



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you that we recently became aware of a security incident involving Blue Bear Software, a software platform that facilitates administration and management of school accounting, student fees, and online stores on behalf of educational institutions. You may have conducted business on the Blue Bear platform when you purchased items from the webstore of an educational institution. The Blue Bear platform is operated by ACTIVE Network, LLC, however, this incident did not impact other systems of ACTIVE or its affiliates.

What Happened?

We recently identified suspicious activity on the Blue Bear platform. Our investigation determined the activity related to Blue Bear webstore users between October 1, 2019 and November 13, 2019. During this time, some personal information that you provided may have been accessed or acquired by unauthorized third parties.

What Information Was involved?

While we are unable to determine with certainty whether your personal information was affected, the personal information involved may have included: name, credit card or debit card number ending in <<b2b_text_1(Impacted Data)>>, expiration date and security code (the three or four-digit value included on the front or back of payment cards and used for verification of certain transactions), and Blue Bear account usernames and passwords. This incident did not involve unauthorized access to Social Security numbers, driver license numbers, or similar government ID card numbers.

What We Are Doing?

We take this matter very seriously. As soon as we identified the suspicious activity, our counsel engaged a leading cybersecurity firm to investigate the incident and took steps to enhance its monitoring tools and security controls. We are also offering you free identity monitoring services. More information on how to access these services can be found below and in the enclosed reference guide.

What You Can Do

We encourage you to be diligent in watching for unauthorized activity associated with your payment card accounts and to quickly report suspicious activity to your bank or credit card company. The phone number to call is usually on the back of the credit or debit card. The Reference Guide contains additional information on steps you can take to monitor and protect your personal information. We have also arranged for Kroll to provide you one year of identity monitoring services at no cost to you. For instructions on how to access these complimentary services, please call the toll-free number, 1-844-967-1237. The Reference Guide contains additional information about these services.

Your Kroll Membership Number is: <<Member ID>>

Other Important Information

The enclosed Reference Guide also includes additional information on general steps you can take to monitor and protect your personal information.

For more information

We apologize for any inconvenience this incident may cause. You may contact us at 1-844-967-1237, Monday through Friday between 8:00 a.m. and 5:30 p.m. Central Time if you have questions or would like additional information about this incident.

Sincerely,

Philip Petescia, Vice President of Global Support and Customer Advocacy
ACTIVE Network, LLC

REFERENCE GUIDE

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Order Your Free Credit Report

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

Upon receiving 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 have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus 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 credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Activate Your Identity Monitoring Services To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration.

Visit enroll.idheadquarters.com to activate and take advantage of your identity monitoring services.

*You have until **March 29, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, you have the right to place a fraud alert on your credit file for one year at no cost. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the applicant's identity. You can place a fraud alert on your credit report by calling any of the toll-free fraud numbers provided below. You

will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax

P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian

P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

Security Freezes

As of September 21, 2018, you have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
800-685-1111
www.equifax.com

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
888-909-8872
www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.