NOTICE OF DATA BREACH

February 10, 2021

Office of the Attorney General
State of New Hampshire
33 Capitol Street
Concord, NH 03301

Dear Office of the Attorney General,

This letter is DACdb,LLC's formal notice of a data breach that affected the payment card information of 2 New Hampshire residents. 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.

Based on our investigation, your specific information affected included the users' name, address, email address and credit or debit card number, expiration date and security code.

We have notified the affected users on February 9, 2021, via the attached template letter.

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 users' personal information. Though the matter has been remediated, we will continue to monitor the situation closely for any additional suspicious activity.

If you have any questions regarding this notice or if you would like more information, please do not hesitate to contact me directly.

Sincerely,

Colleen R Jones,
General Counsel

9457 S. University Blvd #930 Highlands Ranch, CO 80126 (720) 504-7300

DACdb
District and Club database

NOTICE OF DATA BREACH

February 9, 2021

[User name and address]

Dear [User 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.

What Happened?
We recently discovered that malicious code had been inserted into a payment card processing page. When certain DACdb users clicked "Pay" on this page, the malicious code caused their credit or debit card information to be sent not only to the payment processor, but also to the hacker. This malicious code was inserted on or about October 22, 2020, we discovered it on January 19, 2021, and we disabled it immediately. 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?
The information potentially affected by this security incident varied somewhat depending on the information provided by the affected individuals. 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, and no further incidences of malicious activity are anticipated. We have also taken additional proactive measures to help safeguard our services and protect your personal information. All DACdb users are now required to update their user credentials, new and improved firewalls have been deployed on our servers, user payment card information for this processor is now entered directly on a page hosted by the processor, system-wide malware detection software has been installed and we have purchased monthly scanning services as a backstop. 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.
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.

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.

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

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 depending on your state of residence, and you may be required to pay a fee, provide your name and social security number, copies of important identification records (including a list of addresses, copies of government issued IDs, and/or utility bills), provide an incident report if you are a victim of identity theft, or take other measures as described on the credit bureaus' websites. You may need to follow these steps for each individual (such as a spouse or dependent) who will request a security freeze. 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

State – Specific Information

Residents of the following states can obtain additional information about steps to avoid identity theft from these resources:

Maryland:
Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx
Telephone: 1-888-743-0023
Email: idtheft@oag.state.md.us

New York
New York Attorney General
Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
Telephone: 1-800-771-7755
www.ag.ny.gov

North Carolina
Office of the Attorney General of North Carolina
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: 877-566-7226 (Toll-free within North Carolina) or 919-716-6000
www.ncdoj.com/
https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft

Rhode Island
Rhode Island, Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
Telephone: (401) 274-4400
www.riag.ri.gov
http://www.riag.ri.gov/ConsumerProtection/About.php