<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data <<b2b_text_1>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Blauer Manufacturing Co., Inc. ("Blauer") is writing to notify you of an incident that may affect the security of the payment card information you recently used on our website, www.blauer.com. We take this incident very seriously. This letter provides details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or about October 23, 2019, Blauer identified suspicious activity regarding our online e-commerce website, www.blauer.com. Blauer immediately launched an investigation with the assistance of a third-party forensic firm to determine the nature and scope of the activity. Blauer also took steps to implement additional procedures to further protect the security of customer debit and credit card information on our website.

On or about November 11, 2019, the forensic investigation determined it was possible that certain customer credit and debit card information for transactions that occurred on Blauer's e-commerce website between September 26, 2019 and October 23, 2019 may have been subject to unauthorized access and/or acquisition. While the investigation was unable to definitively confirm whether card data was accessed or taken, Blauer is notifying you because we have confirmed that your credit or debit card was used for a transaction on our e-commerce website during the relevant time period.

What Information Was Affected? The information potentially affected includes your name, address, credit or debit card number, expiration date, and card security code number or CVV as they were entered during an online purchase on <<b2b_text_2 (Date)>>. In addition, if you attempted from our checkout page to sign into blauer.com when you had no such account on file, the password that you attempted to use may also have been exposed if you entered it before typing your credit or debit card number.

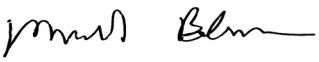
What Are We Doing? We take the security of personal information in our care very seriously. We have security measures in place to protect the data on our systems and we are working to implement additional safeguards to help ensure the privacy and security of information in our care. We are also offering individuals 1 year of complimentary identity monitoring through Kroll. This incident has been reported to your credit card company, and we will be reporting this incident to certain state regulators and law enforcement.

What Can You Do? Please review the enclosed "Steps You Can Take to Help Protect Your Personal Information." We encourage you to activate the complimentary identity monitoring service through Kroll to help monitor your information. In addition, we advise you to report any suspected incidents of identity theft to your credit card company and/or bank, as well as your local law enforcement or the Attorney General.

For More Information: We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance please call our dedicated assistance line at 1-???-???-???? Monday through Friday, 9:00 a.m. to 6:30 p.m., ET. You may also write to Blauer Manufacturing at 20 Aberdeen St, Boston, MA 02215.

Blauer takes the privacy and security of the personal information in our care seriously. We sincerely regret any concern or inconvenience this has caused you.

Sincerely,



Michael Blauer, President
Blauer Manufacturing Co., Inc.

Steps You Can Take to Help Protect Your Personal Information

We advise you to remain vigilant by reviewing all account statements and monitoring free credit reports.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

*You have until **<<Date>>** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze. You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

If you request a security freeze with the above consumer reporting agencies, you will need to provide the following information:

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, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military information, etc.);

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. **For Maryland residents**, the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov. **For New Mexico residents**, 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 may 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 Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. **For New York Residents:** The New York Attorney General provides resources regarding identity theft protection and security breach response at www.ag.ny.gov/internet/privacy-and-identity-theft. The New York Attorney General can be contacted by phone at 1-800-771-7755; toll-free at 1-800-788-9898; and online at www.ag.ny.gov. **For North Carolina Residents:** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov. **For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 24 Rhode Island residents impacted by this incident.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

EXHIBIT B

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data <<b2b_text_1>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Blauer Manufacturing Co., Inc. ("Blauer") is writing to notify you of an incident that may affect the security of the payment card information your organization recently used on our website, www.blauer.com. We take this incident very seriously. We are providing this notice so that organizations who are our customers receive advice comparable to what state breach notification laws require that we provide solely to affected individuals. This letter provides details of the incident and the resources available to your organization to help protect your organization's information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or about October 23, 2019, Blauer identified suspicious activity regarding our online e-commerce website, www.blauer.com. Blauer immediately launched an investigation with the assistance of a third-party forensic firm to determine the nature and scope of the activity. Blauer also took steps to implement additional procedures to further protect the security of customer debit and credit card information on our website.

On or about November 11, 2019, the forensic investigation determined it was possible that certain customer credit and debit card information for transactions that occurred on Blauer's e-commerce website between September 26, 2019 and October 23, 2019 may have been subject to unauthorized access and/or acquisition. While the investigation was unable to definitively confirm whether card data was accessed or taken, Blauer is notifying your organization because we have confirmed that your organization's credit or debit card was used for a transaction on our e-commerce website during the relevant time period.

What Information Was Affected? The information potentially affected includes your organization's name, credit or debit card number, expiration date, and card security code number or CVV as they were entered during an online purchase on <<b2b_text_2 (Date)>>.

In addition, if you attempted from our checkout page to sign into blauer.com when you had no such account on file, the password that you attempted to use may also have been exposed if you entered it before typing your credit or debit card number.

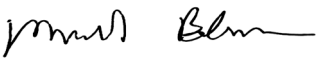
What Are We Doing? We take the security of sensitive information in our care very seriously. We have security measures in place to protect the data on our systems and we are working to implement additional safeguards to help ensure the privacy and security of information in our care. This incident has been reported to your organization's credit card company, and we will be reporting this incident to certain state regulators and law enforcement.

What Can You Do? You can find out more about how to help protect against potential identity theft and fraud in the enclosed Steps Your Organization Can Take To Better Protect Its Information.

For More Information: We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance please call our dedicated assistance line at 1-???-???-???? Monday through Friday, 9:00 a.m. to 6:30 p.m., ET. You may also write to Blauer Manufacturing at 20 Aberdeen St, Boston, MA 02215.

Blauer takes the privacy and security of your organization's information in our care seriously. We sincerely regret any concern or inconvenience this has caused you.

Sincerely,



Michael Blauer, President
Blauer Manufacturing Co., Inc.

STEPS YOUR ORGANIZATION CAN TAKE TO BETTER PROTECT ITS INFORMATION

We encourage your organization to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

Although we have no reason to believe that your organization's information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your organization's name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland-based organizations, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New York-based organizations, The New York Attorney General provides resources regarding identity theft protection and security breach response at www.ag.ny.gov/internet/privacy-and-identity-theft. The New York Attorney General can be contacted by phone at 1-800-771-7755; toll-free at 1-800-788-9898; and online at www.ag.ny.gov.

For North Carolina-based organizations: the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

You may contact the three major credit bureaus directly using the contact information below to request a free copy of your credit report.

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com	www.transunion.com	www.equifax.com

For Rhode Island-based organizations: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.