

From: Adrian Senyszyn <asenyszyn@germer-sa.com>
Sent: Thursday, November 7, 2024 2:43 PM
To: IDTheft
Subject: Maryland Notice of Data Breach / Polk County Sheriff's Office
Attachments: IDX Breach Notification Letter - Adult SSN V.3 (Print Proof).pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Data breach

Dear OAG Representative:

The Polk County Sheriff's Office ("Sheriff's Office") is writing to inform you that it experienced a cybersecurity incident involving the sensitive personal information of two (2) Maryland residents.

What Happened

On September 26, 2024, the Sheriff's Office determined that an unauthorized third-party gained access to some of its systems at various times between September 14-17, 2024. The unauthorized third-party also launched a malicious software attack. The Sheriff's Office immediately began an investigation and engaged leading third-party cybersecurity and forensic experts to assist. It also notified law enforcement and swiftly contained the incident. A thorough review of the impacted data was conducted to identify what information was involved and which individuals may have been impacted.

Number of Maryland Residents Affected

Two (2) Maryland residents appear to have been affected. A sample copy of the notice being sent to consumers is attached.

Information Compromised

The individuals first and last name, and one or more of the following: Social Security number, Driver's License number, and/or other government identification number.

Steps to Restore Integrity of the System

The Sheriff's Office implemented additional security protocols designed to enhance the security of its network, internal systems and applications. The Sheriff's Office continues to work with law enforcement and evaluate additional steps that may be taken to further increase its security posture.

Kindly please contact me if you have any questions or concerns. Sincerely,

Adrian Senyszyn

Principal
Germer PLLC
Plaza Las Campanas
1826 North Loop 1604 West, Suite 300
San Antonio, Texas 78248
Office: (210) 640-1650
Direct: (210) 640-1675
Fax: (512) 472-0721
Email: asenyszyn@germer-sa.com

GERMER

PRIVILEGED & CONFIDENTIAL COMMUNICATION: This e-mail and any files transmitted with it is confidential and is intended solely for the use of the individual or entity to whom they are addressed. This communication may contain material protected by the Attorney-Client privilege and/or constitute attorney work product. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please immediately notify us by telephone at (210) 640-1650, (713) 650-1313, or (512) 472-0288 or return by e-mail to: postmaster@germer.com. You will be reimbursed for reasonable costs incurred in notifying us.

Polk County Sheriff's Office
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>> or <<IMB>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

November 12, 2024

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

The Polk County Sheriff's Office ("Sheriff's Office") is writing to inform you that it experienced a cybersecurity incident involving some of your sensitive personal information. This notice explains the incident, steps we have taken in response to it, and additional information about steps you may take to help protect your information.

What Happened

On September 26, 2024, the Sheriff's Office determined that an unauthorized third-party gained access to some of its systems at various times between September 14-17, 2024. The unauthorized third-party also launched a malicious software attack. The Sheriff's Office immediately began an investigation and engaged leading third-party cybersecurity and forensic experts to assist. It also notified law enforcement and swiftly contained the incident. A thorough review of the impacted data was conducted to identify what information was involved and which individuals may have been impacted.

What Information Was Involved

The review determined that the data involved contained some of your sensitive personal information, including your name, and one or more of the following: Social Security number, Driver's License number, and/or other government identification number.

What We Are Doing

To help prevent a similar type of incident from occurring in the future, the Sheriff's Office implemented additional security protocols designed to enhance the security of its network, internal systems and applications. The Sheriff's Office continues to work with law enforcement and evaluate additional steps that may be taken to further increase its security posture.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: [12 months/24 months] of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 12, 2025.

Again, at this time, there is no indication that your personal information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

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.

Please call 1-833-903-3648 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

Sheriff Byron Lyons
Polk County Sheriff's Office

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/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 IDX identity protection 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, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 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 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.

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.equifax.com

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

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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 (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, 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, 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, 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: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.