

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

May 2, 2024

VIA MAIL

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202



Re: Atronic Alarms – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Atronic Alarms Inc. (“Atronic Alarms”). I am writing to provide notification of an incident at Atronic Alarms that may affect the security of personal information of one (1) Maryland resident. By providing this notice, Atronic Alarms does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Atronic Alarms experienced a network security incident that impacted some operations. Upon learning of this issue, Atronic Alarms immediately commenced a prompt and thorough investigation working very closely with external cybersecurity professionals experienced in handling these types of incidents to determine whether there was any unauthorized access to protected information. After an extensive forensic investigation and document review, we discovered on March 18, 2024, that a limited amount of information stored on our network may have been accessed and/or acquired by an unauthorized individual on July 25, 2023. The information potentially accessed includes full name, address, driver’s license number. The information impacted for the one (1) Maryland resident includes their name, account number, routing number, payment card number, and payment card expiration date.

Atronic Alarms has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, Atronic Alarms is providing notice to the affected resident commencing on May 2, 2024, in substantially the same form as the document attached hereto. Atronic Alarms is also offering complimentary credit monitoring to the impacted individuals who had their Social Security number impacted. Additionally Atronic Alarms will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Atronic Alarms will further advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission and the Maryland Attorney General

At Atronic Alarms, protecting the privacy of personal information is a top priority. Atronic Alarms is committed to maintaining the privacy of personal information in its possession and has

Baltimore | Chicago | Cleveland | Columbus | Detroit | West Palm Beach

mcdonaldhopkins.com

taken many precautions to safeguard it. Atronic Alarms continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Thank you for your cooperation.

Sincerely,

A handwritten signature in blue ink, appearing to read "Dominic A. Paluzzi".

Dominic A. Paluzzi

Encl.



Secure Processing Center
P.O. Box 2623
Duluth, GA 30096-9998

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

[REDACTED]

RE: NOTICE OF DATA SECURITY INCIDENT

Dear [REDACTED],

We are writing with important information regarding a recent cyber security incident at Atronic Alarms, Inc. ("Atronic Alarms") that may involve your personal information. We wanted to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

Atronic Alarms experienced a network security incident that impacted some operations.

What We Are Doing.

Upon learning of this issue, we immediately commenced a prompt and thorough investigation working very closely with external cybersecurity professionals experienced in handling these types of incidents to determine whether there was any unauthorized access to protected information. After an extensive forensic investigation and document review, we discovered on March 18, 2024, that a limited amount of information stored on our network may have been accessed and/or acquired by an unauthorized individual on July 25, 2023.

What Information Was Involved?

The impacted information includes your full name [REDACTED]

What You Can Do

We have no evidence that your information has been misused for identity theft or financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. This letter provides precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and will continue to take many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available for 90 days from the date of this letter, between the hours of 9:00 a.m. to 9:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

Melissa Goodloe
Atronic Alarms
8220 Melrose Drive
Lenexa, Kansas 66214

– OTHER IMPORTANT INFORMATION –

1. Obtain and Monitor Your Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies. You can obtain a free copy of your credit report by calling **1-877-322-8228**, visiting **www.annualcreditreport.com**, 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/index.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. 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. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
e
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Protecting Your Medical Information.

As a general matter, the following practices can help to protect you from medical identity theft.

1. Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
2. Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
3. Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

5. Additional Helpful Resources.

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. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General’s Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.