

Company Letterhead

[DATE]

[CONTACT INFORMATION]

Re: An Important Message

Dear <<Name 1>>

Spiezle Group, Inc. ("Spiezle") is writing to inform you of a recent event that potentially may impact the security of some of your personal information that you and/or your dependents provided to Spiezle as needed in the course of your employment with Spiezle. While we are unaware of any actual misuse of your personal information, we are providing you with information about the incident, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

WHAT HAPPENED?

On June 25, 2021, Spiezle discovered that a malware virus was identified across Spiezle's Information Technology network environment ("Incident"). Upon discovering the Incident, Spiezle engaged a third party forensic firm who, together with Spiezle's internal technical team, were able to respond to the Incident. The forensic firm has identified that a third-party deployed the malware. The team was able to extract the third-party from Spiezle's system and harden Spiezle's defenses against future unauthorized activity.

WHAT INFORMATION WAS INVOLVED?

While employee files have always been segregated on a restricted access drive, as a result of the Incident, the third-party actor may have accessed and downloaded certain internal employee files containing personal information such as your name, social security number, date of birth and employment start date.

WHAT ARE WE DOING?

Spiezle engaged a third party forensic firm who, together with Spiezle's internal technical team, engaged appropriate defenses measures against future unauthorized activity. Among other things, Spiezle deployed anti-malware software, reinforced its firewalls, is updating its policies and procedures and is in the process of evaluating its information security program to determine if additional controls should be implemented to reduce the risk of a similar incident occurring in the future.

Spiezle also has made arrangements for you, and your dependents who may have provided personal information including a social security number to Spiezle, to receive a twelve (12) month membership in Trans Union's *myTrueIdentity* credit monitoring services. ***The details of how to obtain Trans Union's myTrueIdentity services are attached to this letter.***

We have also arranged for a telephone support line for inquiries related to this Incident. A team of qualified support agents are available Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding U.S. holidays at _____.

WHAT CAN YOU DO?

Outlined below are a number of ways that you can protect yourself.

- 1. Sign Up for Credit Monitoring.** We encourage you to take advantage of the complimentary credit monitoring services we are providing. As noted above, a description of the credit monitoring services is provided in the attached material.
- 2. Monitor Account Statements and Free Credit Reports.** You should remain vigilant for incidents of financial fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports.
- 3. Contact the Federal Trade Commission, Law Enforcement, and Credit Bureaus.** To report identity theft incidents or learn about steps you can take to protect yourself from identity theft, you may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement. To learn more, you can go to the FTC's websites at www.IdentityTheft.gov and www.ftc.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 680-7289
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance
Atlanta, GA	Allen, TX 75013	Division
303740241	www.experian.com	P.O. Box 2000
www.equifax.com		Chester, PA 19016-2000
		www.transunion.com

- 4. Obtain Free Copies of Credit Reports.** You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. TransUnion, Equifax and Experian are offering free weekly credit reports on www.AnnualCreditReport.com through April 20, 2022, as part of their efforts to support all Americans during the Covid-19 pandemic. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228.
- 5. Additional Rights Under the FCRA.** You have rights pursuant to the FCRA, 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 FCRA, 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 violators. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

- 6. Request Fraud Alerts and Security Freezes.** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three national consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies’ websites or over the phone, using the contact information below:

Equifax
(800) 525-6285
P.O. Box 740241
Atlanta, GA
303740241
www.equifax.com

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance
Division
P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com

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. The addresses where you have lived over the prior two 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.); and
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.

If the request for a security freeze is made by toll-free number or secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the security freeze on your credit report. If the request is made by mail, the credit reporting agencies have three (3) business days after receiving the request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a mechanism to enable you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

To remove a security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. There is no fee to place or lift a security freeze.

- 7. Additional Information for Certain States.** Please review the final pages of this letter for additional information for certain states.

FOR MORE INFORMATION

Again, please do not hesitate to contact our support agents if you have any questions or concerns by calling [REDACTED]. Our support agents are available Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding U.S. holidays.

Sincerely,

Spiegle Group, Inc.
Encls.

ADDITIONAL INFORMATION FOR CERTAIN STATES

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

For residents of the District of Columbia: For additional information about steps to take to avoid identity theft, you may contact the District of Columbia Attorney General at 441 4th Street, NW, Washington, DC 20001, (202) 727-3400, dc.oag@dc.gov. Additionally, you may also contact the Office of Consumer Protection at Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, (202) 442-9828, consumer.protection@dc.gov.

For residents of Iowa: To report suspected incidents of identity theft, you may contact local law enforcement or the Iowa Attorney General's Office. You can contact the Iowa Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 2815164, <http://www.iowaattorneygeneral.gov/>.

For residents of Maryland: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
<http://www.ftc.gov/idtheft/>

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

For residents of Massachusetts: In addition to the above steps, under Massachusetts law, you have a right to obtain a police report with regard to the Incident. In addition, if you are the victim of identity theft, you have a right to file a police report and obtain a copy of it.

For residents of North Carolina: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6400
<http://www.ncdoj.com>

For residents of New York: You may obtain security breach response information and identity theft and protection information from the FTC, the Department of State, Division of Consumer Protection, and the New York Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
(877) IDTHEFT (4384338)
www.consumer.gov/idtheft

Department of State
Division of Consumer Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

Office of the
Attorney General
(800) 771-7755
<https://ag.ny.gov/>

For residents of Oregon: You may report suspected identity theft to law enforcement, including You may report suspected identity theft to law enforcement, including the Oregon Attorney General and the FTC. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
<http://www.ftc.gov/idtheft/>

Oregon Department of Justice
1162 Court St. NE
Salem, Oregon 97301
(877) 877-9392
<https://www.doj.state.or.us>

For residents of Rhode Island: You have the right to file or obtain a police report (should one be filed) and request a free security freeze, free of charge, as described above. Placing a security freeze may require that you provide certain personal information (e.g., name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. You may also contact the Attorney General's office at: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400, <http://www.riag.ri.gov/>.

[TRANSUNION INFORMATION]