DrakeSoftware

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

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

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

Drake Software ("Drake") writes to notify you of an incident that may affect the security of some of your personal information. Drake provides software to tax professionals and received your information from your tax professional seeking assistance with its software. We want to provide you with information about the incident, our response and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? On April 2, 2019, Drake learned of suspicious activity related to certain employees' email accounts. We immediately launched an investigation to determine the full nature and scope of this incident. The investigation confirmed that an unknown actor(s) gained access on April 2, 2019 to certain Drake employees' email accounts as the result of a phishing attack against the email accounts. The employees' email credentials were immediately changed, and the email accounts were secured the same day. A leading forensic investigation firm was also retained to assist with Drake's investigation into what happened and what information contained within the email accounts may be affected.

The contents of the accounts were reviewed through an extensive manual and programmatic process to determine what sensitive data may have been accessible. We confirmed the identities of the individuals who may have had information accessible as a result of the incident. Drake began the time-consuming process of reviewing our files to ascertain address information for the impacted individuals. Since that time, Drake has been diligently and tediously organizing this information and its records for purposes of notifying potentially affected individuals about this incident.

What Information was Involved? While we have no evidence that your information was accessed during this incident, or subject to actual or attempted misuse, we confirmed that the information contained in the affected email accounts included your <<b2b_text_1 (Breach Details Variable Text) >><<b2b_text_2 (Breach Details Variable Text) >>.

What We Are Doing. The confidentiality, privacy, and security of our sensitive information is one of our highest priorities. Upon learning of the event, we immediately commenced an investigation to confirm the nature and scope of the incident and to identify what information may be present in the affected email accounts. We also immediately changed the account credentials for the employees' email accounts. While we have measures in place to protect information in our systems, we are reviewing our existing policies and procedures for ways to continue improving existing security. In addition, we notified the Internal Revenue Service, State Departments of Revenue and the Federal Bureau of Investigation regarding this incident. We are actively cooperating in their investigations.

As an added precaution, we are offering you access to two (2) years of identity monitoring services through Kroll at no cost to you. Please review the attached *"Steps You Can Take to Help Protect Against Identity Theft and Fraud"* for information on these services and instruction on how to activate. We encourage you to activate these services as we are not able to act on your behalf to do so.

What You Can Do. Please review the enclosed *"Steps You Can Take to Help Protect Against Identity Theft and Fraud,"* which contains information on what you can do to better protect against possible misuse of your information. You may also activate the identity monitoring services we are offering, as we are unable to do so on your behalf.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact 1-877-460-0845, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

Jami Gibson

Jami Gibson
Vice President, Internal Operations
Drake Software

Steps You Can Take to Help Protect Against Identity Theft and Fraud

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 two (2) years. 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, Fraud Consultation, and Identity Theft Restoration.

Visit **enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **February 12, 2020** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 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. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, 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. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/fraud

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such

fraud should you feel it appropriate to do so. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

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.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www. identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those 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 by way of 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 Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from 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.

For New York residents, the Attorney General may be contacted at: 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.

We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.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. N.W., Washington, D.C. 20580.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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.

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.