



CITY YEAR, INC.

287 Columbus Ave
Boston, MA 02116

PHONE 617.927.2500

cityyear.org

VIA First-Class Mail (Return Receipt Requested), Facsimile, and Electronic Mail

October 7, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
(410) 576-6566 (fax)
idtheft@oag.state.md.us (email)

Re: Notice of Data Breach

To whom it may concern:

City Year, Inc. ("City Year")¹ provides this Notice of Data Breach pursuant to Maryland's Personal Information Protection Act (Md. Code Ann. Comm. Law §§14-3501 et seq.).

Brief description of the nature of the security breach

On September 20, 2022, as part of a routine audit, a City Year employee was reviewing City Year personnel I-9 information. The employee discovered that the I-9 identification information provided to City Year by a City Year AmeriCorps member who serves with City Year's Washington, DC site and who lives in Maryland was erroneously uploaded to another City Year AmeriCorps member's file in Workday (Workday is City Year's internal electronic data management system). In addition to being potentially accessible by the other AmeriCorps member, the erroneously uploaded information was also potentially accessible by the manager of the individual who should not otherwise have had access to the information. City Year's investigation later revealed that the information was erroneously uploaded on August 2, 2022.

¹ City Year is a Massachusetts based 501(c)(3) organization that provides youth development and education support services at 29 sites across the United States, including the District of Columbia. Additional information about City Year may be found at <http://www.cityyear.org>. City Year has employees and separately recruits non-employee participants to provide service through the federal AmeriCorps service program. While AmeriCorps members are not City Year employees, City Year must verify their authorization to work in the United States prior to their service.

What information was compromised

The I-9 identification provided to City Year by an individual (passport, social security number, and citizenship information).

Number of Maryland residents to be notified

One (1)

Steps City Year is taking to restore the integrity of the breached system

City Year has removed the erroneously uploaded information from the AmeriCorps member's file. City Year conducted a 30-day lookback audit to see if any persons who should not be able to access the erroneously uploaded information had actually accessed the information. That audit showed the information had not been viewed by anyone else during the lookback period.

City Year will provide notice of the breach to the affected individual (see draft notice attached) and support them with any identity protection/credit monitoring services they may require. City Year will retrain the individual who erroneously uploaded the information to the wrong file to ensure they understand the importance of handling personally identifiable information securely moving forward.

City Year takes its data protection obligations seriously. City Year will undertake all steps it deems appropriate to remedy this data breach and prevent future such occurrences. Should you need any additional information or should you have any questions, you may contact me using the below contact information.

Sincerely,

Shanuah Beamon

Shanuah Beamon
Executive Vice President and General Counsel
City Year, Inc.
(617) 927-2315
sbeamon@cityyear.org

Enclosure

cc: City Year Security Incident Response Team



Memorandum

To:	[REDACTED]
From:	Ellen Gulachenski (CIO) and Shanuah Beamon (GC)
Subject:	Notification of Data Exposure
Date:	10/7/22
CC:	[REDACTED]

On 09/20/22 the City Year Security Incident Response team (SIRT) was notified of a potential exposure of [City Year Protected Data](#) to an unauthorized party which was found during an audit of on-boarding activities for ACMs. A preliminary investigation indicates that certain of your personally identifiable information (PII) was accidentally exposed. What we have determined thus far is that:

- On August 2, 2022, your passport, driver's license, and Social Security card were loaded into Workday in a manner that accidentally allowed two people at City Year to view the information even though they were not authorized to do so.
- An examination of Workday's audit log confirms that while these individuals had access to the information, for a period of 30 days commencing August 21, 2022, through September 21, 2022, they did not view the PII.
- However, since Workday's audit log does not extend past 30 days, we cannot conclude definitively for the period of August 2, 2022, through August 20, 2022, that your PII was not viewed by these individuals.

In an abundance of caution, we have decided to implement the remediation measures described below.

- We have notified the Maryland Attorney General of the incident, as required by Maryland law.
- We have initiated an audit at your site to verify that no other ACMs' information was incorrectly exposed.
- For information on how to prevent identify theft, the following resources are available to you:
 - The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov
(202) 326-2222 (phone)
1-877-382-4357 (toll-free)
 - The Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
<https://www.marylandattorneygeneral.gov>
(410) 576-6300 (phone)
1-888-743-0023 (toll-free)
idtheft@oag.state.md.us (email)

- Credit monitoring at each of:

Equifax

P.O. Box 740241

Atlanta, GA 30374

www.equifax.com

(888) 378-4329 (phone)

Experian

P.O. Box 4500

Allen, TX 75013

www.experian.com

(888) 397-3742 (phone)

TransUnion

P.O. Box 2000

Chester, PA 19016

www.transunion.com

(888) 909-8872 (phone)

- We will be strengthening your site's training on citizenship documentation processing to ensure this does not occur again.
- Your site Executive Director has been informed of this situation.

City Year is deeply concerned that this mistake occurred and that your information was inadvertently exposed. We take data security seriously and we are using this incident to raise awareness of the necessity for people to be meticulously careful when handling such documentation and information. We apologize that this event has happened. By copy of this memorandum, your Impact Manager and MDI are being notified of this incident so that they can provide additional support to you.