AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FLOOR
NEW YORK, NY 10004-2400
WWW.ACLU.ORG

July 19, 2023

Via Email: DOJ-cpb@doj.nh.gov

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

RE: Notice of Security Incident

Dear Attorney General Formella:

I write on behalf of the American Civil Liberties Union Foundation, Inc. ("ACLUF") pursuant to N.H. Rev. Stat.§§ 359-C:20 to inform you of a data security incident suffered by one of our third-party sub-vendors that appears to have involved the
of eleven New Hampshire residents.

Description of Incident

On June 22, 2023, ACLUF was notified by TIAA Kaspick, the third-party service provider that administers our life income gifts program, about a data security incident experienced by one of its vendors involved in this program, Pension Benefit Information, LLC ("PBI"). We are a client of TIAA Kaspick, not PBI, and are not privy to all details of the incident or results of PBI's investigation, nor do we have all of the details TIAA Kaspick has from its own internal assessment. But we have compiled this summary based on information we have received from TIAA Kaspick, including information provided by PBI:

On or about May 31, 2023, the company that provides MOVEit Transfer software –a file transfer software used by thousands of organizations around the globe, including PBI – announced that an unauthorized third party had identified and exploited a vulnerability in the MOVEit software to access data. Upon learning of the MOVEit vulnerability, PBI launched its own investigation – with the assistance of cybersecurity experts – to understand if personal information in PBI's possession had been compromised. PBI determined that the unauthorized third party had in fact accessed one of PBI's MOVEit servers on May 29-30, 2023, and downloaded data. PBI alerted law enforcement and conducted further review to identify the specific individuals and data from PBI's system that was involved. PBI installed software patches released by the MOVEit software provider to close the vulnerability and, on June 19, informed our service provider, TIAA Kaspick, which of its files had been compromised. After activating its incident response team and reconciling PBI's information with its own records, TIAA Kaspick notified ACLUF and confirmed that the data obtained by the unauthorized third party included the

of donors and beneficiaries of the ACLUF life income gift program that TIAA Kaspick administers for us.

Measures taken to prevent a recurrence

Since learning of this incident on June 22, 2023, ACLU has worked closely with TIAA Kaspick to ensure that all necessary steps were being taken by PBI and/or TIAA Kaspick to investigate the incident, prevent future incidents involving ACLUF supporters' information, and to help us identify and notify affected donors and beneficiaries directly.

PBI has informed us that they have patched servers, assessed the security of their systems and are reviewing and enhancing their information security practices and procedures. In addition, ACLU Foundation and TIAA Kaspick have each reviewed our own systems and determined that they are not impacted by the MOVEit vulnerability. ACLUF will continue to assess and update our security practices in order to help prevent this type of incident from occurring again.

On July 21, 2023, we are sending notifications to affected individuals. A copy of the notification letter is attached.

The ACLU remains committed to ensuring the security and privacy of its constituents' information.

If you have questions or concerns that are not addressed in this notice letter please feel free to call me at .

Sincerely,

Elizabeth Bradford
Co-Chief Corporate Counsel

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FLOOR
NEW YORK, NY 10004-2400
WWW.ACLU.ORG

July 21, 2023

<<FirstName>> <<Middle Initial>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Re: NOTICE OF DATA SECURITY INCIDENT

Dear <<FirstName>> <<Middle Initial>> <<LastName>>,

We are writing to inform you about a data security incident involving your personal information. On June 22, 2023, the ACLU Foundation ("ACLUF" or the "Foundation") was notified by TIAA Kaspick, LLC ("TIAA Kaspick"), the third-party service provider that administers our life income gifts program, about a data security incident experienced by one of its vendors involved in this program, Pension Benefit Information, LLC ("PBI"). Specifically, PBI provides audit and address research services to TIAA Kaspick related to donors and beneficiaries in our planned giving program.

During that incident, personal information associated with donors and beneficiaries of ACLUF charitable gift annuities and other life income gifts, such as charitable remainder trusts. was obtained by an unauthorized third party. TIAA Kaspick has confirmed that, unfortunately, this included information about you, including .

PBI has communicated to and through TIAA Kaspick that they currently have no indication of data obtained by the unauthorized third party in this incident being used to commit identity theft or fraud. But ACLUF is taking this matter very seriously and providing this notice to you to explain what happened and how you can protect yourself going forward.

We describe below what happened, what information was involved, and what has been and continues to be done to address this matter. We also outline what steps TIAA Kaspick and the ACLUF will undertake to safeguard your privacy, as well as what steps you may wish to take in response.

What Happened

We are a client of TIAA Kaspick, not PBI, and are not privy to all details of the incident or results of PBI's investigation, nor do we have all of the details TIAA Kaspick has from its own internal assessment. But we have been working closely with TIAA Kaspick to understand the incident, information involved, and the efforts made to contain it. We have compiled the information in this letter based on information we have received from TIAA Kaspick, including information from PBI, over the course of numerous communications since we were notified. On or about May 31, 2023, the company that provides MOVEit Transfer software – a file transfer software used by thousands

of organizations around the globe, including PBI, to securely transfer files – announced that an unauthorized third party had identified and exploited a vulnerability in the MOVEit software to access data. As reported in the press, the MOVEit incident impacted hundreds of organizational users, which, in addition to PBI, include federal and state government agencies, financial services firms, pension funds, and many other types of companies and non-profit organizations. Upon learning of the MOVEit vulnerability, PBI promptly launched its own investigation – with the assistance of cybersecurity experts – to understand if personal information in their possession had been compromised. They determined that the unauthorized third party had in fact accessed one of PBI's MOVEit servers on May 29, 2023 and May 30, 2023, and downloaded data. PBI alerted law enforcement and conducted further review to identify the specific individuals and data from PBI's system that was involved. On June 2, 2023, PBI installed software patches released by the MOVEit software provider to close the vulnerability.

On June 19, 2023, PBI confirmed to TIAA Kaspick which of their files had been compromised. TIAA Kaspick quickly activated its incident response team with its parent company, TIAA, and reconciled the PBI information with its own records before notifying ACLUF on June 22, 2023 that 575 donors and beneficiaries of the ACLUF life income gift program that TIAA Kaspick administers were affected. TIAA Kaspick has confirmed that your personal information was on the PBI server compromised by the unauthorized third party.

We understand from TIAA Kaspick and PBI that (i) in addition to this notice, you can expect to, or may have already received, notification directly from PBI with details regarding this same incident; and (ii) as noted above, at this time, PBI has no indication that any data that was accessed from their server (including yours) has been used for identity theft or other fraudulent activity.

What Information Was Involved

The investigation has concluded that the personal information on the affected PBI server includes . TIAA Kaspick has advised us that no other information about your gift or your planned gift relationship with ACLUF, including information about the bank account(s) to which your periodic payments are made, was exposed. To be clear, no data or systems that ACLUF or our service provider, TIAA Kaspick, directly maintains or controls were accessed or compromised as a result of this incident.

What We Are Doing

We take the privacy and security of your personal information very seriously. Since learning of this incident on June 22, 2023, we have been working closely with TIAA Kaspick to ensure that all necessary steps were being taken by PBI and/or TIAA Kaspick to investigate the incident, prevent future incidents involving ACLUF supporters' information, and to help us identify and notify affected donors and beneficiaries directly. In addition, ACLU Foundation and TIAA Kaspick have each reviewed our own systems and determined that they are not impacted by the MOVEit vulnerability.

ACLUF will continue to assess and update our security practices in order to help prevent this type of incident from occurring again.

Working with TIAA Kaspick, we have confirmed that PBI will be offering to provide you twenty-four (24) months of credit monitoring services at no cost to you. PBI will provide you with instructions to enroll in the free credit monitoring service they are offering to individuals affected by this incident in the notice they sent you directly about this. There is more guidance, including information about legal rights you may have, in Attachment 1 to this letter.

What You Can Do

As always, please be cautious of any unsolicited communications that ask you to provide your personal information electronically and avoid clicking on links or downloading attachments from suspicious emails.

It is a good practice to monitor your accounts and any credit reports you receive for any signs of suspicious activity. As noted above, PBI will arrange for you to obtain of credit monitoring services at no cost to you. Details should be in the notice you receive directly from PBI. Please contact us at the number below if you do not receive that information.

Other guidance, including how to obtain a free credit report, and rights or resources you may have and want to take advantage of, is provided in the enclosed Attachment 1, which we encourage you to review.

For More Information

If you have questions or concerns that are not addressed in this notice letter or want to reach the ACLU Foundation's Planned Giving team for any other reason, please call us between 9:00 AM and 5:00 PM Eastern Time at .

Sincerely,

Terence Dougherty
Deputy Executive Director & General Counsel
American Civil Liberties Union Foundation, Inc.

Mark Wier
Chief Development Officer
American Civil Liberties Union Foundation, Inc.

ATTACHMENT 1
ADDITIONAL INFORMATION

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information
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. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Whether or not you enroll in the credit monitoring product offered, you also have the right to place an initial fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and is placed on a consumer's credit file. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Fraud alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A fraud alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting agencies is:

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Free Credit Report Information
You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself and prevent such activity. If you are a resident of the District of Columbia, Iowa, Maryland, New York, or Oregon, you can also reach out to your respective state's Attorney General's office at the contact information below. All other residents can find information on how to contact your state attorney general at https://www.naag.org/ find-my-ag/.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357) / https://www.consumer.ftc.gov/identity-theft-and-online-security

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392 / https://justice.oregon.gov

New York Attorney General's Office
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/consumer-frauds-bureau/identity-theft

North Carolina Department of Justice
114 West Edenton Street
Raleigh, NC 27603
1-919-716-6400
https://ncdoj.gov/protecting-consumers/identity-theft/

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, DC 20001
1-202-727-3400 / oag.dc.gov

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 / www.marylandattorneygeneral.gov

Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926 / www.iowaattorneygeneral.gov

Security Freeze Information
You have the right to request a free security freeze (aka "credit freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a credit freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A credit freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com/personal/ credit-report-services	www.experian.com/ fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1. Full name, with middle initial and any suffixes;
2. Social Security number;
3. Date of birth (month, day, and year);
4. Current address and previous addresses for the past five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.