

January 23, 2023

SID BOSE
DIRECT NUMBER: 317-236-2243
Sid.Bose@icemiller.com

CONFIDENTIAL

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

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

Re: Written Notification of a Security Breach

To Whom It May Concern:

On behalf of my client, the Indianapolis Housing Agency, Inc (“IHA”), I am hereby submitting a written notification of a data breach, in compliance with Md. Code Ann. Comm. Law § 14-3504(h).

On October 4, 2022, IHA was experiencing unusual activity within its IT environment and discovered that the IHA was a victim of a ransomware attack. An unauthorized actor had deployed malware to encrypt IHA’s IT systems. IHA promptly engaged additional support services, hired security experts and forensics investigators to help investigate the incident.

IHA notified law enforcement and began taking steps to isolate impacted systems, re-secure its environment, and assess the scope of the incident.

IHA’s investigation and a review of the unauthorized actor’s activities show that the actor was likely targeting IHA’s systems and data in order to disrupt the IHA and force a ransom payment. The investigation did not identify any misuse of personal information to commit or attempt to commit identity theft or fraud.

Upon discovery of the incident, IHA promptly engaged additional support services, hired security experts and forensics investigators to help investigate the incident. IHA also took steps to review all data that could have been impacted in this incident.

While the investigation did not reveal any misuse of personal information to commit or attempt to commit identity theft or fraud, out of an abundance of caution, IHA provided notices to

potentially impacted individuals. IHA also included identity protection services, which includes, credit monitoring, an insurance reimbursement policy, and fully managed identity theft recovery services.

Since the incident, IHA has purchased additional managed security services, deployed additional end-point cybersecurity protections to enhance the security of its environment, and is takings steps to continuously monitor and evaluate its cybersecurity practices to better protect its systems against future attacks.

IHA is notifying **116** Maryland residents. A copy of the notices (which vary slightly in identifying the individuals potentially affected) that will be mailed to the affected Maryland residents on January 23, 2022, is attached herewith. Credit monitoring and identity theft protection services will be offered to the affected Maryland residents for a period of twelve (12) months.

If you require further information about this matter, please contact me by telephone at (317) 236-2243 or via email at sid.bose@icemiller.com.

Sincerely,

ICE MILLER, LLP

Sid Bose

Attachment: Exhibit A Individual Notification Letter (Adult)
Exhibit B Individual Notification Letter (Minor)

EXHIBIT A



Return Mail to IDX:
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-896-7335
Or Visit:
<https://response.idx.us/IHA>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<zip>>

January 23, 2023

<<Notice of Data Breach>>

Dear <<First Name>> <<Last Name>>:

The Indianapolis Housing Agency ("IHA") is sending this letter as part of our commitment to privacy. We are writing to you regarding an incident at IHA which may have involved some of your personal information. We want you to understand what happened, what we are doing about it, the steps you can take to protect yourself, and how we can help you.

What Happened.

On October 4, 2022, IHA was experiencing unusual activity within our IT environment and discovered that the IHA was a victim of a ransomware attack. We promptly engaged additional support services, hired security experts and forensics investigators to help us investigate the incident, and ensure the safety of our environment. We also underwent a review of potentially affected data to determine what personal information may have been involved and identify any potentially impacted individuals.

What Information Was Involved.

Please note that we are providing this information in an abundance of caution, as the investigation could not confirm your personal information was *actually* viewed or misused.

The information that *may* have been involved included your name, address, date of birth, <<Impacted Data>>.

What We Are Doing.

We take the confidentiality, privacy, and security of information in our care seriously. We recognize that incidents like this continue to affect large and small organizations throughout the country. We have addressed this matter as thoroughly and expeditiously as possible by conducting a comprehensive investigation into the incident. Since the incident, we have deployed additional cybersecurity measures to enhance the security of our network, and we will be continuously evaluating and evolving our current and future cybersecurity practices to better protect our systems against future attacks.

We are also providing you with services available through IDX, an identity protection services provider. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do.

While we have no reason to believe that any of your information has been or will be misused and the investigation has not revealed any attempts at fraud or identity theft, out of an abundance of caution, we are providing you with <<12/24>> months of credit monitoring and identity protection services through IDX at no cost to you. A description of the services and instructions on how to enroll can be found below. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-896-7335 or going to <https://response.idx.us/IHA> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. The deadline to enroll is April 23, 2023.

We also encourage you to, as always, remain vigilant and monitor your account statements, financial transactions, and free credit reports for potential fraud and identity theft, and promptly report any concerns. We suggest you regularly review bills, notices, and statements, and promptly report any questionable or suspicious activity.

For More Information.

If you have questions about this letter, please call 1-833-896-7335 toll-free Monday through Friday from 9 am □ 9 pm Eastern Time or go to <https://response.idx.us/IHA>. The toll-free number and website have been created to answer your questions about the incident and to help you enroll in identity theft and credit monitoring services.

We value your trust in the IHA and we regret any inconvenience this matter may have caused you.

Sincerely,

Indianapolis Housing Agency



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to <https://response.idx.us/IHA> 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 1-833-896-7335 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

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

EXHIBIT B



Return Mail to IDX:
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-896-7335

Or Visit:

<https://response.idx.us/IHA>

Enrollment Code: <<Enrollment Code>>

To the Parent or Guardian of

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

January 23, 2023

<<Notice of Data Breach>>

Dear Parent or Guardian of <<First Name>> <<Last Name>>:

The Indianapolis Housing Agency (“IHA”) is sending this letter as part of our commitment to privacy. We are writing to you regarding an incident at IHA which may have involved some of the personal information of your child. We want you to understand what happened, what we are doing about it, the steps you can take to protect your child, and how we can help you.

What Happened.

On October 4, 2022, IHA was experiencing unusual activity within our IT environment and discovered that the IHA was a victim of a ransomware attack. We promptly engaged additional support services, hired security experts and forensics investigators to help us investigate the incident, and ensure the safety of our environment. We also underwent a review of potentially affected data to determine what personal information may have been involved and identify any potentially impacted individuals.

What Information Was Involved.

Please note that we are providing this information in an abundance of caution, as the investigation could not confirm your child’s personal information was *actually* viewed or misused.

The information that *may* have been involved included your child’s name, address, date of birth, <<Impacted Data>>.

What We Are Doing.

We take the confidentiality, privacy, and security of information in our care seriously. We recognize that incidents like this continue to affect large and small organizations throughout the country. We have addressed this matter as thoroughly

and expeditiously as possible by conducting a comprehensive investigation into the incident. Since the incident, we have deployed additional cybersecurity measures to enhance the security of our network, and we will be continuously evaluating and evolving our current and future cybersecurity practices to better protect our systems against future attacks.

We are also providing your child with services available through IDX, an identity protection services provider. IDX identity protection services include: <<12/24>> months of CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help resolve issues if your child's identity is compromised.

What You Can Do.

While we have no reason to believe that any of your child's information has been or will be misused and the investigation has not revealed any attempts at fraud or identity theft, out of an abundance of caution, we are providing your child with <<12/24>> months of identity protection services through IDX at no cost to you. A description of the services and instructions on how to enroll can be found below. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll your child in these services on your behalf.

We encourage you to contact IDX with any questions and to enroll your child in the free identity protection services by calling 1-833-896-7335 or going to <https://response.idx.us/IHA> 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 April 23, 2023.

We also encourage you to, as always, remain vigilant and monitor account statements, and financial transactions for potential fraud and identity theft, and promptly report any concerns. We suggest you regularly review bills, notices, and statements, and promptly report any questionable or suspicious activity.

For More Information.

If you have questions about this letter, please call 1-833-896-7335 toll-free Monday through Friday from 9 am - 9 pm Eastern Time or go to <https://response.idx.us/IHA>. The toll-free number and website have been created to answer your questions about the incident and to help you enroll in identity theft and credit monitoring services.

We value your trust in the IHA and we regret any inconvenience this matter may have caused you.

Sincerely,

Indianapolis Housing Agency



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to <https://response.idx.us/IHA> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at 1-833-896-7335 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's credit identity.

3. Watch for Suspicious Activity. 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 on behalf of your child 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 your child has 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.

4. Security Freeze. You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below 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 child's credit files.

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

5. 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: 1-877-877-939

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