

23527



[Date]  
[First Name Last Name]  
[Address]  
[City, State Zip]

Dear [First Name]

### **Notification of Security Incident**

Derby Industries, LLC (“Derby”) takes the security and protection of your personal information seriously. We are providing you with this letter to make you aware of a security incident that may have resulted in the unauthorized access or viewing of your personal information.

### ***What Happened***

On September 4, 2021, we first learned of a security incident that disrupted access to Derby information systems (the “Incident”). The disruption to Derby information systems lasted from September 4, 2021 until access was restored on September 8, 2021. Upon discovery of the Incident, Derby immediately engaged a trusted third-party forensics firm to assist in ending the disruption to Derby information systems as well as understanding the scope and impact of the Incident. Based on our investigation, we learned that the attack was made possible by an unauthorized individual through malicious software on our internal systems and that the initial instance of unauthorized access began on August 26, 2021. We have worked with our third-party forensics firm to secure all systems, remediate any risks, and successfully and securely bring our systems back online, while adopting additional technical and organizational tools to address system vulnerabilities. On October 13, 2021, Derby learned that in addition to the disrupted access to Derby information systems, the Incident may have also resulted in the unauthorized access, viewing, or removal of your personal information from our systems. Once aware of the Incident and its potential impact on personal information, we began analyzing the impacted files to better understand what personal information was potentially at risk, and provide notice to individuals and governmental authorities, as applicable.

### ***What Information Was Involved***

Although Derby has confirmed unauthorized access to its information systems between August 26, 2021 and September 8, 2021, there is no conclusive evidence that the intruder has used any of the accessible personal information. We are informing you that the intruder may have accessed, viewed, or removed from our systems the following categories of personal information: first and last name; mailing address; date of birth; bank account number and routing number; and Social Security number.

### ***What We Did and What We Are Doing***

Upon learning of the Incident, we immediately took protective measures to understand the Incident’s scope and to secure our systems and data. We engaged a third-party forensic firm to investigate the Incident, identify the root cause, and determine the scope of accessible information. We have carefully brought our systems back online, and we continue to closely monitor our network and information systems for unusual activity. Additionally, we are continuing our due diligence efforts, including engaging as appropriate, additional resources and experts and evaluating the extent of risk to personal information.

We will continue to implement the recommendations from our third-party forensics firm to further improve Derby’s administrative, technical, and physical safeguards.

### ***What You Can Do***

We sincerely regret any concern this causes you and any inconvenience resulting from this Incident. Although we have not received reports or indication of such activity, the risks related to unauthorized use of sensitive information, such as Social Security numbers or bank accounting numbers and routing numbers, may include

identity theft, financial fraud, and tax fraud. We encourage you to remain vigilant in reviewing activity on all accounts in which you keep sensitive information, including your credit files. We will continue to keep you posted on any applicable updates.

Please also take care and attention when submitting tax returns to protect against possible fraudulent submissions made on your behalf. To assist you in this effort, we have provided complimentary credit monitoring and ID theft prevention services through Experian. You can access those benefits by following the instructions in the attached letter from Experian.

If you have concerns about identity theft, you can contact local law enforcement and file a police report. You can also contact your state's Attorney General, as well as the Federal Trade Commission or one of the credit bureaus for more information about how to protect your identity.

***For More Information***

You can place an identity theft/fraud alert, get credit freeze information for your state, or order a free credit report by calling any of the following credit reporting agencies at one of the phone numbers listed below or visiting their respective websites.

Equifax - <u>1-888-766-0008</u> P.O. Box 740256 Atlanta, GA 30348 <a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	Experian - <u>1-888-397-3742</u> P.O. Box 4500 Allen, TX 75013 <a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	Trans Union - <u>1-800-680-7289</u> P.O. Box 2000 Chester, PA 19022 <a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
--	---	--

Credit Reports. You can request credit reports be sent to you free of charge from all three credit bureaus. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Periodically checking your credit reports can help you spot problems and address them quickly.

Fraud Alerts. You can place a fraud alert with the credit bureaus free of charge. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Security Freeze. Under state law, a security freeze (or a credit freeze) prohibits a credit bureau from releasing any information from a consumer's credit report without written authorization. There is no fee associated with freezing or thawing your credit. The process of freezing your credit takes only a few minutes. You must contact each credit bureau individually to freeze your credit with each bureau. To place a security freeze, you may need to provide the following information:

1. Your full name;
2. Social Security number;
3. Date of birth;
4. Mobile number;
5. Current postal address;
6. Email address; and
7. Any other information that the credit bureau may require.

The credit bureaus have one business day after your request to place a security freeze if made by telephone or secure electronic means. If the request is made by mail, the credit bureaus have three business days. The credit bureaus must also send written confirmation to you within five business days.

To lift the security freeze, in order to allow a specific entity or individual access to your credit report, you must apply online, call, or send a written request to the credit bureaus by mail. When you contact a credit bureau to lift the security freeze, you will need to include proper identification (name, address, and Social Security number) and the PIN number or password that was provided to you (if provided) when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. If you request a credit thaw online or by phone, the credit bureaus are required by law to complete the request within one hour. If you request the thaw by regular mail, the credit bureaus have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

The Federal Trade Commission (FTC) provides more information about how to protect your identity at either <https://www.ftc.gov/> or <https://www.identitytheft.gov/>. You may also find additional information on any applicable rights under the Fair Credit Reporting Act. You can contact the FTC using the information below.

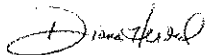
Federal Trade Commission - 1-202-326-2222  
 Bureau of Consumer Protection  
 600 Pennsylvania Avenue, NW  
 Washington, DC 20580

<p><u>For Maryland Residents:</u> You may also contact the Maryland Attorney General's Office for more information about how to protect your identity by using the information below:</p> <p>Attorney General Brain E. Frosh        200 St. Paul Place        Baltimore, MD 21202        Phone: 410-528-8662        Website: <a href="https://www.marylandattorneygeneral.gov/">https://www.marylandattorneygeneral.gov/</a></p>	<p><u>For New York Residents:</u> You may also contact the New York Attorney General's Office for more information about how to protect your identity by using the information below:</p> <p>Attorney General Letitia James        Toll Free Phone Number:        (800) 771-7755        Website: <a href="https://ag.ny.gov/">https://ag.ny.gov/</a></p>
<p><u>For North Carolina Residents:</u> You may also contact the North Carolina Attorney General's Office for more information about how to protect your identity by using the information below:</p> <p>Attorney General Josh Stein        9001 Mail Service Center        Raleigh, NC 27699-9001        Toll Free in NC: 1-877-566-7226        Outside NC: 919-716-6000        Website: <a href="https://ncdoj.gov/">https://ncdoj.gov/</a></p>	<p><u>For Washington D.C. Residents:</u> You may also contact the Washington D.C. Attorney General's Office for more information about how to protect your identity by using the information below:</p> <p>Attorney General Karl A. Racine        400 6th St. NW        Washington, D.C. 20001        Phone: (202)-727-3400        Website: <a href="https://oag.dc.gov/">https://oag.dc.gov/</a></p>

Again, we sincerely regret that this Incident has occurred. If you have any questions, please contact us at:

Contact: Derby Industries, LLC  
 Email: [securityincident@derbyllc.com](mailto:securityincident@derbyllc.com)  
 Telephone: 1-877-759-8882  
 Address: 4451 Robards Lane, Louisville, KY 40218

Sincerely,



Diana Herold  
 President

## Experian – Credit Monitoring Information

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** February 28, 2022 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code:** [code]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-759-8882 by February 28, 2022. Be prepared to provide engagement number [engagement #] as proof of eligibility for the identity restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-759-8882. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for three months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

\*Offline members will be eligible to call for additional reports after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## Derby Industries LLC – Massachusetts Supporting Document

### **General Description**

On September 4, 2021, Derby first learned of a security incident that disrupted access to Derby information systems (the “Incident”). The disruption to Derby information systems lasted from September 4, 2021 until access was restored on September 8, 2021. Upon discovery of the Incident, Derby immediately engaged a trusted third-party forensics firm to assist in ending the disruption to Derby information systems as well as understanding the scope and impact of the Incident. Based on Derby’s investigation, it learned that the attack was made possible by an unauthorized individual through malicious software on its internal systems and that the initial instance of unauthorized access began on August 26, 2021. Derby has worked with its third-party forensics firm to secure all systems, remediate any risks, and successfully and securely bring its systems back online, while adopting additional technical and organizational tools to address system vulnerabilities. On October 13, 2021, Derby learned that in addition to the disrupted access to Derby information systems, the Incident may have also resulted in the unauthorized access, viewing, or removal of personal information from its systems. Once aware of the Incident and its potential impact on personal information, Derby began analyzing the impacted files to better understand what personal information was potentially at risk, and provide notice to individuals and governmental authorities, as applicable.

### **Steps Taken To Mitigate Future Risk**

Upon learning of the Incident, Derby immediately took protective measures to understand the Incident’s scope and to secure our systems and data. Derby engaged a third-party forensic firm to investigate the Incident, identify the root cause, and determine the scope of accessible information. Derby has carefully brought its systems back online, and Derby continues to closely monitor its network and information systems for unusual activity. Additionally, Derby is continuing its due diligence efforts, including engaging as appropriate, additional resources and experts and evaluating the extent of risk to personal information.

To date, Derby has deployed recommended endpoint detection and response tools to perform remote threat hunting, containment, mitigation, and 24/7 security monitoring within its information resources. Derby will continue to implement the recommendations from its third-party forensics firm to further improve Derby’s administrative, technical, and physical safeguards.

### **Number of Massachusetts Residents Affected**

Derby identified 1 Massachusetts resident potentially affected by the Incident.

### **Date/Types/Plan for Consumer Data Security Breach Notification**

Written notice was mailed out to individuals affected by the Incident on November 12, 2021. As mentioned above, although the Incident was initially discovered on September 4, 2021, Derby’s investigation did not conclude that access or acquisition to personal information was possible until October 13, 2021. Since October 13, 2021, Derby conducted due diligence to determine the extent to which personal information may have been at risk as well as the contact information of potentially affected data subjects. On November 1, 2021, Derby identified 1 Massachusetts resident potentially affected by the Incident. We will provide additional updates to consumers as applicable, but at this time do not foresee any need for subsequent communication.