



September 5, 2023

VIA email to idtheft@oag.state.md.us
Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

RE: Corvias Security Incident

Dear Sir/Madam:

I am writing to notify you that Corvias determined that it suffered a security incident resulting in the potential unauthorized access to a limited amount of personal information on 29 Maryland residents.

On December 13, 2023, we identified some suspicious activity in our email environment. We promptly began working with cybersecurity experts to investigate and subsequently determined that an unauthorized third party gained access to a limited number of email accounts between the dates of December 9th and December 13th. Once we identified the data that may have been affected, we immediately engaged a data-review firm to determine what personal information, if any, was in those files. Since receiving the results of the data-review, we have been working diligently with legal counsel to assess our notification obligations and gather addresses for affected individuals.

Having reviewed the data, we have reason to believe that an unknown third party potentially accessed the personal information of 29 Maryland residents, whom Corvias is notifying pursuant to state law. The unknown third party may have accessed files containing some combination of: full names, contact information, date of birth, government identification (such as a driver's license or Social Security number) and financial information (such as bank account or credit card number). At this time, we have no reason to believe the information was, or will be, misused.

We began notifying the affected individuals on September 6th, and we have attached templates of those notification letters. We are offering a free subscription to credit monitoring to those affected individuals. In addition to providing notice, we have taken a variety of measures to bolster our security. For example, we provided additional employee training with increased phishing awareness testing, amended policies and procedures, increased information security personnel, and adopted additional technical safeguards.

If you have questions or need additional information regarding this incident, please contact Jonathan Wilson at jlwilson@shb.com or 202-662-4863.

Sincerely,

A handwritten signature in black ink, appearing to read "SK", followed by a horizontal line.

Shane Kilgore
Vice President, Information Technology

To the Parent or Guardian of:



September 6, 2023

NOTICE OF DATA BREACH

Dear Parent or Legal Guardian of 

We are writing to inform you about an incident that may have exposed your child's personal information to unauthorized persons. While we regret that this incident occurred, we have no evidence to suggest that any of your child's personal information has been misused. However, we are notifying impacted individuals and providing them with an opportunity to enroll in free credit monitoring.

WHAT HAPPENED

On December 13, 2022, we identified some suspicious activity in our email environment. We promptly began working with cybersecurity experts to investigate and subsequently determined that an unauthorized third party gained access to one of our employee's work accounts between the dates of December 9th and December 13th. We did not find any evidence that indicates that any emails or attachments were exported from the user's email account, but we have not been able to confirm whether the files that contained personal information were actually accessed or viewed by the third party. Therefore we cannot say that any of your child's information in those files was actually accessed or viewed. Nevertheless, in an abundance of caution, we are providing this notice to alert you to the potential that your child's information was potentially impacted by this incident.

WHAT INFORMATION WAS INVOLVED

Our investigation determined that affected files may include information such as your child's name, date of birth, and Social Security number. But, importantly, we do not have confirmation that the third party actually viewed/downloaded the emails containing that data or that the affected information will be (or has been) misused.

WHAT WE ARE DOING

We hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to protect your information. This notice was not delayed by a law enforcement investigation.



WHAT YOU CAN DO

Activate your child's complimentary credit monitoring – To help protect your child from fraud or identity theft, we are offering a complimentary two-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your child's personal information. To register, please:

- Ensure that you **enroll by: 11/29/2023** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/minorplus>
- Provide your **activation code:** [REDACTED]
- Provide your child's information when prompted

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **11/29/2023** and provide them with the engagement number [REDACTED].

Remain vigilant – Review your child's account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/.

- You should confirm that your child's credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your child's credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your child's credit file – Consumer reporting agencies have tools you can use to protect your child's credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending your child credit that they should take special precautions to verify your child's identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.
- A security freeze is a more dramatic step that will prevent others from accessing your child's credit report, which will prevent them from extending your child credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe your child is the victim of identity theft, consider notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting your child from fraud or identity theft. For any services not described above, please be aware that the consumer reporting agencies may charge you a fee.

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

For Maryland Residents: the Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at (866) 985-2494 and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in black ink, appearing to read 'SK', followed by a long horizontal flourish line.

Shane Kilgore
Vice President, Information Technology
310 Metro Center Boulevard, Suite 204
Warwick, RI 02886

CORV-MNR-2YR

September 6, 2023

NOTICE OF DATA BREACHDear 

We are writing to inform you about an incident that may have exposed your personal information to unauthorized persons. While we regret that this incident occurred, we have no evidence to suggest that any of your personal information has been misused. However, we are notifying impacted individuals and providing them with an opportunity to enroll in free credit monitoring.

WHAT HAPPENED

On December 13, 2022, we identified some suspicious activity in our email environment. We promptly began working with cybersecurity experts to investigate and subsequently determined that an unauthorized third party gained access to one of our employee's work accounts between the dates of December 9th and December 13th. We did not find any evidence that indicates that any emails or attachments were exported from the user's email account, but we have not been able to confirm whether the files that contained personal information were actually accessed or viewed by the third party. Therefore we cannot say that any of your information in those files was actually accessed or viewed. Nevertheless, in an abundance of caution, we are providing this notice to alert you to the potential that your information was potentially impacted by this incident.

WHAT INFORMATION WAS INVOLVED

Our investigation determined that affected files may include information such as your name, date of birth, government identification (such as Social Security, Passport, or driver's license number), and financial information (such as your bank account or credit card number). But, importantly, we do not have confirmation that the third party actually viewed/downloaded the emails containing that data or that the affected information will be (or has been) misused.

WHAT WE ARE DOING

We hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to protect your information. This notice was not delayed by a law enforcement investigation.



WHAT YOU CAN DO

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: 11/29/2023** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** [REDACTED]

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **11/29/2023** and provide them with the engagement number [REDACTED].

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft. For any services not described above, please be aware that the consumer reporting agencies may charge you a fee.

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

For Maryland Residents: the Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents: the North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; www.ag.ny.gov.

For Washington, D.C. Residents: the District of Columbia Attorney General may be contacted at: Office of the Attorney General, 400 6th Street, NW, Washington, D.C. 20001; (202) 727-3400; <https://oag.dc.gov/>.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 17 Rhode Island residents impacted by this incident.

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at (866) 985-2494 and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in black ink, appearing to read 'SK', followed by a horizontal line.

Shane Kilgore
Vice President, Information Technology
310 Metro Center Boulevard, Suite 204
Warwick, RI 02886

