



May 25, 2022

VIA EMAIL TO:
idtheft@oag.state.md.us

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

RE: Data Breach Notification

In accordance with the Personal Information Protection Act (PIPA), Md. Code Ann. Comm. Law 14-3504, please accept the following as our notification to the State of Maryland of a data breach on our corporate network. The incident is currently the subject of an ongoing third-party forensic investigation; however, at this time we have identified 16 potentially affected Maryland residents, all former employees.

1) Breach Description

On 25 April 2022 at approximately 08:00 CT, Scott Nicholson, CISO, Exhibit Arts, LLC (EA), was notified by the company's MSP of suspicious activity on the corporate network. The activity was flagged in Sentinel One (S1) End Point Detection and Response (EDR). The first alert in S1 was triggered on 23 April 2022 at 19:20 UTC with the last known activity terminating on 24 April 2022 at 02:54 UTC. Upon notification, by our MSP all internet connectivity and network assets were shut down. The company engaged with a third-party Digital Forensics and Incident Response (DFIR) firm to conduct the investigation

The cause of the breach is currently the subject of an ongoing investigation; however, current evidence indicates the threat actor (TA) performed file-level encryption with the extension ".Nokowaya". We have determined that the ransomware group used PowerShell encoded commands, Advanced IP Scanner used, and FileZilla installed. A possible payload "UN_A_.exe" but the sample is not available currently.

2) Number of Maryland residents being notified: 16

A sample of the notification being made to the affected parties, including offers of free credit monitoring, is attached. Notification to affected individuals is being handled by a third-party firm, IDX, on behalf of the company. Credit monitoring is being offered. See attached notification letter.

3) Potentially compromised information of Maryland residents is IRS W-2s.

4) To further secure the company's network and data, after forensic images and device data collection, all HD/SSDs on company workstations were removed and replaced with new (out-of-the-box) SSDs, clean OS, and application installs. All servers, after forensic images and collection, were wiped clean and recovered from known off-domain backups. All devices were

rescanned for malware and S1 and Duo Access multifactor authentication was reinstalled on all workstations and servers.

Subsequently, we have replaced S1 with CrowdStrike EDR and monitoring/IR by a third-party Security Operations Center.

If I may be of further assistance, my contact information is as follows:

326 N. Athenian Ave,
Wichita, KS 67203
316-264-2915 x21,
316-880-8809 (cell)
scott@exhibitarts.net

Sincerely,

A handwritten signature in blue ink, appearing to read "Scott P. Nicholson", with a long horizontal line extending to the right.

Scott P. Nicholson, MSM, CAP
Chief Information Security Officer

Logo
C/O IDX
<<Return Address>>
<<City>>, <<State>> <<Zip>>

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

<<Date>>

To Enroll, Please Call: [TFN] Or Visit: https://response.idx.us/customending https://app.idx.us/account-creation/protect Enrollment Code: [XXXXXXXXXX]
--

Notice of Data Breach

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

What Happened

On May 6, 2022, Exhibit Arts, Inc. ("EA" or the "Company") determined that a ransomware attack may have compromised some of your personal information. Upon learning of the data breach, the Company immediately contained the breach and initiated a forensic investigation. The Company also reported the data breach to the Federal Bureau of Investigation and the Maryland Office of the Attorney General >> for investigation and handling.

We understand and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that involved your personal information.

What Information Was Involved

Although the investigation is still ongoing, EA has learned that the attack may have compromised your W-2 and paystub information, which, in particular, may contain your social security numbers and financial account numbers.

What We Are Doing

EA values your privacy and deeply regrets that this incident occurred. We will continue to monitor if there are any significant developments, but at this time, we can assure you that the inadvertent disclosure has been contained. The Company will continue to implement strict security measures designed to prevent a recurrence of such an incident and to protect the privacy of our valued employees, applicants, and customers/clients.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 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 [TFN] or going to <https://response.idx.us/customending> / <https://app.idx.us/account-creation/protect> 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 [Enrollment Deadline]. Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of the credit monitoring services offering.

Also, please review the attachment to this letter (**Steps to Help Protect Your Information**) for further information on steps you can take to protect your information.

For More Information

Should you have any questions or concerns about the loss of your personal information, you may reach EA's Human Resource Director, Pam Adams, via telephone at 316-264-2915 or via email at Pam@exhibitarts.net.

Sincerely,

Elizabeth Harshfield
President
Exhibit Arts, Inc.

Enclosure:

1. **Steps to Help Protect Your Information**



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to <https://response.idx.us/customending/> <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 **[TFN]** 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 detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Also, if you discover any suspicious activity on your account 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. Additional Information. You can obtain additional information about the steps you can take to avoid identity theft from the following state and federal agencies. The FTC 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 website at www.oag.ca.gov/privacy for additional information on protection against identity theft.
- ☐ **District of Columbia:** Mail: District of Columbia Office of the Attorney General, 441 4th Street, NW., Washington, DC 20001; Telephone: (202) 442-9828; and Email: databreach@dc.gov.
- ☐ **Florida:** Visit the Florida Office of Attorney General Website at <http://myfloridalegal.com/pages.nsf/Main/53D4216591361BCD85257F77004BE16C> for additional information on protection against identity theft.
- ☐ **Iowa:** Mail: Iowa Office of the Attorney General, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106; Telephone: 888-777-4590; and Website: <https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information>
- ☐ **Kansas:** Mail: Kansas Office of the Attorney General, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, Telephone: (800) 908-4490; Website: <https://ag.ks.gov/in-your-corner-kansas/your-identity/what-is-identity-theft->
- ☐ **Maryland Residents:** Mail: Maryland Office of the Attorney General, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202; Telephone: 1-888-743-0023; and Website: www.oag.state.md.us/Consumer.
- ☐ **Missouri:** Visit the Missouri Office of Attorney General Website at <https://ago.mo.gov/civil-division/consumer/identity-theft-data-security/data-breaches> information on protection against identity theft.
- ☐ **Nebraska:** Visit the Nebraska Office of Attorney General Website at <https://protectthegoodlife.nebraska.gov/> for additional information on protection against identity theft.
- ☐ **Nevada:** Visit the Nevada Office of Attorney General Website at https://ag.nv.gov/Hot_Topics/Victims/IDTheft_Protect/ for additional information on protection against identity theft.
- ☐ **New Jersey Residents:** Visit the New Jersey State Police in the Department of Law and Public Safety website at <https://nj.gov/njsp/tech/identity.html> for additional information on protection against identity theft.
- ☐ **Texas:** Visit the Texas Office of Attorney General Website at <https://www.texasattorneygeneral.gov/consumer-protection/identity-theft> for additional information on protection against identity theft.
- ☐ **Virginia:** Visit the Virginia Office of Attorney General Website at <https://www.oag.state.va.us/programs-initiatives/identity-theft> for additional information on protection against identity theft.
- ☐ **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.