



Stuart A. Panensky

Partner

Mail: 420 Main St. #138, Tennent, NJ 07763

Office: 100 Overlook Center, 2nd Fl, Princeton, NJ 08540

Direct: 609.454.6957

Fax: 609.498.6039

Email: stuart.panensky@fisherbroyles.com

www.FisherBroyles.com

August 4, 2020

(Via E-Mail SecurityBreach@atg.wa.gov)

Washington State Office of the Attorney General
Consumer Protection
800 5th Ave., Suite 2000
Seattle, WA 98104-3188

Re: Notice of Data Breach

Dear Madam / Sir:

The undersigned represents Scholarship America, Inc. (“Scholarship America” or “SAI”) in connection with the above-referenced matter. In accordance with RCW § 19.255.010, please accept the following from SAI, as formal notice of a data breach incident. SAI is a Massachusetts company with a principal place of business located at One Scholarship Way, Saint Peter, MN 56082. SAI is a nonprofit organization that manages scholarship and tuition assistance programs for many types of organizations and works with students, colleges, businesses and communities to administer these programs. As part of these services, Scholarship America receives certain personal information. This matter concerns the security of personal information relating to certain affected individuals, of which 2,620 are Washington residents. Of the 2,620 affected individuals, the information at issue for 2,579 was the individual’s name in conjunction with date of birth; for 29, it was the individual’s name in conjunction with a student identification number; and for the remaining 12, the information was some other form of personal information.

Nature of the Data Event

On or about April 28, 2020, SAI internal IT security processes detected suspicious activity within SAI’s email system triggering certain security protocols designed to protect SAI data. Upon discovery, SAI took immediate action to stop the suspicious activity and remediate the problem, including resetting passwords on all impacted email accounts and assuring that used protocols were disabled. SAI also very quickly forced a systemwide email password reset for all users. In addition, SAI activated enhanced monitoring of SAI IT systems by SAI’s managed detection and response service provider.

After being retained, the undersigned retained independent IT security and forensics experts, electronic and digital data discovery consultants, and engaged with the FBI to assist in a federal law enforcement investigation. Working with these providers and experts, SAI conducted a detailed systemwide investigation as well as conducted a detailed review of the contents of any potentially affected email accounts to determine if they contained any personally identifiable information (PII) or other sensitive data. Further, we retained NortonLifeLock on SAI's behalf to provide notifications to affected individuals and to provide two (2) years of complimentary LifeLock Defender Preferred identity theft protection and credit monitoring services. SAI email service is provided by Microsoft Office 365 and not directly attached to the Scholarship America IT network, where student applications and program information are stored. However, in an abundance of caution, SAI conducted a thorough review of SAI's *entire* IT system to confirm the integrity of its security.

SAI's investigation confirmed that there was unauthorized access to nine (9) program sponsor email inboxes and three (3) internal SAI email inboxes and that data containing PII was likely exfiltrated from the SAI network. To date, SAI has seen no evidence that any individual's PII has been misused in any way because of this incident. Based on the steps taken by SAI and its team of experts, SAI's email inboxes are now secured, and no servers or systems were impacted beyond the aforementioned affected inboxes.

Notice to Washington Residents

SAI will begin providing written notice to potentially affected individuals, including the 2,680 Washington residents, by mail on or about August 5, 2020. Written notice is being provided in substantially the same form as the letter attached hereto as Exhibit "A".

Remedial Actions

Scholarship America takes the privacy and security of all sensitive data very seriously and has used/is using the incident as an opportunity to continue to improve the security of all SAI systems. SAI has not seen any further unauthorized or malicious activity since the time of the incident, and has put additional safety measures into place to help better protect SAI data moving forward, including, but not limited to the following list of IT action items:

- Changed and strengthened all passwords
- Disabled unused protocols
- Enhanced monitoring through Managed Detection and Response vendor
- Implemented Multi Factor Authentication on privileged accounts and began working on MFA for all other users
- Removed access to email web portal

- Reviewed Microsoft Office 365 security settings to assure settings meet best practices
- Reviewed security settings with email security vendor
- Reviewed security settings with end point detection and response vendor
- Reviewed reports and alerts with MDR
- Threat Management – changed anti-phishing default policy
- SharePoint sharing policies restricted
- Updated Microsoft Teams settings
- Restricted Microsoft Forms external use

Thank you for your kind and early attention to this matter. Please feel free to contact the undersigned should there be any questions about this notification or any other aspect of this data security event.

Yours very truly,

FISHERBROYLES, LLP

A handwritten signature in black ink, appearing to read 'Stuart A. Panensky', with a large, sweeping flourish extending to the right.

Stuart A. Panensky, Esq.

Cc: Robert C. Ballard
President & CEO
Scholarship America, Inc.

EXHIBIT A [Notification Letter]



1 1 150 *****AUTO**MIXED AADC 300

John Doe
123 Anystreet Dr
Anytown, NY 12345



Re: Important Notice Regarding Possible Disclosure of Private Information

Dear John Doe:

I am writing to inform you about a recent IT incident at Scholarship America that may affect the security of your personal information. We take this incident seriously and as such, are providing you with information and access to resources so that should you feel it is appropriate to do so, you can protect your personal information. Scholarship America is a nonprofit organization that manages scholarship and tuition assistance programs for many types of organizations and works directly with students, colleges, businesses and communities to administer these programs. As part of these services, Scholarship America receives certain personal information. You are receiving this notice because some of your personal information was exposed as a result of unauthorized access to an email account.

What Happened? On or about April 28, 2020, our internal IT security processes detected suspicious activity within our email system which triggered security protocols to protect our data. Upon discovery, we took immediate action to shut down unauthorized access and remediate the problem. We then brought in independent IT security and forensics experts to conduct a detailed systemwide review, which included an extensive inspection of information stored in the email accounts that were accessed. In addition, we are working with law enforcement and sharing information for their investigation.

What Information Was Involved? The data that was subject to unauthorized access was different in individual cases, however, in your case it contained Financial or bank account number, Information regarding medical history, condition, treatment or diagnosis, Username or email address and password for a non-financial electronic account. We have received no indication to-date that anyone's sensitive information has been misused as a result of this incident.

What Are We Doing? We take the security of sensitive information that people entrust to us very seriously. Immediate actions were taken to secure our email system and ensure that any further suspicious activity was prevented. This included resetting passwords on all impacted accounts. We followed that with a systemwide email password resets by all users. In addition, we activated enhanced monitoring of our IT systems. We hired a qualified third-party IT forensic expert to conduct an exhaustive investigation of this matter. The problem has been remediated and our email and IT systems are operating securely. As part of our ongoing commitment to the security of sensitive 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 notice to you, Scholarship America is also providing notice to state regulators as required.

We also want to make sure you have the information you need so that you can take steps to help protect yourself from the potential of identity theft. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps in this letter.

Complimentary Identity Protection and Credit Monitoring Services

Scholarship America has retained **NortonLifeLock, Inc.** to provide two (2) years of complimentary **LifeLock Defender™ Preferred** identity theft protection.

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to **www.LifeLock.com**. Click on the yellow "**START MEMBERSHIP**" button (*do not attempt registration from a link presented by a search engine*).
2. You will be taken to another page where, below the FOUR protection plan boxes, you may enter the **Promo Code: MKFBSCHL2006** and click the "**APPLY**" button.
3. On the next screen, enter your **Member ID: 12345678** and click the "**APPLY**" button.
4. Your complimentary offer is presented. Click the red "**START YOUR MEMBERSHIP**" button.
5. Once enrollment is completed, you will receive a confirmation email (*be sure to follow ALL directions in this email*).

Alternatively, to activate your membership over the phone, please call: (866) 811-6515.

You will have until October 31st, 2020 to enroll in this service.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your LifeLock Defender™ Preferred membership includes:

- ✓ Primary Identity Alert System[†]
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring^{**}
- ✓ Norton™ Security Deluxe² (90 Day Free Subscription)
- ✓ Stolen Funds Reimbursement up to \$25,000^{†††}
- ✓ Personal Expense Compensation up to \$25,000^{†††}
- ✓ Coverage for Lawyers and Experts up to \$1 million^{†††}
- ✓ U.S.-based Identity Restoration Team
- ✓ Annual Three-Bureau Credit Reports & Credit Scores^{1**}

The credit scores provided are VantageScore 3.0 credit scores based on Equifax, Experian and TransUnion respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

- ✓ Three-Bureau Credit Monitoring^{1**}
- ✓ USPS Address Change Verification Notifications
- ✓ Fictitious Identity Monitoring
- ✓ Credit, Checking and Savings Account Activity Alerts^{†**}

¹If your plan includes credit reports, scores, and/or credit monitoring features (“Credit Features”), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. **IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU.** If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.

No one can prevent all identity theft or cybercrime. [†]LifeLock does not monitor all transactions at all businesses.

² Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.

**These features are not enabled upon enrollment. Member must take action to get their protection.

^{†††} Reimbursement and Expense Compensation, each with limits of up to \$25,000 for Defender Preferred. And up to \$1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

What Else Can You Do? In addition to enrolling in the complimentary credit monitoring services being offered (see below), you can review the enclosed *Steps You Can Take to Protect Your Information* for additional information on how to protect against identify theft and fraud.

On behalf of Scholarship America, we are genuinely sorry this incident occurred and apologize for the inconvenience this matter may cause you. We can assure you that we are doing everything we can to protect you and your information, now and in the future. If you have questions about this notice or this incident, or require further assistance, you can reach us at (866) 811-6515, twenty-four hours, seven days a week.

Sincerely,



Robert Ballard, Chief Executive Officer

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Fraud Alert Information

Whether or not you enroll in credit monitoring, we recommend that you place a “Fraud Alert” on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax
PO Box 740256
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

TransUnion
PO Box 2000
Chester, PA 19016
www.transunion.com/fraud
1-800-680-7289

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

Free Credit Report Information

Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

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. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports 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. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or at 1-877-ID-THEFT (1-877- 438-4338). Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC’s website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide “*Identity Theft - A Recovery Plan*”.

Security Freeze Information

You can request a “Security Freeze” on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or

application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
<http://www.freeze.equifax.com>
1-800-685-1111

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
<http://transunion.com/freeze>
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

- Your full name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.)
- Your Social Security Number
- Your date of birth (month, day and year)
- Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
- If you have moved in the past 2 years, give your previous addresses where you have lived for the past 2 years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- Include applicable fee. Call or visit each of the credit reporting company websites listed above for information on fees for Security Freeze services. Forms of payment are check, money order, or credit card (American Express, Discover, MasterCard and Visa), or a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

Within 5 business days of receiving your request for a security freeze, the consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if you choose to remove the freeze on your consumer credit report or to authorize the release of your consumer credit report to a specific party or for a specified period of time after the freeze is in place.