



Robert L. Slaughter III
633 West 5th Street, Suite 4000
Los Angeles, California 90071
Robert.Slaughter@lewisbrisbois.com
Direct: 213.680.5028

May 7, 2021

VIA ELECTRONIC Mail

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330
breach.security@maine.gov

Re: Notice of Data Security Incident

Dear Attorney General Aaron Frey:

We represent Special K Tax & Accounting, a sole proprietorship tax preparation service headquartered in Marlborough, Massachusetts. This letter is being sent on behalf of Special K because personal information belonging to Maine residents may have been affected by a recent data security incident. This information may have included the Maine residents' names and Social Security numbers.

On February 28, 2021, Special K learned of unusual activity involving its email account when several clients reported receiving a suspected spam email. Upon discovering this activity, Special K immediately began an investigation and took steps to secure the affected account. We also engaged an independent computer forensics firm in an effort to determine what happened and whether any information within the account had been accessed or acquired without authorization.

While the forensic investigation identified unauthorized access to the email account, it was not able to identify information within the account that may have been viewed, if any. Out of an abundance of caution, Special K conducted a review of the entire contents of the email account to identify any personal information that could have potentially been affected as a result of the incident.

That review concluded on April 8, 2021. Since that time, we have been working to identify up-to-date contact information needed to notify all individuals potentially affected by this incident. On May 4, Special K identified 3 Maine residents within the potentially affected population.

Special K is preparing to issue notification letters to the potentially affected Maine residents via first-class U.S. mail on May 7, 2021. A sample copy of the notification letter is attached hereto.

Attorney General Aaron Frey
May 7, 2021
Page 2

Special K has taken steps to secure the email account and is exploring further measures that can be taken to help ensure the security of its email environment in order to reduce the risk of a similar incident occurring in the future. Special K is also offering complimentary credit monitoring and identity theft protection services to all potentially impacted individuals, as an added layer of protection.

Special K is committed to protecting the personal information in its possession. If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at (213) 680-5028 or via email at Robert.Slaughter@lewisbrisbois.com.

Very truly yours,



Robert L. Slaughter III of
LEWIS BRISBOIS BISGAARD & SMITH LLP

RLS:ALW

Attachment: Consumer Notification Letter Template

Special K Tax and Accounting

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
(800) 939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

May 7, 2021

Subject: Notice of Data Security Incident

Dear <<First Name>> << Last Name>>:

I am writing to inform you of a data security incident that may have affected your personal information. At Special K Tax and Accounting (“Special K”), we take the privacy and security of personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to ensure your information is protected, including enrolling in the complimentary identity protection services we are making available to you.

What Happened? On February 28, 2021, Special K learned of unusual activity involving its email account when several clients reported receiving a suspected spam email. Upon discovering this activity, Special K immediately began an investigation and took steps to secure the affected account. We also engaged an independent computer forensics firm in an effort to determine what happened and whether any information within the account had been accessed or acquired without authorization.

While the forensic investigation identified unauthorized access to the email account, it was not able to identify information within the account that may have been viewed. Out of an abundance of caution, Special K conducted a review of the entire contents of the email account to identify any personal information that could have potentially been affected as a result of the incident. Special K’s review concluded on April 8, 2021, and indicated that some of your information was within the email account. Since that time, we have been working to gather contact information needed to notify individuals.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other Special K information systems. We are not aware of the misuse of any personal information that may have been involved in this incident.

What Information Was Involved? The affected information may have included your <<Information Affected>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our email environment and to reduce the risk of a similar incident occurring in the future.

In addition, we are providing you with information about steps you can take to help protect your personal information and, out of an abundance of caution, we are offering you IDX credit monitoring and identity theft restoration services at no cost to you through IDX, a leader in risk mitigation and response. These services include <<variable 2>> credit and CyberScan™ monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials, and fully managed identity theft recovery services. With this protection, IDX will help you to resolve issues if your identity is compromised.

To receive the IDX services, you must be over the age of 18, have established credit in the United States, have a Social Security number issued in your name, and have a United States residential address associated with your credit file. Please note that the deadline to enroll in the IDX services is August 7, 2021.

What Can You Do? We recommend that you review the guidance included with this letter about how to help protect your information. You can also contact IDX with any questions and to enroll in the free IDX services by calling (800) 939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available to assist you Monday through Friday from 9:00 am – 9:00 pm Eastern Standard Time.

We encourage you to take full advantage of this service offering. IDX® representatives are fully versed on the incident and can answer questions or respond to concerns you may have. More information is enclosed with this letter.

For More Information: Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call our dedicated call center at (800) 939-4170 Monday through Friday from 9:00 am – 9:00 pm Eastern Standard Time.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Judith A. Kellogg, EA
Special K Tax and Accounting

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and 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. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
--	---	---	---

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, Rhode Island, and the District of Columbia can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Consumer Frauds Bureau 28 Liberty Street New York, NY 10005 www.ag.ny.gov 1-800-771-7755	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 www.oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 www.ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 www.riag.ri.gov 1-401-274-4400	District of Columbia Attorney General 400 6 th Street NW Washington, D.C., 20001 http://www.oag.dc.gov 202-727-3400
---	---	---	---	---

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies may be found above.



1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (800) 939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

If you discover any suspicious items and have enrolled in IDX, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work to identify, stop and reverse the damage quickly.

You should also know that you also have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items.