March 14, 2024

VIA ELECTRONIC MAIL

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301
Tel: 603-271-3643
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents ACR Electronics, Inc. ("ACR"), a technology and manufacturing company located in Ft. Lauderdale, Florida, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute.

Nature of the Security Incident

On October 12, 2023, ACR experienced a network disruption in its digital environment. In response, ACR immediately took steps to secure the environment and launched an investigation with the assistance of a leading computer forensics firm to determine what happened and whether sensitive or personal information may have been accessed or acquired during the incident. As a result of the investigation, ACR identified that a limited amount of data may have been accessed or acquired without authorization. ACR then engaged an independent team to conduct a comprehensive review of all potentially affected data, and on March 4, 2024, that review determined that certain personal information was potentially affected. ACR then worked diligently to identify contact information to effectuate notification to these individuals, which was completed on March 13, 2024.

The information affected varied between individuals but may have included

Please note that we have no current evidence to suggest misuse or attempted misuse of personal information involved in the incident.

Number of New Hampshire Residents Involved

On March 13, 2024, ACR notified two (2) New Hampshire residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

In response to the incident, ACR is providing individuals with information about steps that they can take to help protect their personal information, and, out of an abundance of caution, it is also offering individuals complimentary credit monitoring and identity protection services through IDX. Additionally, to help reduce the risk of a similar future incident, ACR has implemented additional technical security measures throughout the environment.

Contact Information

ACR remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at

Sincerely,

Laura K. Funk
Partner
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter

ACR ELECTRONICS, INC.
5757 Ravenswood Rd. Fort Lauderdale, FL33312 - U.S.A
T: +1-954-981-3333 F: +1-954-983-5087
www.ACRARTEX.com

C/O IDX
4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

<<First Name>> <<Last Name>>
<<Address1>>
<<City>>, <<State>> <<Zip Code>>

March 12, 2024

Subject: Notice of Data Security <<variable 1>>

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a data security incident that may have affected your personal information. At ACR Electronics, Inc. ("ACR"), we take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services.

What Happened. On October 12, 2023, ACR experienced a network disruption and immediately initiated an investigation of the matter. We engaged cybersecurity experts to assist with the process. The investigation determined that certain files may have been accessed or acquired without authorization. After an independent data review team conducted a thorough review of those files, on or about March 4, 2024, some of your personal information was identified as being contained within the potentially affected data.

What Information Was Involved. The information involved in this incident may have included your

What We Are Doing. As soon as we discovered the incident, we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. In addition, we notified the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators accountable.

In addition, we are offering you complimentary credit monitoring and identity protection services through IDX, a leader in consumer identity protection. These services include <<12/24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary services offered to you through IDX by contacting IDX at 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the enrollment code above. Please note the deadline to enroll is June 12, 2024.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-800-939-4170 Monday through Friday from 9am – 9pm Eastern. We take your trust in us and this matter very seriously. We regret any concern or inconvenience this incident may cause.

Sincerely,

Katrin M. Ratassepp
Vice President, HR, Contracts, and Compliance
ACR Electronics, Inc.

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: 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. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may 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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. 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.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.