18754

DACdb
District and Club database

NOTICE OF DATA BREACH TO MASSACHUSETTS RESIDENTS

February 9, 2021

[INSERT ADDRESS/EMAIL]

Dear NAME,

This letter provides details relating to a security incident that may have affected personal information you provided to DACdb when making a payment via iPPay on our site. The security incident began on October 22, 2020, and we discovered it and immediately remediated the issue on January 19, 2021. We then engaged a forensic IT firm to investigate the incident. At this point, this firm and we have completed our investigations, and the security incident has been fully contained.

What Information Was Involved?
Based on our investigation, your specific information affected included your name, address, email address and credit or debit card number, expiration date and security code.

What We Are Doing.
We have engaged a third party forensic IT firm to conduct a comprehensive security review of all of our systems, and they have confirmed that this incident has been successfully resolved. We have also taken additional proactive measures to help safeguard our services and protect your personal information. In addition, we have prepared the attached resources to assist you in the event that you believe you have become a victim of fraud or identity theft. Though the matter has been remediated, we will continue to monitor the situation closely for any additional suspicious activity.

What You Can Do.
As we suggested in our prior communication to you, we recommend that you cancel the credit or debit card disclosed in this incident, and request a new card. In addition, you may want to ask your bank or card issuer to create an automated alert, so that you are notified of all transactions on your account. Immediately contact your bank if you discover anything suspicious related to your financial accounts. Please also be aware that criminals may attempt to send you targeted emails seeking to obtain other confidential information from you (i.e. phishing scams), or may otherwise try to use your personal information.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft or fraud, you also have the right to file a police report and obtain a copy of it. Please report any illegal activities to law enforcement or an appropriate government authority

(see below for helpful resources). If you notice any unauthorized or suspicious financial activity, such as new credit applications, loans, or account openings, report it to the appropriate financial institution in addition to government authorities. Remember, DACdb will never ask for your sensitive personal information via email. If you receive an email from us requesting this information, do not open any attachments and do not provide any personal information. If you have concerns or suspicions about an email from DACdb, please contact support@dacdb.com or call 720-504-7300 x1.

You may wish to implement a security freeze or fraud alert on your credit file with the three major credit bureaus. Instructions regarding how to do this are in the attachment to this letter.

Although no passwords were compromised as part of the security incident, consider taking a moment to change any old, reused, or insecure passwords and remember to follow appropriate security practices when managing your online accounts. More information on creating strong passwords can be found on the Department of Homeland Security's website: https://www.us-cert.gov/ncas/tips/ST04-002.

For More Information.

If you have any questions regarding this notice or if you would like more information, please do not hesitate to contact **support@dacdb.com or call 720-504-7300 x1**. Most importantly, we sincerely regret any concern this security incident may cause, and we value your trust and understanding.

Sincerely,

Mark Landmann,
President

IMPORTANT INFORMATION ABOUT IDENTITY THEFT PROTECTION

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also obtain a copy of your credit report, or request information on how to place a fraud alert or security freeze on your credit file, by contacting any of the national credit bureaus as described below. Remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. The primary contact information for three major credit bureaus are as follows, and specific additional contact information to place a fraud alert or security freeze can be found below:

Equifax P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19022 1-800-888-4213 www.transunion.com

Contact Information for the Federal Trade Commission

In addition to the credit bureaus above, you may contact or visit the website of the Federal Trade Commission to learn more about how to protect yourself against identity theft, or how to place a fraud alert or security freeze on your credit file. The contact information for the FTC is as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

How to Place a Security Freeze on Your Credit File

If you wish to take more extensive measures to prevent new credit being opened in your name, you may consider placing a security freeze on your credit file. You should only place a security freeze if you want to prevent most parties from obtaining your credit report and prevent all credit, loans and related services from being approved in your name without your consent. Please consider that this may also impact or delay your ability to obtain certain government services, rental housing, employment, cell phone plans, insurance, utilities, and other services.

You will need to apply for a security freeze separately with each of the credit bureaus. The requirements to obtain a security freeze vary somewhat depending on which credit bureau you contact. Under federal law, you cannot be charged to place, lift, or remove a security freeze. When applying for a

security freeze, you may be asked to provide some or all of the following information (this may vary depending on the specific credit bureau):

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

You can find more information regarding a security freeze at the following links, or by calling each of the credit bureaus at the numbers listed in this notification letter:

https://www.equifax.com/personal/credit-report-services/credit-freeze/
https://www.experian.com/freeze/center.html
https://www.transunion.com/credit-freeze

How to Place a Fraud Alert on Your Credit File

As an alternative to a security freeze, to protect yourself from the possibility of identity theft or other fraud, you may place an initial or extended fraud alert on your credit file. The fraud alert helps to prevent someone else obtaining credit in your name. If you have a fraud alert on your credit file, creditors will contact you and verify your identity before they open any new accounts or change your existing accounts, but it should not affect your credit score or your ability to obtain new credit (although it may cause a delay in any applications or approvals). As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts, so you do not need to place alerts with more than one of the credit bureaus. To place a fraud alert, contact any of the credit bureaus below, and complete the requested steps:

https://www.experian.com/fraud/center.html
https:// www.equifax.com/personal/credit -report-services
https://www.transunion.com/fraud-alerts