Clark Hill

Jason Schwent
T (312) 985-5939
F (312) 517-7572
Email:jschwent@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

December 30, 2022

Via Portal

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Dear Attorney General Frey:

We represent Wing Financial Services ("Wing Financial") with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. Wing Financial is an independently owned and operated Jackson Hewitt franchise located in Bartlesville, Oklahoma. Wing Financial is committed to answering any questions you may have about the data security incident, the response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On August 7, 2022, certain client records were accessible to unauthorized parties on the internet. Wing Financial immediately began an internal investigation and hired independent computer forensic experts to help with determining what occurred and the scope of individuals that may have been impacted. The investigation determined that there had been unauthorized access to Wing Financial's systems. On November 10, 2022, Wing Financial determined the files exposed included personally identifiable information. Wing Financial provided notice to all individuals whose information was in the system at the time of the unauthorized access. Information stored in the system at the time of the incident may include the following data elements: names, addresses, dates of birth, unique biometric information, Social Security numbers, driver's license numbers or other state identification card numbers, individual tax identification numbers, passport numbers or other government ID, tax identification numbers, financial account numbers with access codes, payment card numbers, health insurance policy numbers, and medical treatment/history.

2. Number of Maine residents affected.

Two (2) Maine residents were notified of the incident. A notification letter was sent to the potentially affected individuals on December 1, 2022 and December 2, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

Wing Financial took steps to address this incident and prevent similar incidents in the future. Since the incident, Wing Financial immediately limited access to the potentially affected systems and began gathering evidence relating to the incident. Wing Financial communicated with the security and privacy professionals to analyze and mitigate any potential issues. Wing Financial changed all of its user's login credentials and further trained its employees on securing information. Additionally, affected individuals were offered 12 months of credit monitoring and identity protection services through Cyberscout.

4. Contact information.

Wing Financial takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

Jason M. Schwent
Senior Counsel

cc: Sunaina Ramesh

Wing Financial Services, LLC
c/o Cyberscout
38120 Amrhein Road
Livonia, MI 48150

WING FINANCIAL SERVICES, LLC

[redacted]

000010103G0500

P

Notice of Data Security Incident

December 1, 2022

Dear [redacted]:

At Wing Financial Services, LLC ("Wing Financial"), maintaining our client's trust and protecting our client's personal information are among our highest priorities. Wing Financial is an independently owned and operated Jackson Hewitt franchise and we provided tax preparation services on your behalf or on behalf of someone else who claimed you as a dependent on their tax return. We are writing with important information regarding a recent data security incident. We want to provide information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that certain client records appeared to have been exposed to an unaffiliated third-party website by an unauthorized user. We performed a thorough review of the disclosed records and have confirmed these records relate to one Wing Financial server. Wing Financial changed all of its user's login credentials and has confirmed that its server is now secure and access is limited. The Jackson Hewitt corporate environment and systems were not impacted as a result of this incident.

What We Are Doing.

Upon learning of the incident, we commenced a prompt and thorough investigation with external security and privacy professionals to assess the scope and extent of the records that were disclosed. After a thorough manual review of the impacted client records, we discovered on November 10, 2022 that the files exposed on August 7, 2022 contained your personal information. Since the incident, Wing Financial has taken the following measures: Wing Financial immediately limited access to potentially affected servers and began gathering evidence relating to the incident. Wing Financial communicated with the security and privacy professionals to analyze and mitigate any potential issues. Wing Financial changed all of its user's login credentials and further trained its employees on securing information.

What Information Was Involved?

The personal information involved included [redacted]. If applicable, your spouse's, partner's and/or dependent(s)' personal information may have also been impacted by this incident. Each impacted individual will receive their own letter.

What You Can Do.

To protect you and your information, 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

twelve (12) 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

This service helps detect possible misuse of your information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This service is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention, including instructions on how to activate your complimentary twelve (12) months membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your information, including placing a fraud alert and/or security freeze on your credit files, obtaining a free credit report, and/or reporting fraudulent activity to the IRS. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We regret any inconvenience that this may cause you. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-888-926-2335 between the hours of 8:00 am and 8:00 pm Eastern time, Monday through Friday, excluding holidays. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information.

Sincerely,

Wing Financial Services LLC

Wing Financial Services, LLC

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary twelve (12) Month Credit Monitoring.

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/wingfinancial** 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 within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. 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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center. html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide

credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. 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.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

6. Reporting Identity Fraud to the IRS.

If you your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- **File an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf)**
    - *Instructions for Form 14039* – In Section A check box 1. / In Section B check box 2. / Insert this in the "Please provide an explanation" box: I receive notice that my name and Social Security number may have been used to file a fraudulent tax return that was accepted by the IRS and/or state tax agency.
        - This form should be mailed or faxed to the IRS: Internal Revenue Service, Fresno, CA 93888-0025; 855-807-5720
- Call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm); and/or
- File a police report with your local police department. It may be appropriate to provide a copy of this letter.

Additional information regarding preventing tax-related identity theft can be found at: http://www.irs.gov/uac/Identity-Protection.

For further information and guidance from the IRS about tax-related identity theft, please visit: https://www.irs.gov/uac/taxpayer-guide-to-identity-theft (Taxpayer Guide to Identity Theft) and https://www.irs.gov/pub/irs-pdf/p5027.pdf (IRS Publication 5027, Identity Theft Information for Taxpayers).

You may request an IRS Identity Protection PIN (IP PIN) at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. An IP PIN is a six-digit number that

prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps IRS verify your identity when you file your electronic or paper tax return.

7. <u>You Can Obtain Additional Information</u>.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

* * * * *

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal

identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.