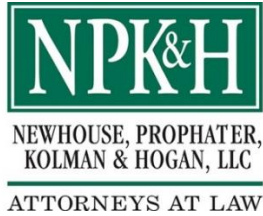


D. Wesley Newhouse
William H. Prophater, Jr.
Michael S. Kolman
Christopher E. Hogan
Amy E. Kuhlman



Of Counsel:
Philip R. Moots

Writer's Direct Contact:
(614) 827-0901
wnewhouse@npkhlaw.com

August 17, 2023

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

Via e-mail only at:
idtheft@oag.state.md.us

RE: Notification of Maryland residents of data breach at the Ohio Historical Society.

To Whom it May Concern;

On July 9, 2023, cyber criminals gained access to and encrypted data stored on the internal servers at the Ohio Historical Society. OHS employed various IT forensic consultants and other IT professionals to assess the extent of the breach, and to identify those whose information may have been accessed. The cyber criminals demanded payment of ransom that OHS, a not-for-profit organization, could not pay. OHS did offer payment of a considerably lesser sum, but the cyber criminals rejected the offer. Some information was recently released to the public.

We serve as general counsel for OHS. Its address and telephone number are:

Ohio Historical Society, dba Ohio History Connection
800 E. 17th Ave.
Columbus, Ohio 43211
(614) 297-2300

Some of OHS's donors reside in Maryland. The cyber criminals gained access to names and checking account numbers of some of OHS's donors. Because these individuals are at risk of breach of personal information, we believe that OHS is required to provide them with notice. OHS is going to notify the three national credit reporting agencies, and will offer credit monitoring and identity restoration services.

OHS has worked with its internal IT staff and its IT consultants and vendors to restore its data and systems, and to upgrade its systems to make them less vulnerable to such attacks.

Thirty (30) persons with addresses in Maryland were among those whose data may have been accessed. Like Maryland, Ohio requires that OHS provide notification of the breach to

those who may be affected within 45 days of the discovery of the breach. As a result, OHS intends to send notification substantially in the form that is attached on August 23, 2023.

Please contact me if you need further information.

Very truly yours,
**NEWHOUSE, PROPHATER, KOLMAN
& HOGAN, LLC**

/s/ D. Wesley Newhouse

D. Wesley Newhouse

August 23, 2023

Name
Mailing address
City, State ZIP

Re: NOTICE OF DATA BREACH

Dear _____,

We are writing to let you know of a data security breach involving Ohio History Connection's (OHC) computer systems and databases. Because this breach has possibly exposed personally identifiable information, we wanted to inform you as soon as possible of steps to protect your identity.

What happened?

In early July, cybercriminals executed a ransomware attack upon internal data servers at OHC, effectively encrypting and holding our data hostage. The group also demanded that OHC pay a ransom in the millions of dollars in order to avoid the release of the data to the public. OHC was unable to afford the demanded amount but made an offer to the cybercriminals to prevent the release of the data. The cybercriminals rejected the offer. Your personal information may now be accessible to those who may be looking for it.

How did this happen?

In most cases, ransomware is spread through phishing emails that contain malicious attachments or through a user unknowingly visiting an infected website, automatically downloading and installing malware without the user's knowledge.

What information was involved and who was impacted?

Names, addresses, and Social Security numbers of current and former OHC employees (from 2009 to 2023) could have been accessed. No credit card information was accessed or stolen as part of this breach. However, cybercriminals may have gained access to W-9 reports and other records revealing the names and personal Social Security numbers of vendors who contracted to provide services to OHC. They also may have gained access to images of checks provided to OHC by some members and donors beginning in 2020. In total, the information of 7,600 individuals has potentially been exposed.

What we are doing to prevent this from happening again?

OHC has notified the FBI and retained forensic IT consulting firms to assist in determining the extent of the data breach, reconstructing its systems and restoring data. OHC also employed a consultant that

specializes in communicating with groups who engage in cybercriminal activity to determine the amount the group was demanding and assess the extent of the data actually accessed, encrypted and released.

In restoring its data and systems, OHC has moved a vast majority of its data to cloud-based services, and has implemented new security systems, features and measures intended to reduce its vulnerability to future attacks and ensure no personally identifiable information is ever accessed again.

What you can do?

OHC is providing **free credit monitoring services for one year** for anyone involved. **Sign up at [this link](#):** OHC has also notified all three national credit reporting agencies. Any questions can be directed to [800-_____](#).

Beyond signing up, we also recommend that you remain vigilant and promptly report any suspicious activity or suspected identity theft to [IDX \[link\] or \(800\) _____](#). Such activity should also be reported to the proper law enforcement authorities, your credit card providers, and your financial institutions.

Please also be wary of solicitations from those who may call you and offer their services. Do not give your personal information to anyone who requests it (online or over the phone) under the guise of helping you protect your personal information.

A complete list of state attorneys general is included in this notification. Here is contact information for the Federal Trade Commission and your state's attorney general:

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580
www.ftc.gov
(202) 362-2222

Ohio Attorney General
30 East Broad Street
Columbus, Ohio 43215
www.ohioattorneygeneral.gov
(800) 282-0515

You can also contact the Privacy Rights Clearinghouse www.privacyrights.org.

Further, if you suspect that your identity has been stolen or that your personal information is being used, you should contact the national credit reporting agencies:

Equifax Credit Information Services, LLC
PO Box 740241
Atlanta, GA 30374
www.equifax.com
(800) 525-6285

TransUnion Consumer Relations
PO Box 2000
Chester, PA 19016-2000
www.transunion.com
(800) 680-7289

Experian National Consumer Assistance
PO Box 4500
Allen, TX
www.experian.com

(888) 397-3742

You can have the credit reporting agencies place a hold on the provision of your credit information, and can obtain from them a report on your credit. You are entitled to receive one free credit report from each of the three national credit reporting agencies once per year. To request a copy of your free credit report, visit www.annualcreditreport.com or call (877) 322-8228.

How can I learn more?

Should you have further questions or concerns regarding this matter or the protections available to you, again, please contact IDX at [link] or call (800)_____.

We sincerely apologize for this incident and regret all the inconvenience it causes you. Please know we greatly your past and future support of the Ohio History Connection.

Thank you.

Charles R. Moses

President, Board of Trustees
Ohio History Connection