

# CLARK HILL

---

Melissa K. Ventrone  
T 312.360.2506  
F 312.517.7572  
Email: [mventrone@clarkhill.com](mailto:mventrone@clarkhill.com)

Clark Hill  
130 East Randolph Street  
Suite 3900  
Chicago, IL 60601  
T 312.985.5900  
F 312.985.5999

[clarkhill.com](http://clarkhill.com)

September 2, 2020

*Via Email to [attorneygeneral@doj.nh.gov](mailto:attorneygeneral@doj.nh.gov)*

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03302

Dear Attorney General MacDonald:

We represent Poulsen & Stowell, PLLC (“Poulsen & Stowell”), a Certified Public Accounting firm, with respect to a data security incident involving the potential exposure of certain personally identifiable information (“PII”) described in more detail below. Poulsen & Stowell is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

## **1. Nature of security incident.**

In June 2020, Poulsen & Stowell learned that a limited number of our clients had experienced fraudulent tax filings. Poulsen & Stowell engaged independent computer forensic experts to investigate its network and systems and determine if there was any unauthorized access to client data. On July 22<sup>nd</sup>, 2020, the forensic investigators informed Poulsen & Stowell that they found a malicious software, called malware, on a corporate computer. Unfortunately, they were unable to determine what client data, if any, may have been accessed via this malware. Thus, out of an abundance of caution, Poulsen & Stowell notified all clients of this incident and provided them with access to credit monitoring and identity protection services. Impacted individuals were informed that information stored on the system at the time malware was present may have included their name, address, Social Security number, bank account information if that was provided to Poulsen & Stowell, and other tax related information.

## **2. Number of residents affected.**

September 2, 2020

Page 2

Four (4) New Hampshire residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on September 2, 2020 (a copy of the form notification letter is enclosed).

**3. Steps taken or plan to take relating to the incident.**

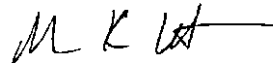
Poulsen & Stowell took steps to address this incident and prevent similar incidents in the future. They removed the malicious software from the infected computer, changed all passwords, and conducted additional anti-virus scanning on all systems. Affected individuals were offered 12 months of credit monitoring and identity protection services through ID Experts.

**4. Contact information.**

Poulsen & Stowell takes the security of the information in its control seriously and is committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at [mventrone@clarkhill.com](mailto:mventrone@clarkhill.com) or (312) 360-2506.

Very truly yours,

CLARK HILL



Melissa K. Ventrone  
Partner

MKV

Enclosure



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

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

<<MAIL MERGE ADRESSEE>>  
<<Address 1>> <<Address 2>>  
<<City>>, <<State>> <<Zip>>

August 25, 2020

### Notice of Data Incident

Dear <<MAIL MERGE ADRESSEE>>,

We wanted to let you know about a potential data security incident experienced by Poulsen & Stowell, PLLC that may have impacted your personal information. We value and respect the privacy of your information, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

#### What happened?

In June 2020, we learned that a limited number of our clients had experienced fraudulent tax filings. As soon as we learned about this, we hired an independent computer forensics firm to investigate our network and systems and determine if there was any unauthorized access to client data. On July 22<sup>nd</sup>, 2020, our forensic investigators informed us that they found a malicious software, called malware, on a corporate computer. Unfortunately, they were unable to determine what client data may have been accessed via this malware, so we are notifying all clients of this incident and offering services to protect against fraud and identity theft.

#### What Information was involved?

Information that may be affected includes your tax return information, such as your name, address, Social Security number, bank account number if you provided that to us, and other tax related information.

#### What we are doing:

In response to this incident, we had our forensic investigators review our server for any signs of malicious activity, we have removed the malicious software from the infected computer, changed all passwords, and conducted additional anti-virus scanning on all systems. We have notified the IRS of this incident and we are working with our investigators to identify additional security measures to further enhance the security of our systems.

The security of your information is of the utmost importance to us. We have arranged for you and your immediate family members to receive complimentary credit monitoring and identity protection services at no cost to you provided by MyIDCare™ powered by ID Experts for 12 months. All you need to do is enroll in the services described below.

#### What you can do:

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (800) 939-4170 or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is November 25, 2020. Please utilize the same enrollment code contained in this letter to enroll members of your immediate family (including spouse and/or minor dependents).

**How to Enroll: You can sign up online or via telephone.**

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

If you received a fraudulent deposit from the IRS into your bank account, the IRS has recommended the following:

1. Do not spend this money, as it must be returned to the IRS.
2. Contact your bank's fraud department and let them know that the money was deposited as a result of a fraudulent tax filing, and that the deposit should be reversed as soon as possible.
3. Do not return the money by check. The most reliable way for the money to be returned and credited to you is to instruct your bank to reverse the deposit.
4. If you have any issues with your bank and the return of the money, please contact me.

If a fraudulent paper check is received in error, do not deposit it. The IRS recommends you write VOID in the endorsement section on the back of the check and promptly send it back to the appropriate IRS location with a note that you are returning an erroneous refund check.

Additionally, if you know or suspect you are a victim of tax-related identity theft, the IRS recommends the following steps:

- Respond immediately to any IRS written notice. **The IRS will not contact you via phone.**
- If you received a Letter 5071C or a Letter 4883C from the IRS indicating that they received a suspicious tax return with your name on it, you should follow the instructions on that letter to verify your identity with the IRS. Once you verify your identity, you can advise the IRS that you did not file the suspicious tax return. Additionally, you may be asked to file a paper return for the current filing season.
- If you believe you may be a victim of tax fraud but have not received a Letter 4883C from the IRS, you should fill out and submit IRS Form 14039, which is available at IRS.gov. We can provide you with a copy of that form and assist you with filling it out if you would like.

If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490. The IRS has teams available to assist. You should also visit <https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works> for more information.

**Other important information:**

If you have any questions or concerns, please call (800) 939-4170 Monday through Friday, 6 am - 6 pm Pacific Time. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

The image shows two handwritten signatures in black ink. The signature on the left is for Ethan Poulsen, and the signature on the right is for Bryan Stowell. Both signatures are written in a cursive, flowing style.

Ethan Poulsen, CPA & Bryan Stowell, CPA  
Poulsen & Stowell, PLLC



## Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go to <https://app.myidcare.com/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 MyIDCare 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, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare 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 credit identity.
- 4. 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](http://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 MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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.

**5. 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  
1-866-349-5191  
P.O. Box 105069  
Atlanta, GA 30348-5069  
[www.alerts.equifax.com](http://www.alerts.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://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.**

**6. 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.

**7. 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 (<http://www.ca.gov/Privacy>) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**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](http://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/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://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/](http://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](http://www.riag.ri.gov), Telephone: 401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.