February 6, 2019

VIA US MAIL **INTENDED FOR ADDRESSEE(S) ONLY**

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

On behalf of Graf & Sons Inc. ("Grafs"), I am writing to notify your office of an incident that may affect the security of certain personal information of eight (8) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Grafs does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On January 29, 2019, Grafs suspected that there may be an issue with its website (www.grafs.com), and it began investigating this issue. Late on January 30, 2019, the service provider that Grafs engages to develop, host and support its website confirmed that it fell victim to a malicious code attack by unknown third parties, which, in turn, affected Grafs' website. Since then it has come to light that as part of this attack, certain customer files of Grafs were affected and the malicious code captured certain credit card transactions from the e-commerce portion of the website. These transaction files included credit card transactions with eight (8) New Hampshire residents. The information in these affected files included the following personal information: the customer's first and last names, email address, mailing address and credit card information, including the credit card number, the expiration date, and the CVV code for such card. Grafs has not been able to determine whether or not this malicious code transmitted such information to any third parties. The malicious code has been removed from Grafs' website. Additional security measures have been taken to further secure the website, Graf's information technology environment and its customers' personal information.

Notice to New Hampshire Residents

In the most expedient time possible and without unreasonable delay, Grafs is providing written notice of this incident to affected individuals, including the eight (8) New Hampshire residents. Written notice is being

provided in substantially the same form as the letter attached here as Exhibit A.

Other Steps Taken and To Be Taken

As soon as Grafs and its service provider recognized there may be a problem, they took steps to investigate the problem, stop the attack and mitigate any damage caused by the malicious code. As part of such efforts, Grafs and its service provider have been notifying the appropriate governmental entities, including you, as the New Hampshire Attorney General, and the Federal Bureau of Investigation.

Additionally, as part of the notice provided to the affected individuals, Grafs is providing guidance on how the impacted individuals may protect against identity theft and fraud, including advising the individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Grafs is also providing such individuals with (i) information on how to place a fraud alert and security freeze on their credit file, (ii) information on protecting against tax fraud, (iii) the contact details for the national consumer reporting agencies, (iv) information on how to obtain a free credit report, (v) a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and (vi) encouragement to contact the Federal Trade Commission, their state's Attorney General, and/or law enforcement agencies to report any attempted or actual identity theft and fraud.

Grafs will continue to take the steps necessary to protect its customers, their personal information and Grafs' information technology environments.

Contact Information

Should you have any questions regarding this notification or other aspects of the incident, please contact either

Paul Seigfreid
President & CEO
Telephone: 1-800-531-2666 ext. 118
Email: pauls@grafs.com

Melissa Perkins,
CFO
Telephone: 1-800-531-2666 ext. 119
Email: mperkins@grafs.com.

Very truly yours,

Paul Seigfreid
President & CEO
Graf & Sons Inc.

GRAF & SONS
THE RELOADING AUTHORITY

TO: Affected Customers of Graf & Sons, Inc.
FROM: Paul Seigfreid, President & CEO
DATE: February 6, 2019

NOTICE OF DATA BREACH

We, at Graf & Sons Inc. ("Grafs"), value and respect the privacy of your information, which is why we are writing to inform you of a data security incident that has occurred.

WHAT HAPPENED?

On January 29, 2019, Grafs suspected there may be an issue with its website (www.grafs.com), and it began investigating this issue. Late on January 30, 2019, the service provider that Grafs engages to develop, host and support its website confirmed that it fell victim to a malicious code attack by unknown third parties, which, in turn, affected Grafs' website. Since then it has come to light that as part of this attack, certain customer files of Grafs were affected and the malicious code captured certain credit card transactions from the e-commerce portion of the website. Grafs has not been able to determine whether or not this malicious code transmitted such information to any third parties. However, out of the utmost caution, we are sending you this notice so that you can take steps to protect your personal information.
As soon as Grafs and its service provider recognized there may be a problem, they took steps to investigate the problem, stop the attack and mitigate any damage caused by the malicious code. As part of such efforts, Grafs and its service provider have been notifying the appropriate governmental entities, including the Federal Bureau of Investigation. We are currently working with such governmental entities in their investigation of the incident. We will continue to take the steps necessary to protect our customers, their personal information and Grafs' information technology environments.

WHAT INFORMATION WAS INVOLVED?

As stated above, Grafs' e-commerce website fell victim to a malicious code attack. This malicious code captured certain customer transaction files. The transaction files that were captured by the malicious code included the following personal information: the customer's first and last names, email address, mailing address and credit card information, including the credit card number, the expiration date, and the CVV code for such card. However, Grafs has been unable to determine whether or not such information has been disclosed to, or stolen by, any third parties. Grafs does not collect through its e-commerce site any social security numbers or protected health information, and so this information was not collected by the malicious code.

WHAT WE ARE DOING

Grafs values your privacy and deeply regrets that this incident occurred. We are conducting a thorough review

of the incident and will notify you if there are any other significant developments. We have implemented additional security measures designed to prevent a recurrence of such an incident and to protect the privacy of our valued customers and to prevent further unauthorized access.
As referenced above, we are working closely with the applicable governmental officials to ensure the incident is properly addressed.

WHAT YOU CAN DO

Please also review the Steps You Can Take to Further Protect Your Information attachment for further information on steps you can take to protect your information.

FOR MORE INFORMATION

For further information and assistance, please contact

Paul Seigfreid
President & CEO
Telephone: 1-800-531-2666 ext. 118
Email: pauls@grafs.com
US Mail:
4050 South Clark Street,
Mexico Missouri 65265

Melissa Perkins,
CFO
Telephone: 1-800-531-2666 ext. 119
Email: mperkins@grafs.com
US Mail:
4050 South Clark Street,
Mexico Missouri 65265.

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").

To file a complaint with the FTC, go to https://identitytheft.gov/, or https://www.ftccomplaintassistant.gov or call 1-877-ID-THEFT (877-438-4338). The FTC's mailing address is 600 Pennsylvania Avenue, N, Washington, DC 20580. 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 https://www.annualcreditreport.com/index.action, 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. Alternatively, 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
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
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.

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

We also recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit https://identitytheft.gov/ or call 1-877-ID-THEFT (877-438-4338). In addition, you may want to review 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 https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf and the pamphlet, Identity Theft Information for Taxpayers, IRS Publication 5027, which can be found at https://www.irs.gov/pub/irs-pdf/p5027.pdf.

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.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, by sending an email to idtheft@oag.state.ms.us, or by calling 410-576-6491 (or toll-free at 888-743-0023), or by sending a letter to the Office of Attorney General, Attn: Security Breach Notification 200 St. Paul Place, 25th Floor, Baltimore, Maryland 21202.

Rhode Island residents may request additional information by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400.
North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

We also recommend to promptly change your username, password, and security question answer on the Grafs website. If this username and password is used with additional online accounts, please take other appropriate steps to protect all other login information.

OTHER IMPORTANT INFORMATION

- **Security Freeze**

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, cell 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 (their contact information above) 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. A fee may be required to be paid to the consumer reporting agencies, though there is no charge to request a security freeze or to remove a security freeze.

- **Your Rights Under the Federal Fair Credit Reporting Act**

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting by visiting www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W. Washington, DC 20552.

- **Police Report**

You also have the right to file a police report in the location in which the offense occurred or the city or county in which you reside. You may obtain a copy of the report Grafs has filed with the Federal Bureau of Investigation and the local police.