From: [redacted]
To:
Subject: FW: Notice of Data Security Incident
Date: Thursday, September 3, 2020 4:17:00 PM
Attachments: AFP Notification Letter.pdf

Security Breach for 9/3

From: [redacted]
Sent: Thursday, September 3, 2020 4:04 PM
To: [redacted]
Subject: FW: Notice of Data Security Incident

From: Alex Varban <avarban@standtogether.org>
Sent: Thursday, September 3, 2020 2:13 PM
To: DOJ: Attorney General <attorneygeneral@doj.nh.gov>
Subject: Notice of Data Security Incident

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

September 3, 2020

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

Dear Attorney General MacDonald:

Pursuant to New Hampshire Section 359-C:20 – Notification of Security Breach, we are writing to notify you of a breach of security/an unauthorized access or use of personal information involving 1 New Hampshire resident.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS
Americans for Prosperity (AFP) is a non-profit education and advocacy organization. Blackbaud, located at 65 Fairchild Street in Charleston, SC 29492, is a third-party service provider of a software management system that supports the financial systems, fundraising and donor relations efforts for many nonprofit organizations. AFP leverages Blackbaud for several of these services. Blackbaud notified us on July 16, 2020 that they had been a target of a ransomware attack that resulted in the compromise of certain clients' data, including Americans for Prosperity. Blackbaud

has told us that they discovered the attack on May 14, 2020, and its Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files, and ultimately expelled the cybercriminal from their system.

However, prior to locking the cybercriminal out, a copy of certain AFP backup files was removed, including a file that contained individual's personal information. We have been told that this theft occurred at some point between February 7, 2020 and May 20, 2020. The personal information involved included name, postal address and tax ID number (which in some cases was a Social Security number) that were used by AFP for payment and tax purposes. Blackbaud indicated that it believed, based on the nature of the incident, their research and their third party (including law enforcement) investigation, that the cybercriminal deleted all data copied during the ransomware attack and has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made publicly available.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

The breach involved 1 New Hampshire resident who will be notified by Americans for Prosperity via U.S. Mail on September 4, 2020. A copy of the notice is attached.

STEPS TAKEN RELATING TO THE INCIDENT

Americans for Prosperity has arranged for identity protection and credit monitoring services to our impacted clients for two years at no cost through Experian's® IdentityWorksSM. This product provides identity detection and resolution of identity theft.

Blackbaud has indicated the following related to their Cybersecurity Practices and Next Steps Following this Incident:

> *Over the last five years, we have built a substantial cybersecurity practice with a dedicated team of professionals. Independent reviewers have evaluated our program and determined that it exceeds benchmarks for both the financial and technology sectors. We follow industry-standard best practices, conduct ongoing risk assessments, aggressively test the security of our solutions, and continually assess our infrastructure. We are also a member of various Cyber Security thought leadership organizations, including: The Cloud Security Alliance and Financial Services Information Sharing and Analysis Center (FS-ISAC), where we team up with other experts to share best practices and tactical threat information for the Cyber Security community. We believe the strength of our cybersecurity practice and advance planning is the reason we were able to shut down this sophisticated ransomware attack. We have already implemented changes to prevent this specific issue from happening again. You can review more details on our security, risk, compliance and privacy programs at https://www.blackbaud.com/security.*

CONTACT INFORMATION

Should you have any further questions or concerns regarding this matter, please contact Should you have any further questions or concerns regarding this matter, please contact Americans For Prosperity at (703)224-3200 or info@afphq.org.

Sincerely,

Alex Varban
Treasurer
Americans For Prosperity
1310 N. Courthouse Rd., Suite 700
Arlington, VA 22201

1310 N. Courthouse Rd. | Ste. 700 | Arlington,VA 22201 | p: (703) 224-3200
AmericansforProsperity.org

<Mailing Date>
<Street Address>
<City>, <State> <Zip>

RE: Notice of Blackbaud Data Security Incident

Dear <Full Name (First & Last)>,

We are writing to let you know about a data security incident that affected one of our third-party service providers, Blackbaud. Americans for Prosperity (AFP) takes the protection and proper use of your information very seriously. We are therefore contacting you to explain the incident and provide you with steps you can take to protect yourself.

What Happened

We recently became aware that Blackbaud, a software management system that supports financial and accounting activities for many nonprofit organizations, was the target of a ransomware attack that resulted in the compromise of certain data associated with Blackbaud's clients, including AFP. Blackbaud has confirmed that, after discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files, and ultimately expelled the cybercriminal from their system. However, prior to locking the cybercriminal out, the cybercriminal removed a copy of certain backup files, including a file that contained your personal information. This occurred at some point beginning on February 7, 2020 and could have occurred intermittently until May 20, 2020. Blackbaud has indicated that it believes that all data copied during the ransomware attack was deleted by the cybercriminal and has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made publicly available.

What Information Was Involved

Among the backup files that were removed by the cybercriminal, we understand that one of the files contained your name, postal address and tax ID number (which may be a Social Security number) that were used by us for payment and tax purposes.

What We Are Doing

We are notifying you so that you can take action to protect yourself. Ensuring the safety of our partners' data is of the utmost importance to us. As part of Blackbaud's ongoing efforts to help prevent something like this from happening in the future, Blackbaud confirmed that they have implemented several changes designed to help protect client data from similar incidents. Additional details from Blackbaud are available here: https://www.blackbaud.com/securityincident.

What You Can Do

We take our obligation to safeguard personal information very seriously and are alerting you about this issue so you can take steps to help protect yourself. Steps you can take include the following:

- Order a Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.
- Register for Credit Monitoring Services. We have arranged to offer identity protection and credit monitoring services to you for **two years** at no cost to you. The attached Reference Guide provides additional information about enrollment.
- Review the Attached Reference Guide. The attached Reference Guide provides information on registration for identity protection services and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

For More Information

We sincerely apologize for this incident at Blackbaud, and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact AFP directly at: (703) 224-3200 or info@afphq.org.

Sincerely,

Alex Varban

Treasurer
Americans for Prosperity
1310 N. Courthouse Rd., Suite 700
Arlington, Virginia 22201

Reference Guide

We encourage affected individuals to take the following steps:

Register for Identity Protection and Credit Monitoring Services. To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **December 31, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- 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 toll-free at **877-890-9332** by **December 31, 2020.** Be prepared to provide engagement number **DB22351** 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.*
- **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**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the

information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

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

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov/

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/internet/resource-center

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov