Website Notice

Summit Insurance Services, Inc. Issues Notice of Data Security Incident

On or about December 2, 2024, Summit Insurance Services, Inc. ("Summit") experienced a data security incident which may have affected the personal or health information of certain individuals. Summit has since diligently worked to determine what happened and what information was involved as a result of this incident. Summit promptly launched an investigation, reported the incident to law enforcement and engaged a national cybersecurity firm to assist in assessing the scope of the incident and took steps to mitigate the potential impact to the community. Following an investigation conducted by third-party forensic specialists, it was determined the incident occurred between September 18, 2024, and December 2, 2024. Upon identification of the potentially impacted data set, data mining was conducted over several months to identify the potentially impacted individuals and what elements of personally identifiable information and/or health information may have been affected. Upon completion of the forensic investigation and data mining, efforts were then initiated to locate sufficient address information for the potentially impacted population.

The elements of personal information that may have been impacted as a result of this incident varies per individual and potentially included: name, address, date of birth, medical information, and health insurance information and Social Security number or tax identification number. As of this writing, Summit has not received any reports from individuals of misuse, identity theft or fraud related to the incident. As data incidents are increasingly common, Summit encourages you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information.

Unfortunately, these types of incidents are becoming increasingly common and organizations with the most sophisticated IT infrastructure available continue to be affected. Summit understands the inconvenience or concern this incident may cause, is committed to ensuring the security of all information in its control, and has taken steps to strengthen its security posture.

Summit mailed formal notification letters to potentially affected individuals on _____. The letters included additional information about what occurred, outlined the personal information that was potentially impacted for each individual, and provided a toll-free number that individuals can call to learn more about the incident. The call center can be reached at 1-800-405-6108, and is available Monday through Friday, 8:00 a.m. and 8:00 p.m. Eastern Time, Monday through Friday, excluding US holidays.

Steps Individuals Can Take to Protect Personal Information

Monitor Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Fraud Alerts

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a

fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

Security Freeze

Consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report.

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094

Free Credit Reports

Further, you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available

Website Notice

at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Implementing an Identity Protection PIN (IP PIN) with the IRS

An Identity Protection PIN (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 the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.
- FAQs about the Identity Protection Personal Identification Number (IP PIN)

Individuals may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.