

# WINDES

AUDIT | TAX | ADVISORY

Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

***RE: Important Security Notification. Please read this entire letter.***

Dear Sir or Madam:

I am writing to inform you of a data security incident experienced by Windes, Inc. (“Windes”) that may have involved your personal information described below.

Windes is a recognized leader in the field of accounting, assurance, tax, and business consulting services. You may be receiving this letter because of a relationship you have with Windes or one of Windes’ partner organizations.

Windes takes the privacy and security of all information very seriously. While we have no evidence to suggest that any of the impacted information was viewed or misused during this compromise, it is crucial that we be as supportive and transparent as possible. That is why I am writing to inform you of this incident, to offer information about steps that can be taken to help protect your information, and to let you know about complimentary credit monitoring services that we are offering you through TransUnion, one of the three nationwide credit reporting companies.

I sincerely apologize for any concern that this incident may cause you. Let me reassure you that Windes is fully committed to providing the best services possible to you.

**What Happened:**

On or around March 19, 2020, Windes learned of a potential compromise to one (1) of its employee email accounts. Windes swiftly secured the suspected account and engaged a third-party forensics company to investigate. Following progress by experts in their thorough investigation, it was ultimately determined on May 4, 2020 that two (2) employee email accounts experienced unauthorized access between March 16-19, 2020 and on March 25, 2020. Upon confirmation of the unauthorized access to the Windes employee email accounts, Windes’ third-party forensic experts immediately investigated whether the affected email accounts contained individuals’ sensitive information. On June 15, 2020, Windes learned that the unauthorized access may have enabled access to your personal information.

While we have no reason to believe that any information within the affected email accounts was actually viewed, collected or misused during this compromise, we are providing this notification to you out of an abundance of caution and so that you may diligently monitor your personal information and resources. We take great care in the security of our technology systems, and regret that this incident has occurred.

**What Information Was Involved:**

It is important to note, as mentioned above, that there is no evidence to suggest that any personally identifiable information has been viewed or misused. The personal information that could have been viewed by the unauthorized individual(s) may have included your first and last name, in combination with one or more of the following data elements: date of birth, social security number, driver’s license number, financial account number, credit card information, tax identification number, passport number, digital signature, username and password combination, diagnosis information, medical treatment information, prescription information, medical record number, medical history and/or health insurance member/group number. Importantly, the information potentially impacted as it relates to you may be limited to only one of the above-listed types of information.

**What We Are Doing:**

Windes has taken every step necessary to address the incident and is committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately secured the affected accounts and took steps to enhance the security of all information to help prevent similar incidents from occurring in the future. We retained a third-party forensic firm to conduct a thorough investigation and are offering you complimentary credit monitoring and identity protection services.

**Credit Monitoring:**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. Due to privacy laws, we cannot register you directly. Additional information regarding how to enroll in the complimentary credit monitoring service is enclosed.

**What You Can Do:**

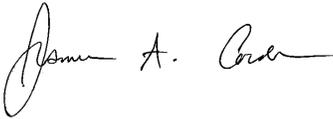
In addition to enrolling in the complimentary credit monitoring service detailed within, we recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

**For More Information:**

Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 855-942-0401, Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time.

Windes has no relationship more important or more meaningful than the one we share with our clients and partners. I want to personally express my deepest regret for any worry or inconvenience that this incident may cause you.

Sincerely,



James A. Cordova  
Managing Partner  
Windes, Inc.

## ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

### TransUnion® *myTrueIdentity* provides you with the following key features:

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- One year of unlimited access to your TransUnion® credit report and credit score.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible.<sup>1</sup>

### **How to Enroll: You can sign up online or via U.S. mail delivery.**

- To enroll in this service, go to the *myTrueIdentity* website at [www.MyTrueIdentity.com](http://www.MyTrueIdentity.com) and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

#### ➤ PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

#### **TransUnion**

Fraud Victim Assistance Dept.  
P.O. Box 6790  
Fullerton, CA 92834  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

#### **Experian**

National Consumer Assistance  
P.O. Box 1017  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

#### **Equifax**

Consumer Fraud Division  
P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

#### ➤ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. You should be aware that using a security 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 security freeze on your credit report. In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail: 1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); 2. Social Security Number; 3. Date of birth; 4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or

<sup>1</sup> (Policy limitations and exclusions may apply.)

ID card, military identification, etc.); 7. Social Security Card, pay stub, or W2; 8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

### ➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

### ➤ **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

### ➤ **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

### ➤ **BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE**

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefits forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

### ➤ **RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)**

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [https://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

### ➤ **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at <http://www.annualcreditreport.com>.

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft). For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580.
- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202, 1-888-743-0023, <https://www.marylandattorneygeneral.gov/>.

- **For New York residents**, you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>
- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, [www.ncdoj.gov](http://www.ncdoj.gov).
- **For Rhode Island Residents**, the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov> or 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.