



Robyn Anderson
Chief Privacy Officer
Corteva Agriscience
974 Centre Road
CRP 735
Wilmington, DE 19805

March 31, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Pl.
Baltimore, MD 21202

To Whom It May Concern:

On behalf of Corteva Agriscience ("Corteva"), I am writing to inform you about a recent incident at ADP, our payroll vendor, in which personal information relating to one (1) Maryland resident was accessed by an unauthorized third party.

In connection with providing payroll services to Corteva, ADP maintains the ADP Global myView and/or iPay portal ("Portal") that Corteva employees can use for certain payroll purposes. The Portal contains various features, such as hosting Corteva employee pay statements and year-end tax documents and allowing Corteva employees to manage their direct deposits.

On March 13, 2023, ADP alerted Corteva to a security incident involving the Portal. Corteva immediately commenced an investigation, including requesting that ADP investigate and provide Corteva with information about the nature and details of the incident. On March 30, ADP confirmed to Corteva that the specific information detailed below may have been accessed by a third-party.

Based on ADP's investigation, a third party called an ADP call center on March 1, 2023 and impersonated a Maryland resident who is a Corteva employee. The ADP call center representative provided the third party with a link that allowed the third party to access the relevant Portal pages for this employee. Based on ADP's investigation, the third party may have been able to view the following information relating to the employee through the Portal: name, home address, Social Security number, bank account information used for direct deposit, e-mail address, and W-2 information. Ultimately, the third party changed the password credentials and direct deposit instructions for the employee. These changes initiated an e-mail to the employee who then contacted ADP on the same day, which lead ADP to suspend Portal access for this individual until ADP was able to issue a new user ID and password.

We have requested that ADP put in place additional authentication for Portal access through the call center. In addition, ADP has agreed to provide the Maryland resident with a free offer for a two-year membership to the Experian IdentityWorks™ identity theft protection service.

We will notify the one (1) Maryland resident of this incident April 1, 2023. Attached is a sample of the letter that we are providing to the Maryland resident.

Please do not hesitate to contact me at (515)218-0261 or robyn.anderson@corteva.com if you have any questions.

Sincerely,

Robyn E. Anderson

Robyn Anderson
Chief Privacy Officer
Corteva Agriscience

Attachment



Robyn Anderson
Chief Privacy Officer
Corteva Agriscience
974 Centre Road
CRP 735
Wilmington, DE 19805

March 31, 2023

Notice of a security incident

Dear _____,

We are writing to inform you about a recent incident involving unauthorized access to certain personal information about you through the ADP Global myView and/or iPay portal ("Portal"). ADP is the payroll vendor for Corteva. The Portal contains various features, such as hosting Corteva employee pay statements and year-end tax documents and allowing Corteva employees to manage their direct deposits.

What happened?

As you know, on March 1, 2023, you called ADP's call center to report a notification of a change to your direct deposit instructions you received that day. ADP has since investigated and reports that a third-party called into ADP's service center that day and impersonated you using your name and date of birth. The ADP call center representative provided the third-party with a link which allowed the third-party to access your Portal pages. The third-party then changed your access credentials and direct deposit instructions. Due to your quick action in calling ADP, however, ADP has indicated that they were able to secure your account the same day.

ADP alerted Corteva to a security incident involving the Portal on March 13. Corteva immediately commenced an investigation, including requesting that ADP investigate and provide Corteva with more information about the nature and details of the incident. On March 30, ADP confirmed to Corteva that the specific information detailed below may have been accessed by the third-party.

What information was involved?

Based on ADP's investigation, the third party may have been able to view the following information relating to you through the Portal: Your name, home address, Social Security number, bank account information used for direct deposit, e-mail address, and W-2 information.

What have we done in response to this incident?

Upon being alerted to the incident, Corteva immediately began working with ADP to investigate the incident. We have requested that ADP put in place additional authentication for Portal access via the call center. In addition, ADP has informed us that ADP initially suspended online access to your account until they were able to issue you a new user ID and password to access the Portal.

Please be aware that ADP's systems will continue to send auto-generated emails if a password change is attempted on your account. Please pay special attention to this email if you receive it. In addition to contacting ADP, you can also call Corteva's HR department at 1-888-244-7570 if you receive an email from ADP and have any questions as to its legitimacy.

Steps you can take

It is important that you always remain diligent for incidents of fraud and identity theft. As a precaution, ADP is offering you a two-year membership to Experian IdentityWorks™ identity theft protection (product letter is included) at no cost to you. This product helps detect possible misuse of personal information about you and provides you with identity protection services focused on immediate identification and resolution of identity theft. If you wish to use this free service, please follow the directions in the letter, using the code provided to sign up for the service by the date provided.

In addition, we recommend that you review your account statements and credit reports 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. In addition, you may report incidents of identity theft or learn more about steps you can take to protect yourself from identity theft by contacting the Federal Trade Commission or the Maryland Attorney General's Office, at:

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

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

You may also periodically obtain credit reports from the three nationwide credit reporting agencies. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.Equifax.com/personal/credit-report-services

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.Experian.com/help

TransUnion
(888) 909-8872
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19022
www.TransUnion.com/credit-help

You also can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. You may place a fraud alert in your file by calling any of the nationwide credit reporting agencies listed above. As soon as that agency

processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place. You must separately place a freeze on your credit file with each credit reporting agency.

We apologize for any inconvenience or concern this matter may cause you. Please do not hesitate to contact the Corteva HR department at 1-888-244-7570 if you have any questions or concerns.

Sincerely,

Robyn E. Anderson

Robyn Anderson
Chief Privacy Officer
Corteva Agriscience