

BakerHostetler

Baker&Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Benjamin D. Wanger
direct dial: 215.564.1601
bwanger@bakerlaw.com

June 15, 2022

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Brian E. Frosh
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, the City of Hobart, Indiana (“the City”), to provide notice of a security incident involving Maryland residents. The City of Hobart is a local government in the State of Indiana operating exclusively within Indiana and, as such, is providing this notice as a courtesy.

The City recently concluded its investigation of an incident that involved unauthorized access to certain City computer systems. Upon identifying the incident, the City immediately secured the systems involved and began an investigation. Through the investigation, the City determined that between December 28, 2021 and January 24, 2022, an unauthorized actor accessed certain files contained on the Police Department’s servers. The City reviewed those files and on April 26, 2022, the City determined that a file contained the name and one or more of: Social Security number, driver’s license number, payment card number and/or medical treatment information of six Maryland residents.

Beginning today, the City is providing written notice via United States Postal Service mail to the Maryland¹ residents whose personal information was potentially accessed by an unauthorized party. To help monitor for any potential misuse of personal information, the City is offering a complimentary one-year membership in credit monitoring and identity theft protection services

¹ This report is not, and does not constitute, a waiver of the City’s objection that Maryland lacks personal jurisdiction over the City regarding any claims related to this data security incident.

June 15, 2022

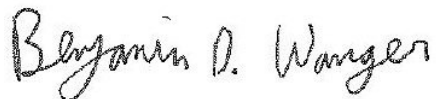
Page 2

through IDX to the residents whose Social Security or driver's license numbers were affected. The notice letter also provides a telephone number that notice recipients can call with any questions they may have.

To help prevent a similar incident from occurring in the future, the City has implemented additional security measures to enhance the security of its network and is continuing to train its employees concerning data security.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink that reads "Benjamin D. Wanger". The signature is written in a cursive, slightly slanted style.

Benjamin D. Wanger
Counsel

Enclosure



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:

1-833-774-2041

Or Visit:

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

Enrollment Code:

<<XXXXXXXX>>

<<Name 1>> <<Name 2>>
<<Address 1>> <<Address 2>>
<<City>><<State>><<Zip>>

June 15, 2022

Dear <<Name 1>> <<Name 2>>:

The City of Hobart, Indiana recognizes the importance of protecting the personal information we maintain. We are writing to let you know of a data security incident that involved some of your information. This notice explains the incident, measures we have taken, and some additional steps you may consider taking in response.

We recently concluded our investigation of an incident that involved unauthorized access to certain City computer systems. Upon identifying the incident, we immediately secured the systems involved and began an investigation. Through the investigation, we determined that between December 28, 2021 and January 24, 2022, an unauthorized actor accessed certain files contained on the Police Department's servers. We reviewed those files and on April 26, 2022, we identified one or more file(s) containing your name and <<VARIABLE DATA>>.

We encourage you to remain vigilant by regularly reviewing your credit reports and financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, please contact the relevant provider immediately. We are offering you one year of complimentary identity monitoring services through IDX. IDX identity protection services include: one year of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-774-2041 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. Please note the deadline to enroll is September 15, 2022. For more information on identity theft prevention, please see the pages following this letter.

To help prevent a similar incident from occurring in the future, we have implemented additional security measures to enhance the security of our network and we are continuing to train our employees concerning data security. If you have any questions, please call our dedicated call center at 1-833-774-2041 Monday through Friday from 8:00 am to 8:00 pm Central Time.

Sincerely,

A handwritten signature in blue ink, appearing to read "Brian K. Snedecor".

Brian K. Snedecor
Mayor, City of Hobart

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

You may contact The City of Hobart, Indiana via U.S. mail at 414 Main Street, Hobart, IN 46342 or via telephone at 219-942-2489.

Additional Information for Residents of the Following States

Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies:

- New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>
- New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.