manatt
manatt | phelps | phillips

Donna L. Wilson
Manatt, Phelps & Phillips, LLP
Direct Dial: (310) 312-4144
E-mail: DLWilson@manatt.com

April 28, 2017

Client-Matter: 62634-036

BY E-MAIL AND EXPRESS MAIL

Hawaii Office of Consumer Protection
Leiopapa A Kamehameha Building
235 South Beretania St., Ste. 801
Honolulu, Hawaii 96813

Dear Office of Consumer Protection:

We are writing to notify you that as a result of what appears to be potential access by an unauthorized third party, the personal information of 5,659 customers and family members of Jackson Hewitt Tax Service Inc. ("Jackson Hewitt") with addresses in Hawaii may have been accessed.

Specifically, in February 2017, Jackson Hewitt identified what appeared to be unusual system activity. As a result of this activity, unauthorized third parties may have viewed and/or taken the personal information of Hawaii residents. Jackson Hewitt enlisted the help of the IRS in March and the company has been working with a nationally-recognized cyberforensics team as they investigate this situation. The investigation determined that the potentially unusual activity appears to have occurred primarily between May and December 2016. Jackson Hewitt immediately took steps to minimize the possibility of the activity recurring. It is not conclusive at this time whether personal information may have been misused or taken as a result of this activity, and the company is notifying potentially impacted individuals as a precaution.

At this time, it is not conclusive whether any of the potentially impacted individuals' personal information was misused or taken. However, the personal information may have included names, addresses, telephone numbers, email addresses, social security numbers, taxpayer identification numbers, driver's license or other government identification numbers, bank account numbers and other tax-return preparation related information, including backup or supporting documentation. The information may also have included the names and social security numbers of any individuals claimed as dependents on the involved tax return.

Jackson Hewitt takes this situation seriously. The company is working with government authorities, including the IRS, and nationally recognized experts as they continue to investigate this potential offense against its customers and the company. In addition, the IRS has indicated that it will flag potentially involved returns in order to further protect the associated tax payers.

Jackson Hewitt has been and will continue to proactively implement additional security procedures to help prevent future incidents.

Jackson Hewitt has also taken several important steps to assist customers and address customer concerns, including sending written notices, offering free credit monitoring and protection services, and setting up a hotline for potentially affected customers to call.

Attached hereto is an anonymized draft of the notice letter to be sent by mail on April 29, 2017 to the Hawaii residents whose personal information may have been compromised as a result of this incident.

Best regards,

Donna L. Wilson
Richard P. Lawson
Counsel for Jackson Hewitt Tax Service Inc.

cc: Jackson Hewitt Tax Service Inc.

Enclosure

Jackson Hewitt
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00002
ACD1234

00066
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

April 29, 2017

Dear John Sample:

Thank you for giving us the opportunity to serve you. As a valued customer, we strive to provide you with the highest level of service. Protecting customer information is a top priority for Jackson Hewitt, and we take very seriously our responsibility to our customers. That is why we are reaching out to inform you of a situation that may affect you.

As part of our security efforts, we recently found what appears to have been unusual system activity potentially affecting a limited number of customers. At this time, it is not conclusive whether your personal information may have been misused or taken as a result of this activity. We are notifying you as a precaution. We also are working with government authorities and cyberforensics experts as they continue to investigate this potential offense against our customers and our company. In addition, we are continually seeking to strengthen efforts to protect customer information.

We are taking all necessary actions to address this situation and minimize the risk of a similar incident in the future. We remain laser-focused on serving the interests of our customers and regret any inconvenience this situation may have caused you. Please see more specific details below on the incident, what we have done and are doing, and resources we have made available to you.

Sincerely,

Alan D. Ferber, Chief Executive Officer
Jackson Hewitt Tax Service Inc.

What Happened?
Our detailed review of this situation has identified what may have been unauthorized access to or viewing of some customers' information. Specifically, in February 2017 we identified what appeared to be unusual system activity.

As a result of this activity, unauthorized third parties may have viewed and/or taken your personal information. We enlisted the help of the IRS in March and we have been working with a nationally-recognized cyberforensics team as they investigate this situation. The investigation determined that the potentially unusual activity appears to have primarily occurred between May and December 2016. We immediately took steps to minimize the possibility of the activity recurring. Again, it is not conclusive at this time whether your personal information may have been misused or taken as a result of this activity and we are notifying you as a precaution.

What Information Was Involved?
At this time, it is not conclusive whether any of your personal information was misused or taken. However, the personal information may have included names, addresses, telephone numbers, email addresses, social security numbers, taxpayer identification numbers, driver's license or other government identification numbers, bank account numbers and other tax-return preparation related information, including backup or supporting documentation. The information may also have included the names and social security numbers of any individuals you claim as dependents.

What We Are Doing
We take this situation seriously. We are working with government authorities, including the IRS, and nationally recognized experts as they continue to investigate this potential offense against our customers and our company. In addition, the IRS has indicated that it will flag potentially involved returns in order to further protect the associated tax payers. We have been and will continue to proactively implement additional security procedures to help prevent future incidents.

In addition, Jackson Hewitt has taken several important steps to assist customers and address customer concerns, including sending these notices, offering free credit monitoring and protection services and setting up a hotline for potentially affected customers to call (see below).

For More Information
We have established a confidential and dedicated hotline so you can contact us with questions about the incident or the contents of this letter. This hotline is staffed with professionals familiar with this incident and is available Monday through Saturday, 9 a.m. to 9 p.m. EST. Please refer to the information below.

What You Can Do
As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-865-4452 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-865-4452 using the following redemption code: Redemption Code. If you believe anyone else in your household may have been impacted in this situation, please call AllClear ID at 1-855-865-4452.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options. In addition to providing complimentary identity protection services to you, if you believe that this situation may have impacted other individuals whose personal identification information you provided to Jackson Hewitt in connection with a prior year's return (e.g., non-notified dependents or household employees), please call AllClear ID at 1-855-865-4452.

There are certain steps you can take to protect against potential fraudulent activity. To the extent that your account name and access information may have been compromised, we encourage you to promptly change your credentials and take appropriate steps to protect all online accounts for which you use the same credentials.

You are entitled to obtain a copy of your credit report, free of charge. A credit report contains information about your credit history and the status of your credit accounts. Your credit report could alert you to fraudulent activity being carried on in your name by an identity thief. Please remain vigilant for incidents of fraud and identity theft by reviewing all of your account statements and monitoring your free credit reports by contacting any one of the national consumer reporting agencies set forth below.

The agencies can also provide you with information on how to place a fraud alert or security freeze on your account. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been the victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift or permanently remove a security freeze. In order to request a security freeze, you will need to provide the following information: full name, Social Security number, date of birth, addresses of residence for the past five years, proof of current address, legible photocopy of a government-issued identification card, copy of police report or other law enforcement complaint or report (if the victim of identity theft), and payment by check, money order or credit card (if not a victim of identity theft).

Equifax
P.O. Box 740241
Atlanta, GA 30374
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 6790
Fullerton, CA 92834
1-800-680-7289
www.transunion.com

Other Important Information

RESIDENTS OF ILLINOIS: State law advises you to obtain information from the Federal Trade Commission, as well as the above-listed consumer reporting agencies, about fraud alerts and security freezes.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, D.C. 20580
202-326-2222
www.ftc.gov

RESIDENTS OF IOWA: State law advises you to report any suspected incidents of identity theft to local law enforcement or the Attorney General.

RESIDENTS OF MARYLAND: You can obtain information from the Federal Trade Commission and the Office of the Attorney General about steps you can take to avoid identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, D.C. 20580
202-326-2222
www.ftc.gov

RESIDENTS OF NORTH CAROLINA: You can obtain information from the North Carolina Office of the Attorney General and the Federal Trade Commission about preventing identity theft.

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.gov

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, D.C. 20580
202-326-2222
www.ftc.gov

RESIDENTS OF OREGON: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission.

RESIDENTS OF RHODE ISLAND: State law advises you that the state Attorney General can be contacted at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077