WILLIAM H. BREWER
Certified Public Accountant
858 Washington Street
P.O. Box 306
Bath, Maine 04530
---
(207) 443-9759

Notice of Data Breach

What Happened

We are writing to inform you of a recent security incident at William H. Brewer & Co., CPA (Brewer). In late February of this year, Brewer experienced an unauthorized breach of our servers. We do not know when the breach first occurred but on February 29, 2024, Brewer's two servers were discovered to be encrypted. There is no evidence that any data was extracted, however it cannot be ruled out. We are providing notice that as a result of the breach incident, personally identifiable information (PII) relating to you which existed on our computer system may have been accessed or even transferred during the event.

What Information Was Involved

We understand that the PII potentially accessed or taken may include Social Security numbers (SSN's), tax identification numbers, birthdates, bank account numbers, and telephone and address information from such files, among other information that was located on our system.

What We Are Doing

Brewer has consulted with IT experts, computer security experts, a forensic consultant and retained counsel to assist in our response to this incident. Although forensic efforts continue, the investigation suggests that your PII may have been exposed and/or exfiltrated during the incident. Please note, we have received no information to date that any individual's PII has in fact been taken or otherwise used.

We are offering to pay for the costs of credit monitoring/identity theft protection for you from Equifax Complete Premier for the next 18 months and would urge you to lock your credit with the credit reporting agencies if you have not already done so. Credit locking/freezing is addressed in a separate section below. While some commentators believe that third party credit and/or identity theft monitoring is unnecessary if your credit reports are locked, we leave that decision to you. If you decide you do want the credit monitoring option, please email us at office@whbrewercpa.com or phone (207) 443-9759 and we will provide you with details on how to enroll.

Massachusetts Mandated Notice Information

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

What You Can Do

The principal risks from stolen PII include unauthorized credit risks and risks to governmental transactions including tax returns and government benefits. Attached to this email is a pamphlet from the Social Security Administration reflecting governmental resources and further specific links for reporting and monitoring.

With respect to unauthorized credit risks, it is recommended that you immediately lock down your credit reports with each of the credit rating agencies (E.g. Equifax, Transunion, Experian, etc.) if you have not already done so. When locked, no third parties are allowed to make credit inquiries even if they have your social security number, unless and until you unlock your account for that purpose. Further information on this process is available here:

https://www.nerdwallet.com/article/finance/how-to-freeze-credit.

In short, you may place a security freeze on your credit reports, free of charge. 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. Please remember, under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail to the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
https://www.equifax.com/personal/credit-report-services/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2; and
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

You may also place a fraud alert on your credit report. A fraud alert makes it more difficult for someone to open a new credit account in your name. A business must verify your identity before it issues new credit in your name. When you place a fraud alert on your credit

report, you can get a free copy of your credit report from each of the three credit bureaus. A fraud alert typically lasts for one year but can be renewed thereafter. To place a fraud alert, you may do so through any one of the three credit bureaus mentioned above, Equifax, Experian, and TransUnion. You do not need to contact all three credit bureaus. The credit bureau you contact must tell the other two credit bureaus. More information about fraud alerts and security freezes can be found at the Federal Trade Commission's website, here: https://www.ftc.gov/.

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts

Credit Monitoring

While some commentators believe that third party credit and/or identity theft monitoring is unnecessary if your credit reports are locked, we leave that decision to you and are offering to pay for the costs of credit monitoring/identity theft protection for you from Equifax Complete Premier[1] for the next 18 months. Please contact us by email (office@whbrewercpa.com), mail or phone (207) 443-9759 and we will provide you with details on how to enroll.

More Information

We are in the process of reporting the incident to the relevant law enforcement authorities. While such events have unfortunately become much more commonplace, we apologize in advance for any inconvenience resulting from this incident. Please contact us if you have any questions regarding this notice or believe you have been impacted by the incident other than as reported in this letter.

Regards,

Dated: April , 2024

William H. Brewer

Enclosure

[1] The Equifax Complete Premier per person plan is described here: https://www.equifax.com/personal/products/credit/monitoring-product-comparison

Securing today and tomorrow

Identity Theft and Your Social Security Number

SSA.gov

Identity theft is one of the fastest growing crimes in America. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.

Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

Your number is confidential

The Social Security Administration protects your Social Security number and keeps your records confidential. We don't give your number to anyone, except when authorized by law. You should be careful about sharing your number, even when you're asked for it. You should ask why your number is needed, how it'll be used, and what will happen if you refuse. The answers to these questions can help you decide if you want to give out your Social Security number.

How might someone steal your number?

Identity thieves get your personal information by:

- Stealing wallets, purses, and your mail (bank and credit card statements, pre-approved credit offers, new checks, and tax information).
- Stealing personal information you provide to an unsecured site online, from business or personnel records at work, and personal information in your home.
- Rummaging through your trash, the trash of businesses, and public trash dumps for personal data.
- Buying personal information from "inside" sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services, or credit.
- Posing by phone or email as someone who legitimately needs information about you, such as employers, landlords, or government agencies.

Be careful with your Social Security card and number

When you start a job, make sure your employer has your correct Social Security number so your records are correct. Provide your Social Security number to your financial institution(s) for

tax reporting purposes. Keep your card and any other document that shows your Social Security number in a safe place. DO NOT routinely carry your card or other documents that display your number.

What if you think someone is using your number?

Sometimes more than one person uses the same Social Security number, either on purpose or by accident. If you suspect someone is using your number for work purposes, you should contact us to report the problem. We'll review your earnings with you to ensure our records are correct.

You also may review earnings posted to your record on your *Social Security Statement*. The *Statement* is available online to workers age 18 and older. To get your *Statement*, go to ***www.ssa.gov/myaccount*** and create an account.

What if an identity thief is creating credit problems for you?

If someone has misused your Social Security number or other personal information to create credit or other problems for you, Social Security can't resolve these problems. But there are several things you should do.

Visit ***IdentityTheft.gov*** to report identity theft and get a recovery plan. ***IdentityTheft.gov*** guides you through each step of the recovery process. It's a one-stop resource managed by the Federal Trade Commission, the nation's consumer protection agency. You can also call **1-877-IDTHEFT (1-877-438-4338)**; TTY **1-866-653-4261**.

You may want to contact the Internal Revenue Service (IRS). An identity thief also might use your Social Security number to file a tax return to receive your refund. If you're eligible for a refund, a thief could file a tax return before you do and get your refund. Then, when you do file, the IRS will think you already received your refund. If your Social Security number is stolen, another person may use it to get a job. That person's employer would report earned income to the IRS using your Social Security number. This will make it appear that you didn't report all of your income on your tax return. If you think you may have tax issues because someone has stolen your identity, go to ***www.irs.gov/uac/Identity-Protection*** or call **1-800-908-4490**.

Also, you should file an online complaint with the Internet Crime Complaint Center (IC3) at ***www.ic3.gov***.

The IC3 gives victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations.

IC3 sends every complaint to one or more law enforcement or regulatory agencies with jurisdiction.

IC3's mission is to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cybercrime. The IC3 serves the broader law enforcement community that combats internet crime. This includes federal, state, local, and international agencies.

The IC3 reflects a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center, and the Bureau of Justice Assistance.

You should also monitor your credit report periodically. You can get free credit reports online at ***www.annualcreditreport.com***.

Should you get a new Social Security number?

If you've done all you can to fix the problems resulting from misuse of your Social Security number, and someone is still using your number, we may assign you a new number.

You can't get a new Social Security number:

- If your Social Security card is lost or stolen, but there's no evidence that someone is using your number.
- To avoid the consequences of filing for bankruptcy.

- If you intend to avoid the law or any legal responsibility.

If you decide to apply for a new number, you'll need to prove your identity, age, and U.S. citizenship or immigration status. For more information, ask for *Your Social Security Number and Card* (Publication Number 05-10002). You'll also need to provide evidence that you're having ongoing problems because of the misuse.

Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security number, you shouldn't use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.

Contacting Social Security

The most convenient way to do business with us from anywhere, on any device, is to visit ***www.ssa.gov***. There are several things you can do online: apply for benefits; get useful information; find publications; and get answers to frequently asked questions.

Or, you can call us toll-free at **1-800-772-1213** or at **1-800-325-0778** (TTY) if you're deaf or hard of hearing. We can answer your call from 7 a.m. to 7 p.m., weekdays. You can also use our automated services via telephone, 24 hours a day. We look forward to serving you.

Social Security Administration
Publication No. 05-10064
July 2021 (June 2018 edition may be used)
Identity Theft and Your Social Security Number
Produced and published at U.S. taxpayer expense