



PIERSON FERDINAND

MARYAM M. MESEHA, ESQ.
FOUNDING PARTNER

Mail

11010 Lake Grove Boulevard, Suite 100-167
Morrisville, NC 27560

Office

525 North Tryon Street, Suite 1600
Charlotte, NC 29202

Direct: 973.419.7819

Email: Maryam.meseha@pierferd.com

March 14, 2024

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: Notice of Data Security Incident

Dear Attorney General Brown:

The undersigned represents Skyview Networks (“Skyview”), a broadcast technology and audio solutions provider, with a principal place of business at 4605 N Airport Dr Ste 370, Scottsdale, Arizona, 85260. We write to inform your office of a recent data security incident, described in more detail below. Skyview 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.

I. Description of the Incident

On September 26, 2023, Skyview learned of a potential unauthorized access into the email account of one of its finance employees, despite its robust security measures and safeguards. Skyview promptly initiated its incident response protocols, launched an investigation, and engaged a national cybersecurity firm to assist in assessing the scope of the incident.

Their investigation determined the potential for acquisition of certain data that was limited to Skyview’s business partners and direct employees. The information involved the following elements of personal information belonging to 1 Maryland resident: name, date of birth, address and/or Social Security Number.

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

II. Number of Maryland Residents Affected.

Skyview discovered that the Incident may have resulted in the unauthorized exposure of information pertaining to one (1) resident of Maryland. A notification letter to this individual was



PIERSON FERDINAND

March 14, 2024

Page 2 of 2

sent via First-Class Mail on or around March 6, 2024. A sample notification letter identical to the notification letters to the affected Maryland resident is attached as **Exhibit A.**

III. Steps Taken.

Skyview takes the security of information that its business partners and employees entrust in it very seriously. Upon detection, Skyview secured the email account in question and took steps to prevent further unauthorized access. Skyview also engaged a third-party digital forensic investigator to conduct an exhaustive investigation of this matter. As of this writing, no additional indicators of suspicious or malicious activity has been identified on Skyview's network. As part of Skyview's ongoing commitment to the security of personal information in its care, Skyview is working to implement additional safeguards and security measures to enhance the privacy and security of information in its email systems.

Skyview is committed to strengthening its systems' security to prevent a similar event from occurring again in the future.

IV. Contact Information.

Skyview 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 maryam.meseha@pierferd.com or (973) 419 – 7819.

Very truly yours,



PIERSON FERDINAND

/s/ Maryam Meseha

Maryam M. Meseha, Esq.
Founding Partner

EXHIBIT A

CyTrex Cyber
1100 13th St. NW, Ste. 925
Washington, DC 20005



March 4, 2024

RE: Notice of Data Breach. Please read this entire letter.

Dear 

This letter is to inform you that Skyview Networks("Skyview") recently experienced a data security incident which may have affected your personal information. **At present, there is no evidence that any of your personal information has been misused**; however, out of an abundance of caution, we are notifying you of this incident and offering you the resources discussed below so that should you wish to, you can take steps to protect yourself. This notification was not delayed as a result of a law enforcement investigation.

We take the protection and proper use of your information seriously and understand the inconvenience and concern this incident may cause. This letter contains additional information about the incident, our response to this incident and steps you can take to protect yourself.

What Happened

On September 26, 2023, Skyview learned of a potential unauthorized access into the email account of one of its finance employees, despite our robust security measures and safeguards. We promptly initiated our incident response protocols, launched an investigation, and engaged a national cybersecurity firm to assist in assessing the scope of the incident. Unfortunately, these types of incidents are becoming increasingly common and even organizations with some of the most sophisticated IT infrastructure available are affected. We have worked diligently to determine what happened and what information was involved as a result of this incident.

What Information Was Involved

The types of information that may have been compromised was different for each individual, but may have included your: name, address, date of birth, and/or financial account information. **Please note that we have no evidence at this time that any of your personal information has been misused as a result of the incident.**

What We Are Doing

We take the security of information that our employees and business partners entrust in us very seriously. Upon detection, we secured the email account in question and took steps to prevent further unauthorized access. We also engaged a third-party digital forensic investigator to conduct an exhaustive investigation of this matter.

As of this writing, no additional indicators of suspicious or malicious activity has been identified on Skyview's network. As part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and security measures to enhance the privacy and security of information in our systems. In addition to providing this notice to you, we are providing notice to privacy regulators and other parties as required.

Out of an abundance of caution, we are offering complimentary access to Identity Protection Service ("IPS") from CyEx for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an identity restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident

(including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that identity restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at: <https://app.identitydefense.com/enrollment/activate/skyv>

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through IPS as a complimentary 12 month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by 06/06/2024** (Your code will not work after this date.)
- **Visit** the IPS website to enroll: <https://app.identitydefense.com/enrollment/activate/skyv>
- Provide your **activation code**: SKYA-2KYZ-MVQJ-29CM

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in IPS online, please contact our customer care team at (800) 297-6391 by 06/06/2024.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH IPS MEMBERSHIP

A credit card is not required for enrollment in IPS. You can contact IPS immediately regarding any fraud issues, and have access to the following features once you enroll in IPS:

- **Credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

At this time, we are not aware of anyone experiencing fraud as a result of this incident. We encourage you to 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 page, which contains 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. If you have further questions or concerns, or would like an alternative to enrolling online, please call (800) 297-6391 toll-free Monday through Friday from 8 am – 11 pm Eastern, or Saturday from 9 am – 6 pm Eastern (excluding major U.S. holidays).

Sincerely,
Steve Jones,
CEO at Skyview Networks

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by insurance company subsidiaries or affiliates of American International Group, Inc. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

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, 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, 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.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 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

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338)
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.

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%20Alert%20Request%20Form.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/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

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