

## **CONFIDENTIAL**

December 8, 2023

**Via E-Mail: Idtheft@oag.state.md.us**

Attorney General Anthony G. Brown  
Office of the Attorney General  
Identity Theft Unit  
200 St. Paul Place  
Baltimore, MD 21202

Re: Data Security Incident

Dear Attorney General Brown:

FisherBroyles, LLP represents Aiphone Corporation, located at 6670 185th Ave NE, Redmond, WA 98052, with respect to a data security incident described in more detail below. Aiphone Corporation takes the security and privacy of the information in its control seriously and has taken steps to prevent a similar incident from occurring in the future.

### **1. Description of the Incident.**

On or about July 25, 2023, Aiphone Corporation experienced a ransomware incident which may have resulted in the inadvertent exposure of personal information (the “Incident”). Aiphone Corporation has since worked diligently to determine what happened and what information may have been impacted as a result of this Incident.

An investigation conducted by third-party forensic specialists determined the incident occurred between July 22, 2023 and July 25, 2023. A data mining exercise was conducted to identify the potentially impacted individuals and what elements of personally identifiable information may have been affected. The investigation and data mining exercise determined that the following elements of personal information of Maryland residents were potentially accessed and/or acquired by an unauthorized individual: names, Social Security numbers, taxpayer ID numbers, dates of birth, financial account information, medical information, and health insurance information.

As of this writing, Aiphone Corporation has not received any reports of fraud or identity theft related to this matter.

# FisherBroyles

## **2. Number of Maryland residents affected.**

Aiphone Corporation discovered that the Incident may have resulted in the unauthorized exposure of information pertaining to ten (10) Maryland residents. Notification letters to these individuals were mailed on November 14, 2023, via First Class Mail. A sample copy of the notification letter is attached as **Exhibit A**.

## **3. Steps taken.**

Upon discovery of the Incident, Aiphone Corporation reported the Incident to law enforcement and worked with cybersecurity counsel and forensic experts to investigate how the Incident occurred and what information may have been impacted. Aiphone Corporation is committed to ensuring the security of all information in its control and is taking steps to prevent a similar event from occurring in the future, including strengthening its security posture. Additionally, the notified Maryland residents whose Social Security numbers were potentially impacted were offered complimentary identity theft and credit monitoring services for twelve (12) months.

## **4. Contact information.**

Aiphone Corporation remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at [Kelly.Garrison@fisherbroyles.com](mailto:Kelly.Garrison@fisherbroyles.com) or (914) 582-3787.

Very truly yours,

*Kelly Garrison*

Kelly Garrison  
FisherBroyles, LLP

**EXHIBIT A**

<Return Name>  
c/o Cyberscout  
<Return Address>  
<City>, <State> <Zip>



*Via First-Class Mail*

<<FirstName>> <<LastName>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

November xx, 2023

**Notice of Data <<Incident/Breach>>**

Dear <<First name>> <<Middle name>> <<Last name>> <<Sufx>>:

Aiphone Corporation recently experienced a data security incident which may have affected your personal information. Based on our current review, we have no indication that your personal information has been or will be used inappropriately, but we wanted to make you aware of the incident, the measures we have taken in response, and to provide details on the steps you can take to help protect your information. We take the protection and proper use of your information seriously and are working to prevent a similar incident from occurring again in the future.

**What Happened**

On or about July 25, 2023, Aiphone Corporation experienced a ransomware incident. During a typical ransomware incident, cybercriminals try to encrypt or “lock” an organization’s digital files in an attempt to get paid for a digital key to unlock the files. We promptly launched an investigation, engaged a national cybersecurity firm to assist in assessing the scope of the incident and took steps to mitigate the potential impact to our community. Unfortunately, these types of incidents are becoming increasingly common and organizations with some of the most sophisticated IT infrastructure available continue to be affected. We have worked diligently to determine what happened and what information was involved as a result of this incident. A third-party forensic investigation determined the incident occurred between July 22, 2023 and July 25, 2023.

**What Information Was Involved**

The elements of your personal information that may have been impacted may have included, and potentially were not limited to, your: name, address, <<Data Elements>>. Please note that we have no evidence at this time that any of your personal information has been or will be misused as a result of the incident.

**What We Are Doing**

We are taking this incident seriously and are committed to strengthening our systems’ security to prevent a similar event from occurring again in the future. Additionally, out of an abundance of caution, we are providing you with access to Single Bureau Credit Monitoring, Credit Report and

Credit Score services at no charge. These services provide you with alerts for <<service length>> months from the date of enrollment when changes occur to your credit file. With this service, notifications will be sent to you the same day that a change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

### **What You Can Do**

To enroll in the complimentary services we are offering you, please visit **URL** and follow the instructions provided. When prompted please provide the following unique code to receive services: <<**Unique Code**>>. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter.

Please note that to activate monitoring services, you will need an internet connection and e-mail account and may not be available to minors under 18 years old. Additionally, you may be required to provide your name, date of birth, and Social Security number to confirm your identity. Due to privacy laws, we cannot register you directly. Please note that the certain services might not be available for individuals who do not have a credit file with the credit bureaus or an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score.

At this time, we are not aware of anyone experiencing fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following pages, which contain important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

### **For More Information**

Please know that the protection of your personal information is a top priority, and we understand the inconvenience and concern this incident may cause. Representatives can be reached at **1-800-xxx-xxxx** and are available for 90 days from the date of this letter to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

Aiphone Corporation

### **Additional Important Information**

#### **For residents of all states:**

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud\\_Alert\\_Request\\_Form.pdf](https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf)); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

**Monitoring:** You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

**Security Freeze:** You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

#### **Equifax Security Freeze**

P.O. Box 105788  
Atlanta, GA 30348  
[equifax.com/personal/credit-report-services/](https://equifax.com/personal/credit-report-services/)  
1-800-349-9960

#### **Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
[experian.com/freeze/center.html](https://experian.com/freeze/center.html)  
1-888-397-3742

#### **TransUnion Security Freeze**

P.O. Box 160  
Woodlyn, PA 19094  
[transunion.com/credit-freeze](https://transunion.com/credit-freeze)  
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.

#### **Implementing an Identity Protection PIN (IP PIN) with the IRS:**

To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.

- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.

---

**For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming:** It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

---

**For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:**

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

---

**For residents of Vermont:** If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

---

**For residents of New Mexico:** Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting [https://files.consumerfinance.gov/f/documents/bcfrp\\_consumer-rights-summary\\_2018-09.pdf](https://files.consumerfinance.gov/f/documents/bcfrp_consumer-rights-summary_2018-09.pdf), or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

---

**For Residents of Washington, D.C.:** You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; [www.oag.dc.gov](http://www.oag.dc.gov).

---

**For residents of Iowa:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

---

**For residents of Oregon:** State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

---

**For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:** You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

---

**Maryland Office of the Attorney General** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 [www.oag.state.md.us](http://www.oag.state.md.us)

**Rhode Island Office of the Attorney General** Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 [www.riag.ri.gov](http://www.riag.ri.gov)

**North Carolina Office of the Attorney General** Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 [www.ncdoj.com](http://www.ncdoj.com)

**Federal Trade Commission** Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**New York Office of Attorney General** Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

---

**For residents of Massachusetts and Rhode Island:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.