

JONATHAN E. DAVIS
Attorney at Law

7 Times Square, Times Square Tower
New York, NY 10036
T: (212) 297-2473 F: (212) 298-9958
jdavis@daypitney.com

December 30, 2018

Hon. Gordon McDonald
Attorney General
State of New Hampshire
33 Capitol Street
Concord, NH 03301
Attention: Consumer Protection Unit

Re: **Notice of Security Breach**

Dear Sir:

Day Pitney LLP represents Blauer Manufacturing Company 20 Aberdeen St, Boston, MA 02215 ("Blauer"). We respectfully submit this letter to notify your office of an incident that likely affects the security of personal information relating to 7 individuals who are residents of New Hampshire. We further and voluntarily disclose that the incident also likely affected the security of identifying information of an organization based in the state. Blauer reserves all rights and defenses regarding the application of New Hampshire law or personal jurisdiction in making this submission.

Nature of the Breach Of Security

Blauer designs and sells tactical gear and apparel to first responders and other interested customers. It operates a website at www.blauer.com ("Blauer.com") through which customers may order merchandise. On or about September 25, 2018, Blauer discovered that unknown intruders had installed malicious software ("malware") in a part of Blauer.com that handles online retail orders. Blauer took steps the same day to disable the malware. We also promptly retained outside forensic investigators to evaluate that malware, its duration and its operation. On October 30, 2018, based on the outside investigators' findings, Blauer determined that the malware had been installed by unknown intruders on September 13, 2018, and had remained active until September 25, 2018. While the malware was active, if a retail customer submitted an online checkout form into which he or she had typed his or her credit card information, all of the details entered into the form would be transmitted to the intruders at the same time as the customer's card details were sent to Blauer's payment processor and

December 30, 2018

Page 2

other order details were sent to Blauer. The investigation indicates that between September 13, 2018 and September 25, 2018, the malware's reprogramming likely worked as the intruders had intended.

Immediately upon confirming the duration of the malware's operation, Blauer took steps to confirm the identities and addresses of the individuals whose personally identifiable information was likely exposed in the course of placing orders on Blauer.com between September 13, 2018 and September 25, 2018. Blauer began providing statutorily-required notice to the individuals affected by this incident as soon as their individual status and personal address information could be confirmed. With respect to residents of this state, the information affected by the breach of security includes (1) name together with credit card numbers and credit verification ("CV") codes and, (2) only when customers requested new Blauer.com accounts when they placed their orders, the account passwords that they selected. Although such passwords are not statutorily protected, Blauer notified individuals residing in this state who included password requests within their likely compromised orders. To date, Blauer has not received any reports of the misuse of any of this information.

Notice to New Hampshire Residents

Blauer is commencing tomorrow, December 31, 2018, to issue written notice of this incident to affected individuals, including 7 residents of this state whose statutorily-protected personal information was likely exposed. At the same time, we also voluntarily providing written notice of this incident to an organization in this state, whose information was also likely affected. Written notice to those individuals and that organization is being provided in substantially the same forms as the letters attached at *Exhibits A and B*, respectively.

Other Steps Taken and To Be Taken

Upon discovering the malware, Blauer moved quickly to disable it, determine its spread, duration and functions, identify individuals and organizations likely to have been affected, put in place resources to assist them, and provide them with notice of this incident. Blauer is also working to implement additional safeguards to protect the security of information in its system.

Blauer is providing written notice to those individuals who are likely affected by this incident. This notice includes an offer of prepaid access to one year of credit and identity monitoring services, including identity restoration services through Kroll, and the contact information for a dedicated call center for likely affected individuals to contact with questions or concerns regarding this incident. Additionally, Blauer is providing the same individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer

December 30, 2018

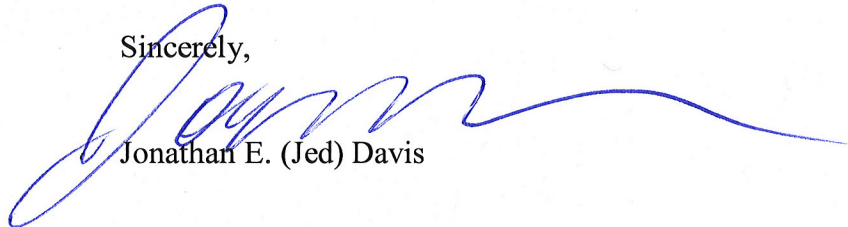
Page 3

reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. In addition, we are providing likely affected organizations with notifications similar to those provided to individuals with parallel guidance on how to better protect against identity theft and fraud, which regulators to contact, and how.

Contact Information

My contact information appears at the top of this letter. Please address any questions or concerns about the above incident or Blauer's response to Day Pitney LLP and me.

Sincerely,



Jonathan E. (Jed) Davis

EXHIBIT A



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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

With regret, Blauer Manufacturing Co. ("Blauer") writes to inform you of a recent event in which unauthorized third parties likely compromised some of your personal information, including credit card information, when you ordered merchandise from us. This letter provides you with a summary of the breach of security in issue, our response and additional steps that you may take to better protect yourself against the risk of identity theft and fraud.

What Happened? On September 25, 2018, Blauer discovered that unknown intruders had installed malicious software ("malware") in a part of the online platform at www.blauer.com (Blauer.com) that handles online retail orders. Blauer took steps the same day to disable the malware. We also promptly retained outside forensic investigators to evaluate that malware, its duration and its operation. On October 30, 2018, based on the outside investigators' findings, Blauer determined that the malware had been installed by unknown intruders on September 13, 2018, and had remained active until September 25, 2018. While the malware was active, if a retail customer submitted an online checkout form into which he or she had typed his or her credit card information, all of the details entered into the form would be transmitted to the intruders at the same time as the customer's card details were sent to Blauer's payment processor and other order details were sent to Blauer. The investigation indicates that between September 13, 2018 and September 25, 2018, the malware's reprogramming likely worked as the intruders had intended.

What Information Was Involved? It is likely that the malware installed by the intruders enabled them to acquire the credit card account number and credit verification (CV) code included in a retail order that you submitted to Blauer.com sometime between September 13, 2018 and September 25, 2018. Ordinarily, only our outside payment processor receives customer-supplied card information and only it can store that data and then only with your advance consent. The malware implanted by the intruders was designed to circumvent those controls, however. Upon detecting that the form contained a manually-entered card number and CV code, the malware likely caused the form to transmit to the intruders all of your order's details, including the credit card information.

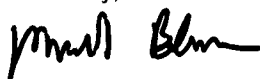
What We Are Doing. We take this incident and the security of your personal information seriously. Upon discovering the malware, we immediately took steps to disable it. Moreover, as a follow-up to the outside forensic investigation and as part of our ongoing commitment to the privacy of personal information in our care, we have examined and continue to assess our systems, policies and procedures, have implemented additional safeguards and are evaluating still more. We are also notifying state regulators, as required. As an added precaution, we also are offering complimentary access to 12 months of identity monitoring, fraud consultation and identity theft restoration services through Kroll.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed Steps You Can Take to Prevent Fraud and Identity Theft. There you will also find more information on the identity monitoring services we are offering and how to enroll.

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, please call our dedicated assistance line at 1-866-775-4209, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your Kroll membership number ready. This number can be found below. You may also write me in care of Blauer Manufacturing Co., 20 Aberdeen St, Boston, MA 02215.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,



Michael Blauer
President

STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

We have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. 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, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **March 31, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

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

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

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, 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 identification, etc.);
7. 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.

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

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal 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 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 consumer reporting agencies, 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 North Carolina residents, 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.

For Maryland residents, 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 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 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 four Rhode Island resident individuals impacted by this incident.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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 Internet Explorer, Chrome, Firefox, and Safari. 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 A

CONTINUES ON NEXT PAGE



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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

With regret, Blauer Manufacturing Co. ("Blauer") writes to inform you of a recent event in which unauthorized third parties likely compromised some of your personal information, including credit card information and an account password, when you ordered merchandise from us. This letter provides you with a summary of the breach of security in issue, our response and additional steps that you may take to better protect yourself against the risk of identity theft and fraud.

What Happened? On September 25, 2018, Blauer discovered that unknown intruders had installed malicious software ("malware") in a part of the online platform at www.blauer.com (Blauer.com) that handles online retail orders. Blauer took steps the same day to disable the malware. We also promptly retained outside forensic investigators to evaluate that malware, its duration and its operation. On October 30, 2018, based on the outside investigators' findings, Blauer determined that the malware had been installed by unknown intruders on September 13, 2018, and had remained active until September 25, 2018. While the malware was active, if a retail customer submitted an online checkout form into which he or she had typed his or her credit card information, all of the details entered into the form would be transmitted to the intruders at the same time as the customer's card details were sent to Blauer's payment processor and other order details were sent to Blauer. The investigation indicates that between September 13, 2018 and September 25, 2018, the malware's reprogramming likely worked as the intruders had intended.

What Information Was Involved? It is likely that the malware installed by the intruders enabled them to acquire (1) the credit card account number and credit verification (CV) code included in a retail order that you submitted to Blauer.com sometime between September 13, 2018 and September 25, 2018, and (2) a password that you had tasked us in that order to reserve for your use. Ordinarily, only our outside payment processor receives customer-supplied card information and only it can store that data and then only with your advance consent. The malware implanted by the intruders was designed to circumvent those controls, however. Upon detecting that the form contained a manually-entered card number and CV code, the malware likely caused the form to transmit to the intruders all of your order's details, including the credit card information. Moreover, the data forwarded to the intruders likely also included a password that you had directed that we use to create a new online account for you at Blauer.com. <<ClientDef1(Variable Text)>>

What We Are Doing. We take this incident and the security of your personal information seriously. Upon discovering the malware, we immediately took steps to disable it. Moreover, as a follow-up to the outside forensic investigation and as part of our ongoing commitment to the privacy of personal information in our care, we have examined and continue to assess our systems, policies and procedures, have implemented additional safeguards and are evaluating still more. We are also notifying state regulators, as required. As an added precaution, we also are offering complimentary access to 12 months of identity monitoring, fraud consultation and identity theft restoration services through Kroll.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed Steps You Can Take to Prevent Fraud and Identity Theft. There you will also find more information on the identity monitoring services we are offering and how to enroll.

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, please call our dedicated assistance line at 1-866-775-4209, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your Kroll membership number ready. This number can be found below. You may also write me in care of Blauer Manufacturing Co., 20 Aberdeen St, Boston, MA 02215.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,



Michael Blauer
President

STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

We have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. 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, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **March 31, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

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

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

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, 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 identification, etc.);
7. 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.

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

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal 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 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 consumer reporting agencies, 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 North Carolina residents, 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.

For Maryland residents, 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 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 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 four Rhode Island resident individuals impacted by this incident.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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 Internet Explorer, Chrome, Firefox, and Safari. 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)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<ClientDef1(Entity Name)>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

With regret, Blauer Manufacturing Co. ("Blauer") writes to inform you of a recent event in which unauthorized third parties likely compromised some of your organization's identification information, including credit card information, when you ordered merchandise from us. We are providing this notice so that organizations who are our customers receive advice similar to what state breach notification laws require that we provide solely to affected individuals. This letter provides you with a summary of the breach of security in issue, our response and additional steps that you may take to better protect your organization against the risk of impersonation and fraud.

What Happened? On September 25, 2018, Blauer discovered that unknown intruders had installed malicious software ("malware") in a part of the online platform at www.blauer.com (Blauer.com) that handles online retail orders. Blauer took steps the same day to disable the malware. We also promptly retained outside forensic investigators to evaluate that malware, its duration and its operation. On October 30, 2018, based on the outside investigators' findings, Blauer determined that the malware had been installed by unknown intruders on September 13, 2018, and had remained active until September 25, 2018. While the malware was active, if a retail customer submitted an online checkout form into which he or she had typed his or her credit card information, all of the details entered into the form would be transmitted to the intruders when the customer's card details were sent to Blauer's payment processor and other order details were sent to Blauer. The investigation indicates that between September 13, 2018 and September 25, 2018, the malware's reprogramming likely worked as the intruders had intended.

What Information Was Involved? It is likely that the malware installed by the intruders enabled them to acquire the credit card account number and credit verification (CV) code that your organization included in a retail order submitted to Blauer.com sometime between September 13, 2018 and September 25, 2018. Ordinarily, only our outside payment processor receives customer-supplied card information and only it can store that data and then only with your advance consent. The malware implanted by the intruders was designed to override those controls, however. Upon detecting that the form contained a manually-entered card number and CV code, the malware likely caused the form to transmit to the intruders all of your order's details, including the credit card information.

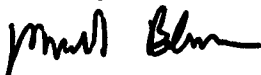
What We Are Doing. We take this incident and the security of your organization's information seriously. Upon discovering the malware, we immediately took steps to disable it. Moreover, as a follow-up to the outside forensic investigation and as part of our ongoing commitment to the privacy of identification information in our care, we have examined and continue to assess our systems, policies and procedures, have implemented additional safeguards and are evaluating still more. We are also notifying state regulators, as required with respect to affected individuals and voluntarily with respect to affected businesses.

What You Can Do. You can find out more about how to 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, please call our dedicated assistance line at 1-866-775-4209, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. You may also write me in care of Blauer Manufacturing Co., 20 Aberdeen St, Boston, MA 02215.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Michael Blauer", written in a cursive style.

Michael Blauer
President

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 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.

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 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.