20658

wellspring EAP

<<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>>:

Wellspring Family Services ("Wellspring") previously provided an Employee Assistance Program for Avanade Inc. employees and dependents. Wellspring is writing to inform you of an incident that involved information about you that was processed by Wellspring as part of its delivery of these services. Wellspring takes the privacy of information in our care seriously, and although we have no indication of misuse of information, this letter provides details of the incident, our response, and steps you may take to protect your information from possible misuse, should you feel it necessary to do so.

What Happened: On October 23, 2020, Wellspring became aware of unusual activity related to an employee's email account. We took steps to investigate this activity and change employee email account passwords. We also began working with computer specialists to investigate the nature and scope of the incident. From this investigation, we determined that an unauthorized person(s) gained access to certain employee email accounts between September 25, 2020 and October 23, 2020. Our investigation could not conclusively determine whether or what information within the accounts may have been accessed. Therefore, in an abundance of caution, we undertook a detailed and diligent review of all potentially accessible data in the accounts to determine what records were present at the time of the incident, to whom those records related, and the contact information for those individuals. On March 26, 2021, we completed our review and confirmed the impacted accounts contained certain personal information. While to date, the investigation has found no evidence of actual or attempted misuse of this information, we are notifying individuals whose information was present in the accounts.

What Information Was Involved: Our investigation determined that the following information related to you was present in the impacted email accounts at the time of the incident: <<b2b_text_1(DataElements)>>. This information is related to your eligibility to use Wellspring services and did not, in any way, indicate any other information about you, such as whether you used Wellspring's services.

What We Are Doing: Information privacy and security are among our highest priorities, and we have strict security measures in place to protect information in our care. Upon discovering this incident, we immediately took steps to confirm the security of our systems, and we are reviewing our policies and procedures related to data security to protect against future incidents. In an abundance of caution, we are also notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. Although we are unaware of any actual or attempted misuse of information as a result of this incident, we have engaged Kroll, a global leader in risk mitigation and response, to provide you with its identity monitoring services for **twenty-four (24) months** at no cost to you.

What You Can Do: We encourage you to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious activity. You may also review the information contained in the attached "Steps You Can Take to Help Protect Your Information," and activate the identity monitoring services we are making available to you. There is no charge to you for this service; however, you will need to activate yourself in this service.

For More Information: If you have additional questions, please call Wellspring's dedicated incident assistance line at 1-855-930-6237 (toll free), Monday through Friday, 8:00 a.m. to 5:30 p.m., Central Time, excluding major U.S. national holidays.

We sincerely regret any concern this incident may cause you. Protecting your information is important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Kevin Host

Kevin Host
Senior Director – Enterprise Services
Wellspring Family Services

Steps You Can Take to Help Protect Your Information

Activate Identity Monitoring Services

We have engaged Kroll to provide identity monitoring services to you, at no cost, for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have experienced unauthorized access of their personal information. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **July 19, 2021** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your services is included below.

Monitor Your Accounts

We are providing you with the following information about steps that you can take to protect against potential misuse of your personal information.

You should always remain vigilant against incidents of identity theft and fraud, including by regularly reviewing your account statements and monitoring your free credit reports for suspicious charges. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit bureaus listed below to request a free copy of your credit report.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the past five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Should you wish to obtain a credit report, or place a fraud alert or credit freeze, please contact any one of the three major credit bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 2000, Chester, PA 19016

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages individuals who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint using the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents: You can obtain information about preventing identity theft from the North Carolina Attorney General, who may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. You can also obtain information about preventing identity theft from the Federal Trade Commission, using the contact information above.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will be able to help you determine if it is an indicator of identity theft.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.