

Dear [INDIVIDUAL NAME]:

We deeply value your business. Your security is our top priority, which is why, as a precautionary measure, we write to inform you of a data security incident involving your personal information.

During the period between April 23rd and July 15th, 2014, individuals obtained unauthorized access to The Dreslyn's credit card data during payment processing. We immediately investigated the situation and determined the data includes customers' login credentials, password, name, address, credit or debit card number, expiration date and CVV code. It did not include debit card pin codes or billing information from PayPal.

Criminals could use the captured information to make third-party purchases. This does not mean fraudulent activity has occurred, but we recommend that you closely monitor your credit card statements for suspicious activity, and review the information provided in the attachment to this letter to protect against potential misuse of your credit.

Our brand is built on a foundation of transparency with our customers, and we assure you the root of this issue has been addressed and resolved so you may continue to shop with confidence at The Dreslyn.

We take crimes like this seriously. We are working with law enforcement and forensic investigators to conduct a thorough review of the potentially affected records and systems. We have reset the account passwords of those affected and implemented additional security measures designed to prevent a recurrence of such an attack.

Additionally, credit card suppliers have been notified to ensure the incident is properly addressed. You will not be held responsible for charges resulting from fraudulent use of the compromised credit card information.

We truly apologize for any inconvenience this may cause. If you require further information or assistance, please contact The Dreslyn Customer Service at 1-855-373-7596 between 8:00 a.m.- 6:00 p.m. PST daily or email info@thedreslyn.com.

Sincerely,
Brooke Taylor Corcia

President & CEO, The Dreslyn

STEPS YOU SHOULD TAKE TO PROTECT YOUR CREDIT CARD INFORMATION

Consumers are generally not liable for fraudulent use of their credit or debit card information. We recommend that you closely monitor your account activity and statements. If you notice any suspicious activity on an account, you should promptly notify the financial institution that issued the affected card. In addition, you should take the following steps.

- **Notify Law Enforcement and the Federal Trade Commission of Suspicious Activity**

You should also promptly report any fraudulent activity or suspected identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a complaint with the Federal Trade Commission, go to www.ftc.gov/idtheft 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.

- **Monitor Your Credit Report**

You can also protect yourself against unauthorized use of your credit card by monitoring your credit report. A credit report is a detailed report of an individual's credit history, prepared by a credit bureau, and used by lenders in determining a loan applicant's creditworthiness.

You may 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 print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. 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
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
475 Anton Blvd.
Costa Mesa, CA 92626

TransUnion
(800) 916-8800
www.transunion.com
P.O. Box 1000
Chester, PA 19022

- **Place 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 ninety 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 using the contact information above. Additional information is available at <http://www.annualcreditreport.com>.

- **Place A Security Freeze On Your Credit File**

In some states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to \$5 to place, lift or remove the security freeze.

- **Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit <http://www.ftc.gov/idtheft> or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, 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 <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idtheft04.shtm>.