

Jason M. Schwent
T (312) 985-5939
F +13125177573
Email:jschwent@clarkhill.com

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

January 18, 2024

VIA ELECTRONIC MAIL

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown,

We represent Hamilton Investment Group LLC (“Hamilton Tax”) with respect to a cybersecurity event involving personal information as described below. Hamilton Tax provides tax preparation and planning services to individuals. Hamilton Tax takes the security of the information of its patients seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident.

On September 20th, 2023, Hamilton Tax discovered that a server managed by a third party containing the tax information of certain Hamilton Tax clients was infected with malware. This malware potentially provided an unauthorized user the ability to obtain the data of clients of Hamilton Tax. Hamilton Tax then investigated the data contained within the affected server and on November 30th, 2023, identified the affected clients. The affected personal information contains names and some combination of the following: date of birth, address, Social Security number, financial account information and income related information.

2. Number of residents affected.

Eight (8) Maryland residents were notified of the incident. A letter is being sent to the affected individuals on January 18th, 2024. A copy of the of the template notification letter is enclosed.

3. Steps taken in response to the incident.

Hamilton Tax took several steps to enhance its security posture after learning of the incident. Hamilton Tax ceased using its secure file transfer tool and upgraded to a tool with more robust security measures. Hamilton Tax now requires all clients to obtain their own IRS IP PIN and enhanced the security controls around client documents. Affected Hamilton Tax clients will be offered twelve months of credit monitoring and identity protection services through IDX.

4. Contact Information

CCH takes the security of the information in its control seriously and is committed to ensuring it is appropriately 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

A handwritten signature in black ink, appearing to read 'JS', followed by a long horizontal line extending to the right.

Jason M. Schwent

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 18, 2024



K6696-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 ADULTS

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



RE: Notice of Data [Security Incident/Breach]

Dear Sample A. Sample:

Hamilton Investment LLC ("Hamilton") recently learned that it was impacted by a cybersecurity incident (the "Incident") that may have involved some of your data. While we have no indication that any of your personal information has been misused, out of an abundance of caution, we wanted to let you know about the Incident. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience that this notification may cause you.

What Happened?

On September 20th, 2023, Hamilton discovered that a server managed by a third party containing the tax information of certain Hamilton clients was infected with malware. Immediately upon detection of the malware, we took action to contain and investigate the Incident. The investigation determined that a vendor's security controls didn't function as intended, allowing the deployment of malware that allowed unauthorized access to information on that server. We reviewed the server and determined that it contained personal information of some of our clients and that, specifically, the server contained some of your personal information. While the presence of the malware was confirmed, there is no evidence that your data was impacted. This notice is being provided out of an abundance of caution.

What Information Was Involved?

From our review of the data in the server, your name, date of birth, address, social security number, financial account information and income related information may have been accessed during the Incident.

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary ##-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: April 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**



If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-918-0252 by April 30, 2024. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

IRS Guidance On Potential Identity Theft:

The IRS has put together a list of signs that may indicate when a taxpayer has been the victim of identity theft. These signs include the following:

- You get a letter from the IRS inquiring about a suspicious tax return that you did not file.
- You can't e-file your tax return because of a duplicate Social Security number.
- You get a tax transcript in the mail that you did not request.
- You get an IRS notice that an online account has been created in your name.
- You get an IRS notice that your existing online account has been accessed or disabled when you took no action.
- You get an IRS notice that you owe additional tax or refund offset, or that you have had collection actions taken against you for a year you did not file a tax return.
- IRS records indicate you received wages or other income from an employer you didn't work for.
- You've been assigned an Employer Identification Number, but you did not request an EIN.

If you experience any of these signs, the IRS has provided additional steps taxpayers can take to protect themselves and additional resources at <https://www.irs.gov/identity-theft-central>.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at sign-up:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-833-918-0252. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Additional Recommended Steps to Help Protect Your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, 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 ID Care 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 on your behalf to identify, stop and reverse the damage quickly.

You should also know that you 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. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud Reporting and
Credit Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.



4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

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

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 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_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.

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/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 1-833-918-0252 toll-free Monday through Friday from 8 am – 8 pm Central Time (excluding major U.S. holidays).

Sincerely,

Hamilton Tax & Accounting

Steven C. Hamilton II

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.