Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Notice of Data Breach

Dear <<Name 1>>:

Personify Financial* appreciates its consumers and recognizes the importance of protecting your personal information. We have taken steps to investigate and address a data security incident involving employee business e-mail accounts. Our internal investigation has revealed that information about you may have been accessed by an unauthorized third-party hacker through those business e-mail accounts. This notice explains what happened, the information involved, measures we have taken, and some preventive steps you can take in response.

What Happened

On or about November 9, 2018, we were alerted to suspicious activity regarding an employee's business e-mail account. We immediately began investigating this activity and subsequently determined that an unauthorized third party had illegally gained access to the employee's business e-mail account on July 21, 2018. The hacker also gained access to a second employee's email account. The hacker was able to view the contents of both e-mail accounts and send "spear-phishing" e-mails to others. A "spear-phishing" e-mail is a message that appears to be from someone the recipient knows and trusts, but it is actually sent by a different person trying to illegally obtain access to the recipient's computer system, e-mail accounts, or personal information. We have seen no evidence of this hack extending outside of our email servers into the rest of our IT system.

What Information Was Involved

Some e-mails or their attachments in our employees' e-mail accounts included information about loan applicants, current and former customers, and others. The information may have included names, residence addresses, telephone numbers, e-mail addresses, Social Security numbers, Personify Financial account numbers, or other personal or account information.

What Are We Doing

Personify Financial regrets this incident occurred. Upon discovering the suspicious activity, we took immediate steps to disable the affected employees' business e-mail accounts and further strengthen the security of our e-mail systems to prevent similar e-mail hacking attempts. We also began working with a nationally recognized computer forensics investigation firm to determine what happened, how it happened, and what information may have been compromised.

We have reported this security incident to federal law enforcement. We are notifying the appropriate state regulatory authorities where required and have advised the three major consumer reporting agencies (Equifax, Experian, and TransUnion) about this incident.

* Applied Data Finance, LLC ("ADF") and its wholly-owned subsidiaries, doing business in certain states as Personify Financial. Those subsidiaries include ADF of Alabama, ADF of California, ADF of Idaho, ADF of Illinois, ADF of Missouri, ADF of New Mexico, and ADF of South Carolina.

What You Can Do

Personify Financial has also taken steps to help you monitor and protect your personal information. We have retained Epiq, a worldwide provider of legal services, to help us provide you with credit monitoring and identity theft restoration services at no charge to you. We have arranged for you to enroll, again at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide reporting companies. To enroll in this service, go to the *my*TrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes. If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit-monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code <<Engagement Number>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or, if you believe you may be a victim of identity theft, to speak to a TransUnion representative.

In addition, if you believe you are the victim of identity theft or have reason to believe your personal data has been misused, you should immediately contact local law enforcement.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, an address in the United States (or its territories), or a valid Social Security number. Enrolling in this service will not affect your credit score. Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program which provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible (policy limitations and exclusions may apply).

We recommend that you sign up for the credit monitoring service described above or use your existing credit monitoring service to alert you to activity in your credit report. You should also monitor your financial accounts, including your credit and debit card accounts. If you see any unauthorized activity, please promptly contact your financial institution or card issuer. Please refer to the "Important Disclosures" included with this notice for more information and for other preventive steps you can take.

For More Information

We have established a dedicated call center to answer questions you may have about this incident. You may contact our incident response call center toll-free at 877-209-9506 Monday through Friday from 6 am to 6 pm Pacific Time. This call center will be available to you through April 30, 2019.

Personify Financial values your business and takes the security of your personal information seriously. We apologize for any inconvenience this data security incident may cause you.

Sincerely,

Krishna Gopinathan, CEO

Special note for minors affected by this incident: The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

Notice to Maryland Residents: Information about the steps you can take to prevent or avoid identity theft is available from the Maryland Attorney General's Office at: 200 St. Paul Place, Baltimore, MD 21202 / (410) 576-6300 / Toll-Free: (888) 743-0023 / TDD: (410) 576-6372 / http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx.

Notice to North Carolina Residents: Information about the steps you can take to prevent or avoid identity theft is available from the North Carolina Attorney General's Office at: 9001 Mail Service Center, Raleigh, NC 27699-9001 / Toll-Free within North Carolina: (877) 566-7226 / http://www.ncdoj.gov/.

Notice to Rhode Island Residents: You have the right to file and obtain a copy of a police report. You also have the right to request a security freeze. Information about the steps you can take to prevent or avoid identity theft is available from the Rhode Island Attorney General's Office at: 150 South Main Street, Providence, RI 02903 / (401) 274-4400 / www.riag.ri.gov.

More Information and Important Disclosures from Personify Financial

---

Identity Theft Protection Information

You may visit the website of the Federal Trade Commission ("FTC") at https://www.identitytheft.gov for free information to help you guard against identity theft and for guidance on the recovery steps you can take if you have been the victim of identity theft, including information on how to file an identity theft complaint. You can also write to the FTC at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Your State Attorney General's Office may also provide free information about identity theft protection measures and the reporting of identity theft. Please visit http://www.naag.org/ to find the link to your State Attorney General's website for more information.

Financial and Credit and Debit Card Accounts

You should monitor the activity in your checking and other financial accounts and review any account statements that you receive for the next 12 24 months and promptly report any suspicious activity to your financial institution.

You should also review your most recent credit and debit card account statements and those that you receive for the next 12 24 months and promptly report any suspicious activity to your card issuer. For information from the Federal Trade Commission on how federal law limits your liability for unauthorized card charges, please visit http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

Free Credit Report

You may obtain a free credit report from each of the three major U.S. credit reporting agencies (Equifax, Experian, and TransUnion) every 12 months by calling 1-877-322-8228 or logging onto www.annualcreditreport.com. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. Any information already accessed by cyber-criminals can still be used to initiate fraudulent transactions at a later date. Stolen personal information is sometimes held for use, or later shared, or sold among a group of cyber-criminals. Periodically checking your credit reports can help you spot problems and address them quickly.

Fraud Alerts and Security Freezes

You can place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or make changes to your existing accounts, such as address changes. You can place this alert on your file by contacting any one of the three major U.S. credit reporting agencies identified below. We recommend that you contact one of the agencies, as identified below, by phone or go online to find out the specific requirements and expedite this process. As soon as one credit reporting agency confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days. After your fraud alert request, all three credit reporting agencies will send you one free credit report for your review.

You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to contact each of the three major U.S. credit reporting agencies separately. The credit reporting agency may charge a fee, which varies by state, to place a freeze or lift or remove a freeze. The freeze should be free if you are a victim of identity theft or the spouse of a victim of identity theft and you have submitted a valid police report relating to the identify theft incident to the credit reporting agency. You may contact the credit reporting agencies, as identified below, by telephone or go online to find out more information about this process.

Equifax
1-800-525-6285
Fraud Alerts: https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
Security Freezes: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
P. O. Box 105788, Atlanta, GA 30348

Experian
1-888-397-3742
Fraud Alerts: https://www.experian.com/fraud/center.html
Security Freezes: https://www.experian.com/freeze/center.html
P. O. Box 9554, Allen, TX 75013

TransUnion
1-800-680-7289
Fraud Alerts: https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp
Security Freezes: https://www.transunion.com/credit-freeze/place-credit-freeze
P. O. Box 6790, Fullerton, CA 92834-6790

You may also obtain information about fraud alerts and security freezes from the FTC at https://www.identitytheft.gov or by calling 1-877-438-4338 (TTY: 1-866-653-4261).

Law Enforcement

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local police department and file an identity theft police report. You should ask for a copy of the police report as you may need a copy of the report to clear up any fraudulent debts. You can also file a complaint with the FTC at https://www.identitytheft.gov/ or at 1 877 ID THEFT (877-438-4338). Although the FTC does not have criminal jurisdiction, it supports criminal investigations and prosecutions through its Identity Theft Data Clearinghouse, the nation's repository for identity theft complaints.
