ıber 16, 2020

18167

[redacted]

NOTICE OF DATA BREACH

[redacted]

:atly appreciate your relationship with Flexsteel Industries, Inc. ("Flexsteel"). We respect and p
vacy of your information, and we are writing to let you know about a data security incident tha
: unauthorized access to your personal information that was contained in email accounts maint
xsteel.

T INFORMATION WAS INVOLVED?

nail accounts that were compromised included documents that potentially contained some or
lowing information: name, address, bank account number, routing number, and social secur
ument identification number. We have no evidence that the attacker has used any of this inform
our knowledge, no other personal information was contained in the compromised email accou

T WE ARE DOING

liately upon learning of the incident, Flexsteel began an investigation to investigate the nature
and what information, if any, could have been compromised. Flexsteel also contacted the recip
phishing email and instructed them to delete the email and change their passwords if they opene
ous attachment. The Federal Bureau of Investigation has been notified of the incident.

:el took further steps to eradicate the intrusion, including requiring all employees to change
ords and implementing other network safeguards and enhancing its company-wide training
y procedures to help prevent future attacks and to better protect the privacy of our valued empl
siness partners.

ıber 16, 2020

[redacted]

NOTICE OF DATA BREACH

[redacted]

ɜatly appreciate your relationship with Flexsteel Industries, Inc. ("Flexsteel"). We respect and p
vacy of your information, and we are writing to let you know about a data security incident tha
ɛ unauthorized access to your personal information that was contained in email accounts maint
xsteel.

T INFORMATION WAS INVOLVED?

nail accounts that were compromised included documents that potentially contained some or
lowing information: name, address, bank account number, routing number, and social secur
ument identification number. We have no evidence that the attacker has used any of this inform
our knowledge, no other personal information was contained in the compromised email accou

T WE ARE DOING

liately upon learning of the incident, Flexsteel began an investigation to investigate the nature
and what information, if any, could have been compromised. Flexsteel also contacted the recip
ɔhishing email and instructed them to delete the email and change their passwords if they opene
ɔus attachment. The Federal Bureau of Investigation has been notified of the incident.

ɜel took further steps to eradicate the intrusion, including requiring all employees to change
ɹrds and implementing other network safeguards and enhancing its company-wide training
y procedures to help prevent future attacks and to better protect the privacy of our valued empl
siness partners.

WHAT YOU CAN DO

CONTACT YOUR FINANCIAL INSTITUTION

Because your bank account and routing numbers may have been accessed, we recommend that you contact your financial institution to notify them of the situation and change your account and routing numbers. 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.

NOTIFY LAW ENFORCEMENT OF SUSPICIOUS ACTIVITY

As a precautionary measure, we recommend that you remain vigilant by reviewing your personal accounts. 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's office and the Federal Trade Commission (FTC). You have the right to file or obtain a police report regarding the breach.

To report fraudulent activity with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Reports 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.

SECURE YOUR ONLINE ACCOUNTS

Because the breach involved a malicious email, we recommend you promptly change your username or password and security question or answer, as applicable, and take any other steps appropriate to protect all online accounts for which you use the same user name or email address and password or security question and answer.

WHAT WE ARE DOING TO PROTECT YOUR INFORMATION

We are offering identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to https://app.myidcare.com/account-creation/protect and using the following Enrollment Code: [redacted] MyIDCare experts are available Monday through Friday from 5 am - 5 pm Pacific Time. Please note the deadline to enroll is May 30, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

FOR MORE INFORMATION

For further information and assistance, please contact us at 1-888-790-0167.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code contained in this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-800-939-4170 or go to https://app.myidcare.com/account-creation/protect for assistance or for any additional questions you may have.

We also 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 http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

FRAUD ALERT AND SECURITY FREEZE

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.

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 above.

er to request a security freeze, you will need to provide the following information:

Your full name (including middle initial as well as J., Sr., II, III, etc.);
Social security number;
Date of birth;
If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
Proof of current address, such as a current utility bill or telephone bill;
A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
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.

redit reporting agencies have 1 to 3 business days after receiving your request to place a security on your credit file report, based upon the method of the request. The credit bureaus must also send n confirmation to you within 5 business days and provide you with the process by which you may ve the security freeze, including an authentication mechanism. Upon receiving a direct request from o remove a security freeze and upon receiving proper identification from you, the consumer reporting y shall remove a security freeze within 1 hour after receiving the request by telephone for removal or n 3 business days after receiving the request by mail for removal.

teel values your privacy and deeply regrets that this incident occurred.

rely,

ael J McClaflin
Information and Technology Officer
teel Industries, Inc.
ell Street | Dubuque, IA 52001
flexsteel.com

MyIDCare

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://ide.myidcare.com/*customending*; https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-9939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

specific additional rights pursuant to the Fair Credit Reporting Act. You can 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have