Notice of Data Breach

August 3, 2022

A. Duda & Sons, Inc. and its affiliates and subsidiaries, including but not limited to Duda Farm Fresh Foods, Duda Ranches, DUDA Commercial Properties, The Viera Company, Viera Builders, and Duran Golf Club (collectively, "DUDA"), recently experienced a data security incident, and we are providing this notice to potentially affected individuals in compliance with applicable law. DUDA has always taken measures to protect the personal information it maintains and remains committed to helping affected individuals protect themselves to the best of the company's ability. Please read the below notice for more details and to see what steps you can take to help protect yourself.

What happened?
In June and July of 2022, an unauthorized third party used sophisticated security exploits to gain access to DUDA's information technology systems. On July 9, 2022, these cybercriminals deployed ransomware on DUDA's systems, encrypting most of DUDA's computer network. DUDA has since learned that, during this attack, the attackers also downloaded files from our systems that included personally identifiable information. DUDA reported the incident to law enforcement and has worked diligently to restore operations and security since the attack.

What information was involved?
The data accessed by the attackers was varied and substantial. In some cases, the information included full names, social security numbers, payroll data, financial information, dates of birth, email addresses, telephone numbers, addresses, employee identification numbers, employee dependent information, a combination of these data, or other data an individual may have provided to DUDA in the past. However, due to the volume of files taken and the nature of logging information, DUDA cannot determine with certainty the exact scope of personal information the attackers may have extracted.

To be safe, if you have provided personal information or data to DUDA or its affiliates in the past, you should assume that your personally identifiable information or data may have been compromised in this incident and take appropriate precautions.

What we are doing
DUDA has taken swift action to restore the functionality and security of its data systems following the attack. We are cooperating with law enforcement investigating the attack. DUDA is also working with outside consultants to strengthen our information security systems to reduce the risk of a similar attack in the future. We are offering certain credit monitoring services at no cost to individuals who are or who have a good faith belief that they have been affected by this incident. Further information on this offering is below.

What you can do
The most important thing you can do in response to this incident is to remain vigilant and

secure your financial and other accounts. Whether you have been affected by this specific breach or not, it is important to regularly review personal account statements and credit reports to ensure no unauthorized activity has occurred. Here are a few warning signs to help you determine whether your personal information may have been used by someone else:

- Receiving a bill for services or items you did not purchase
- Being contacted by a debt collector about debt you do not owe
- Seeing collection notices on your credit report that you do not recognize

Malicious actors may try to trick you into giving them more information using the compromised data. If you receive any suspicious communications, particularly regarding financial matters, you should verify the source of these communications before revealing any personal information. If you are threatened by anyone, you should contact law enforcement. If you believe you have been the victim of identity theft, you should also contact law enforcement, your state attorney general, or the Federal Trade Commission ("FTC").

You may want to change your passwords to various online accounts. If you do change your passwords, your new password should be substantially different from your old password to best ensure security. Remember, it is never a good idea to use the same password from work for your personal or household applications.

Additionally, you may also consider placing a security freeze on your credit report, as allowed by state law. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please note that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any request you make for new loans, credit, credit or debit cards, mortgages, employment, housing, or other services.

How to freeze your credit report
To place a security freeze on your credit report, you must contact each of the three major consumer reporting agencies individually: Equifax, Experian, and TransUnion. You can do this online, or in writing.

To do this online, you can go to each of these websites and create an account. You will need to set up a user ID and password with each agency.

If you prefer to contact the agencies in writing, you can send a security freeze request by regular, certified, or overnight mail to the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion Security Freeze
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
1-800-909-8872

In order to request a security freeze in writing, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. The addresses where you have lived over 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.)
7. If you are victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you elect to set up a security freeze online, the agencies may instead request an email address and telephone number for identity verification.

Identity theft resources
The Federal Trade Commission (FTC) is located at 600 Pennsylvania Avenue, NW Washington, DC 20580. If you believe you may have been a victim of identity theft, you may file a complaint with the FTC at www.ftc.gov/idtheft or by calling 1-877-ID-THEFT (877-438-4338).

You may also consider taking additional steps, which are outlined on the FTC's website: https://www.identitytheft.gov/. Here, you will find resources and a checklist of steps you can take to protect yourself.

State governments also provide resources on protecting yourself against identity theft. Some examples of these resources are listed below.

Florida Attorney General
Office of the Attorney General
PL-01 The Capitol
Tallahassee, FL 32399
1-866-966-7226

California Attorney General
P.O. Box 944255
Sacramento, CA 94244-2550
(800) 952-5225

North Carolina Attorney General
114 West Edenton Street
Raleigh, NC 27603
(919) 716-6400

Texas Attorney General
PO Box 12548
Austin, TX 78711-2548
(800) 621-0508

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
410-576-6300

Oregon Attorney General
1162 Court St. NE
Salem, OR 97301-4096
1-877-877-9392

How to sign up for credit monitoring services
In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score* services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll on or before November 1, 2022.

As information relating to employees' dependents may have been included in the compromised data, we are also providing the parents of impacted minor dependents with access to Cyber Monitoring* services for you and your minor child for twenty-four (24) months at no charge. Cyber monitoring will look out for yours and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Cyber Monitoring* services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. Once you have enrolled yourself, click on your name in the top right corner and select Manage Family Protection. In the Family Protection area, click on "Add Child Monitoring", to add the information for the child that you are wanting to be included in the monitoring services. In order for you to receive the monitoring services described above, you must enroll by November 1, 2022.

For questions related to these offerings, please call Cyberscout's customer service line at 1-800-405-6108. Representatives are available until November 1, 2022, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

If you would like more information from DUDA, or have any questions, please email datasecurity@duda.com or call (407) 365-2035.

Services marked with an "" require an internet connection and email account and may not be available to minors under the age of 18 years of age; different services outlined in this correspondence are available for minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.