XPAN Law Partners
4 N. Maple Avenue
Marlton, New Jersey 08053

February 15, 2024

VIA Email
NH Department of Justice

Consumer Protection and Antitrust Bureau
1 Granite Place South
Concord, New Hampshire 03301

Re: **International Center of Photography Personal Data Breach**

Dear :

On behalf of my client, the International Center of Photography ("ICP"), enclosed herein please find:

- Data Breach Notification for ICP; and
- Sample Breach Notification Letter to Affected Individuals.

Should you require any additional information, please do not hesitate to contact me.

Respectfully Submitted,

/s/ Rebecca L. Rakoski
Rebecca L. Rakoski, Esquire
Managing Partner
Counsel for the International Center of Photography

Data Breach Notification

Name of Entity	International Center of Photography
Address of Entity	79 Essex St, New York, NY 10002
Contact Person	Rebecca L. Rakoski, Esquire
Function of Contact Person	Attorney
Postal Address of Contact Person	XPAN Law Partners 4 N. Maple Avenue Marlton, New Jersey 08053
Email Address of Contact Person	
Phone Number of Contact Person	
Type of Breach	Ransomware
Became Aware of Ransomware	February 16, 2023
Date Determined a Legal Breach Occurred	December 15, 2023
Type of Data Potentially Impacted	
Impact to Data Subjects	Exposure of personal information.

Credit Monitoring	None
Number of Data Subject Impacted	2 data subjects in New Hampshire.
Notification to Data Subjects	ICP intends to notify data subjects impacted by data breach before the end of February, 2024.
Mitigation Efforts	ICP has engaged forensic experts and legal professionals to conduct a thorough investigation of the potential data impacted and is in the process of identifying the categories of data to inform the data subject. Additionally, ICP has engaged forensic experts to upgrade and make changes to its network infrastructure. There were multiple steps taken to secure the environment and reduce the risk of subsequent incidents. The entire Active Directory structure was completely rebuilt on new servers. All of the workstations were fully wiped before being connected to the new Active Directory. All workstations and servers now have Cylance EDR and Infocyte installed. These systems are monitored by a 24/7/365 SOC for security alerts. All systems have been enrolled in a patch management system to ensure updates are installed. An offsite backup system has been implemented for core servers. The new Domain Controllers have had their Kerberos passwords rotated. The network has been reconfigured with multiple VLANs and ACLs preventing access between systems. Public facing systems have been placed in a DMZ with ACLs limiting network access between systems. No domain

	joined systems are exposed to public access. Use of VPN was discontinued. The Microsoft 365 environment was disconnected from the legacy Active Directory environment. MFA policies are enforced using Conditional Access rules in Azure Active Directory. All full time employees are required to use MFA for access. Geo-IP blocks were put in place to limit logins to specific countries (North America and the EU) for all accounts. Users who are known to reside outside of these locations were given specific policies to allow access from their home locations. We are in the process of enforcing MFA on all education staff as well. All passwords were forced to reset, and the Azure AD Password Protection policy was enabled. SaaS Alerts has been configured and connected to Microsoft 365 to monitor and record system access. The SaaS Alerts system is monitored 24/7/365 by a SOC. Alerts have been configured on creation of mail forwarding rules as well as other signs of compromise. Access to PowerShell was limited to only Administrative users. We are in the process of implementing additional security measures including a vulnerability management system, regular external vulnerability scans, upgraded firewalls with East/West DPI scanning and upgraded servers with additional backup components.
Description of Data Breach	The International Center of Photography ("ICP"), a New York not-for-profit school and museum, located at 79 Essex St, New York, NY 10002 became aware of a ransomware incident on February 16, 2023 ("Incident").

	ICP engaged an information technology (IT) provider and a MSSP to address the Incident and determine the extent of the information compromised. ICP did not pay the threat actor, but instead was able to restore some information from a 2019 backup. However, due to the fact that log data was not available ICP was unable to determine the nature and extent of the exfiltration. Accordingly ICP has engaged legal counsel and a cyber forensic company to further investigate the Incident.
Additional Facts Related to Investigation	Cyber forensics reviewed whatever logging was available to determine if there was any forensic evidence of the Incident. Unfortunately, since there were no logging sources present that could be utilized to determine how the initial compromise occurred or what data was exfiltrated, cyber forensics was not able to determine which of the restored files were part of the threat actor's data exfiltration. Cyber forensics reviewed the blog of the threat actor group, Medusa, to view the sample set of data. During the review, it was observed that a sample of confirmed ICP files were posted online for sale. Based on that information cyber forensics was able to target certain files that were likely subject to the ransomware Incident. Unfortunately, without necessary logs, it took time to determine the potential data impacted. Once cyber forensics was able to obtain potential impacted data ("data"), ICP again encountered issues as it is a small non-profit with limited resources and did not have insurance coverage for the Incident. Using the data set, cyber forensics also encountered significant difficulty in determining whether

	the data was personal information due to: (i) the dissociated nature of the impacted data; (ii) imprecise or inaccurate labeling of records; (iii) the diverse geography of the affected population; and (iv) a significant amount of data in multiple foreign languages. Further, it took time to determine where the data subjects are located given that ICP is a school; many individuals are associated with two (2) or more addresses, including some local to ICP in the United States (which may have been temporary during their education) and others from various international jurisdictions.

[Vendor Return Address]

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>> <<Date>>
<<City>>, <<State>> <<Zip>>
<<Country>>

NOTICE OF DATA BREACH

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

The International Center of Photography ("ICP") is writing to inform you of a recent event that may impact the privacy of some of your information. While we have no indication of any identity theft or fraud occurring as a result of this incident, we are providing you information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On February 16, 2023, ICP became aware of suspicious activity involving our computer network. We launched an investigation into the nature and scope of the incident with the assistance of industry-leading cybersecurity specialists. Through the investigation, we learned that an unauthorized individual accessed our network and that files containing your information may have been viewed and/or taken by the unauthorized individual.

With third-party support, we then conducted a comprehensive review of the impacted files in order to determine what information was affected and to whom the information related. Upon completion of the third-party review, we then conducted a manual review of our records internally to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. On or around December 15, 2023, we completed our review.

What Information Was Involved? The investigation determined that the following types of information related to you could potentially be involved: [redacted]

What We Are Doing. Upon discovering this incident, we moved quickly to investigate and respond, assess the security of relevant ICP systems, and identify any impacted data. As part of our ongoing commitment to the security of information, we are evaluating opportunities to improve security and to better prevent future events of this kind.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, and to review your account statements, explanation of benefits forms, and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Personal Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. Should you have any questions, you may contact us at ###-###-###, which can be reached Monday through Friday from X:00 a.m. to X:00 p.m. Eastern Time.

Sincerely,

_____

Steps You Can Take to Help Protect Your Personal Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances

of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. U.S. Vision, Inc. is located at 1 Harmon Drive, Blackwood, NJ 08012

For 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 bureaus 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 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. We encourage you to 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.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 [#] Rhode Island residents impacted by this incident.

For Massachusetts residents, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.