

RECEIVED

AUG 29 2022

# Frankfurt Kurnit Klein + Selz PC CONSUMER PROTECTION

Caren Decter  
28 Liberty Street, New York, New York 10005  
T (212) 705-4833 F (347) 438-2133  
cdecter@fkks.com

August 26, 2022

**VIA FEDEX**

The Honorable John M. Formella  
Attorney General of New Hampshire  
Office of the Attorney General  
33 Capitol St.  
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

On July 29, 2022, Semikron, Inc. (“Semikron”) learned of a ransomware attack on its system. Upon discovery of the incident, Semikron hired an outside forensic expert to determine whether the incident resulted in the unauthorized access to any personal information.

Based on Semikron’s investigation to date, we believe there may have been access to the following information: name, date of birth, and Social Security numbers.

As a precaution, on August 26, 2022, Semikron will formally notify via U.S. mail or other authorized delivery method those individuals who may have been affected by the incident—including one hundred and twenty three (123) New Hampshire residents—in substantially the same form as the letter attached hereto. Semikron is also providing free credit monitoring services to all United States residents who may have been affected by the incident.

Please do not hesitate to contact me at (212) 705-4833 if you have any questions regarding this matter.

Very truly yours,

Caren Decter

Enclosure



11 Executive Drive  
Hudson, NH 03051  
603-883-8102

To Enroll, Please Call:  
1-800-939-4170  
Or Visit:  
<https://app.idx.us/account-creation/protect>  
Enrollment Code:  
«Enrollment\_Code»

«First\_Name\_DC» «Last\_Name\_DC»  
«Primary\_Address\_Line\_1» «Primary\_Address\_Line\_2»  
«Primary\_City», «Primary\_State» «Primary\_ZIP\_Code»

<<Date>>

### Notice of Data Breach

Dear «First\_Name\_DC» «Last\_Name\_DC»,

On behalf of Semikron, Inc. (“Semikron”), I write to inform you of a security incident that we believe may have involved your personal information. This incident was a “ransomware” attack, as described below, and the attacker was seeking a ransom payment. We are sending this letter to you comply with our legal obligations but also to provide you with information regarding what happened and additional steps we are taking to protect your personal information.

#### What Happened

On July 29, 2022, we became aware that an unauthorized party had obtained access to and installed ransomware on certain of our systems. Upon learning of the unauthorized access, Semikron immediately deactivated VPN access. We also retained forensic experts who launched an investigation. As a result of our investigation, we confirmed that personal information relating to you was stored on the affected systems. This information may have been accessed and we are sending this notice in an abundance of caution.

#### What Information Was Involved

The personal information involved may have included your name, date of birth, and Social Security number.

#### What We Are Doing

We are taking several steps to further strengthen and enhance our information security controls and procedures, including working with independent third party security consultants.

In addition, we are offering identity theft protection and credit monitoring services through IDX. IDX identity protection services include: 24 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, and ID theft recovery services. These services are not being offered to comply with our legal obligations, but otherwise as a courtesy and at no cost to you.

#### What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm ET. Please note the deadline to enroll is December 16, 2022.

Classified as Business

Also, enclosed is an "Information about Identity Theft Protection" guide, which describes recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring service with IDX.

**For More Information**

We are taking this matter very seriously and we apologize for any inconvenience it may cause you. Please call 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

Dr. Frank Pfeiffer  
President/CEO

(Enclosure)

CONFIDENTIAL

### Information about Identity Theft Protection

You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

**Equifax**, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, [www.equifax.com](http://www.equifax.com)

**Experian**, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com)

**TransUnion**, P.O. Box 6790, Fullerton, CA , 1-800-916-8800, [www.transunion.com](http://www.transunion.com)

Vigilance with respect to reviewing account statements and credit reports may help reduce fraud or identity theft. Any suspicious activity or suspected identity theft may be reported to the proper law enforcement authorities, including local law enforcement, your state's Attorney General, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft). Residents of the following states may also obtain information about preventing and avoiding identity theft by contacting their Attorney General: **New York Residents**: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, Website: <https://ag.ny.gov>, Telephone: 1-800-771-7755; **North Carolina Residents**: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Fraud Alerts:** There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one (1) year. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any one of the three national credit reporting agencies at the toll-free numbers listed below:

**Equifax**  
800-525-6285

**Experian**  
888-397-3742

**TransUnion**  
800-680-7289

**Credit Freezes:** You have the right to put a credit freeze on your credit file so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Placing, temporarily lifting, or removing a credit freeze is free of cost. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Please contact the three major credit reporting companies as specified below to find out more information.

**Equifax Security Freeze**  
P.O. Box 105788  
Atlanta, GA 30348  
[www.equifax.com](http://www.equifax.com)

**Experian Security Freeze**  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

**TransUnion (FVAD)**  
P.O. Box 2000  
Chester, PA 19022-2000  
[freeze.transunion.com](http://freeze.transunion.com)

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above. If you have additional questions about steps you can take to avoid identity theft, you can contact your state Attorney General, or the FTC.