PSAV®

May 14, 2020

VIA FEDEX

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

On behalf of Audio Visual Services Group, LLC d/b/a PSAV ("PSAV"), and pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(b), this letter provides notice of a computer data security incident.

On or about January 15, 2020, PSAV learned that an unauthorized party had gained remote access to certain employees' business email mailboxes. The unauthorized activity was part of an apparent attempt to use email accounts to re-route wire transfer payments from vendors to bank accounts under the control of the bad actors.

After PSAV became aware of the incident, we took steps to terminate the unauthorized access and began a thorough investigation of the incident, including hiring leading outside cybersecurity experts to assist in these efforts. That ongoing investigation has uncovered evidence that suggests the unauthorized access began on or before October 22, 2019 and ended on or about February 5, 2020. As part of the investigation, PSAV conducted a detailed analysis of the affected email accounts and ultimately identified personal information in those accounts. Based on the review performed to date, the incident involved the following personal information categories relating to individuals residing in New Hampshire: names and social security numbers.

Based on the information we have currently, it appears the number of potentially impacted individuals in New Hampshire is three.

To prevent recurrence of this type of incident, we have implemented multi-factor authentication for all employee business email accounts and reset passwords for impacted accounts. PSAV expects to begin the process of notifying impacted individuals via letter on or about May 15, 2020. A sample of the letter is enclosed. As stated in the attached sample notice, PSAV will offer to provide affected individuals with two years of free credit monitoring services and identity theft protection services.

PSAV takes this incident seriously, and is committed to answering any question that your office may have about it. Please do not hesitate to contact me at 562-366-0140.

Sincerely,

Whit Markowitz
Chief Legal Officer
Audio Visual Services Group, LLC d/b/a PSAV

Enclosure

May 15, 2020

[NAME
ADDRESS]

NOTICE OF DATA BREACH

Dear [NAME]:

We are writing to inform you of an incident involving data that Audio Visual Services Group, LLC d/b/a PSAV ("PSAV") holds.

What Happened?

On or about January 15, 2020, PSAV learned that an unauthorized party had gained remote access to certain employees' business email mailboxes. The unauthorized activity was part of an apparent attempt to use email accounts to re-route wire transfer payments from vendors to bank accounts under the control of the unauthorized party.

After PSAV became aware of the incident, we took steps to terminate the unauthorized access and began a thorough investigation of the incident, including hiring leading outside cybersecurity experts to assist in these efforts. That ongoing investigation has uncovered evidence that suggests the unauthorized access began on or before October 22, 2019 and ended on or about February 5, 2020. As part of the investigation, PSAV has conducted a detailed analysis of the affected email accounts and ultimately identified personal information in those accounts. The investigation has identified that your personal information may have been exposed in this incident.

What Information Was Involved?

The incident may have involved your name and social security number.

What We Are Doing.

We have implemented multi-factor authentication for all employee business email accounts and reset passwords for impacted accounts. We have arranged for you to receive a complimentary two-year membership of Experian's® IdentityWorks^{SM}, which helps detect misuse of your personal information and provides you with identity protection focused on identification and resolution of identity theft.

To activate your membership and start monitoring your personal information, please follow these steps:

May 15, 2020

- Ensure that you **enroll by**: August 31, 2020 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- Provide your **activation code**: [code]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 855-252-2731 by August 31, 2020. Be prepared to provide engagement number [engagement #] as proof of eligibility for the identity restoration services by Experian.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 855-252-2731. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (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).

---

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

May 15, 2020

Please note that this Identity Restoration support is available to you for two year 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 www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do.

Please find enclosed additional steps that you can take to protect yourself, including 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.

For More Information

PSAV sincerely regrets any inconvenience this unfortunate incident has caused. If you have any questions, you can contact us at 562-366-0140.

Sincerely,

Whit Markowitz
Chief Legal Officer
Audio Visual Services Group, LLC, d/b/a PSAV

May 15, 2020

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements 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 incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	**Experian**:	**TransUnion**:
equifax.com equifax.com/personal/credit-report-services P.O. Box 740241 Atlanta, GA 30374 866-349-5191	experian.com experian.com/help P.O. Box 2002 Allen, TX 75013 888-397-3742	transunion.com transunion.com/credit-help P.O. Box 1000 Chester, PA 19016 888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. If you have already been a victim of identity theft, you may have an extended alert

placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

May 15, 2020

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

***