identity detection and resolution of

identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Enroll by: February 2, 2020 (Your code will not work after this date)
- Visit the Experian IdentityWorks website: <https://www.experianidworks.com/3bplus>
- Provide your activation code: [XXX]

If you have any questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by February 2, 2020. Be prepared to provide engagement number DB16311 as proof of eligibility for the identity restoration services by Experian.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

- **Consider Placing Security Freeze on Your Credit File**

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.