



Richard W. Goldberg
550 E. Swedesford Road, Suite 270
Wayne, PA 19087
Richard.Goldberg@lewisbrisbois.com
Direct: 215.977.4060

November 29, 2022

File No.: 28310.1586

VIA ELECTRONIC MAIL SUBMISSION

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD. 21202
Email: IDtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP (“Lewis Brisbois”) represents Jobs With Justice Education Fund (“JWJEF”) with respect to a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident pursuant to Maryland’s data breach notification statute. (Md. Code Ann. Comm. Law §§ 14-3501-3508).

1. Nature of the Security Incident

On November 9, 2022, JWJEF learned that personal information belonging to its former and current employees along with their dependents may have been involved in an incident. The information may have included first and last names, addresses, date(s) of birth, social security numbers, health care, retirement account, and other benefits enrollment information.

On August 11, 2022, JWJEF discovered that two of its employees had misused the organization’s credit cards resulting in the theft of funds. Upon further investigation, JWJEF also determined that the employees had access to the employment records of others. JWJEF reported the incident to law enforcement and took immediate steps to remove the employees’ access to the network and recover the workstations. In response to the incident, JWJEF engaged independent digital forensics and incident response experts to determine the extent of unauthorized activity in the environment. This included identifying any personal information that may have been accessed or acquired without authorization.

2. Number of Maryland Residents Affected

JWJEF notified 22 Maryland residents of this incident via first class U.S. mail on November 28, 2022. A sample copy of the notification letter is included with this correspondence.

3. Steps Taken Relating to the Incident

Following discovery of the data security incident, JWJEF is working to reduce the risk of a similar incident occurring in the future. Additionally, JWJEF retained IDX, a company specializing in credit and identity monitoring services, to offer complimentary privacy and identity theft protection for 24 months to those with impacted Social Security numbers. These services also include credit and CyberScan monitoring, identity restoration, and a \$1 million identity theft insurance policy. The affected residents were also provided with additional information about steps to take to protect their confidential information and privacy.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at Richard.Goldberg@lewisbrisbois.com or by phone at 215.977.4060.

Respectfully,



Richard W. Goldberg
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

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

November 28, 2022

Subject: Notice of Data <<Variable 1 – Security Incident or Breach>>

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

I write to inform you about a data security incident experienced by Jobs With Justice Education Fund (“JWJEF”) that may have affected your personal information. JWJEF takes the privacy and security of all personal information in its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? We recently learned that your information may have been involved in a data security incident. On August 11, 2022, we discovered JWJEF’s credit cards had been misused. Upon further investigation, we also determined that the employees involved also had access to some employment records. We took immediate steps to revoke the employees’ permissions to the network and promptly launched an investigation. In so doing, we engaged independent digital forensics and incident response experts to help us determine what happened and to identify any information that may have been accessed without authorization. Although your personal information may have been involved in the incident, which is the reason for this notification, we have no reason to believe that this information has been misused.

What Information Was Involved? The information potentially impacted in connection with this incident included your first and last name, date of birth, mailing address, Social Security number, health insurance, retirement account, and other benefits enrollment information.

What Are We Doing? As soon as we discovered this incident, we took the immediate steps described above. In addition, we are working to minimize the risk of a similar incident occurring in the future. We also notified law enforcement about this incident and will continue to cooperate with any investigation they are conducting.

Although we have no evidence of the misuse of any potentially impacted information, we are providing you with information about steps that you can take to help protect your personal information and are offering you and your family (2 adults and up to 5 minors) complimentary identity theft protection services through IDX – a global identity protection and recovery services expert. These services include 24 months of credit and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your or your family’s identity is compromised.

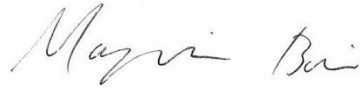
Visit <https://app.idx.us/account-creation/protect> to activate the identity monitoring services. You have until February 28, 2023 to activate your identity monitoring services. Please use the enrollment code listed above.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. JWJEF also encourages you to enroll in the complimentary services being offered to you through IDX by using the enrollment code provided above.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call IDX at 1-800-939-4170 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). IDX call center representatives are fully versed on this incident and can answer any questions that you may have.

Please know that we take this matter very seriously and deeply regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in cursive script, appearing to read "Mackenzie Baris".

Mackenzie Baris
Deputy Director
Jobs With Justice Education Fund
1150 Connecticut Avenue NW, Suite 200
Washington, DC 20036

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

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

November 28, 2022

Subject: Notice of Data <<Variable 1 – Security Incident or Breach>>

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

I write to inform you about a data security incident experienced by Jobs With Justice Education Fund (“JWJEF”) that may have affected your personal information. JWJEF takes the privacy and security of all personal information in its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? We recently learned that your information may have been involved in a data security incident. On August 11, 2022, we discovered JWJEF’s credit cards had been misused. Upon further investigation, we also determined that the employees involved also had access to some employment records. We took immediate steps to revoke the employees’ permissions to the network and promptly launched an investigation. In so doing, we engaged independent digital forensics and incident response experts to help us determine what happened and to identify any information that may have been accessed without authorization. Although your personal information may have been involved in the incident, which is the reason for this notification, we have no reason to believe that this information has been misused.

What Information Was Involved? The information potentially impacted in connection with this incident included your first and last name, date of birth, mailing address, Social Security number, health insurance, retirement account, and other benefits enrollment information.

What Are We Doing? As soon as we discovered this incident, we took the immediate steps described above. In addition, we are working to minimize the risk of a similar incident occurring in the future. We also notified law enforcement about this incident and will continue to cooperate with any investigation they are conducting.

Although we have no evidence of the misuse of any potentially impacted information, we are providing you with information about steps that you can take to help protect your personal information and is offering you complimentary identity protection services through IDX – a global identity protection and recovery services expert. These services include 24 months of credit and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

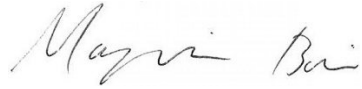
Visit <https://app.idx.us/account-creation/protect> to activate the identity monitoring services. You have until February 28, 2023 to activate your identity monitoring services. Please use the enrollment code listed above.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. JWJEF also encourages you to enroll in the complimentary services being offered to you through IDX by using the enrollment code provided above.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call IDX at 1-800-939-4170 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). IDX call center representatives are fully versed on this incident and can answer any questions that you may have.

Please know that we take this matter very seriously and deeply regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in cursive script, appearing to read "Mackenzie Baris".

Mackenzie Baris
Deputy Director
Jobs With Justice Education Fund
1150 Connecticut Avenue NW, Suite 200
Washington, DC 20036

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

To the Parent or Guardian of:

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

November 28, 2022

Subject: Notice of Data <<Variable 1 – Security Incident or Breach>>

Dear the Parent or Guardian of <<First Name>> <<Last Name>>,

I write to inform you about a data security incident experienced by Jobs With Justice Education Fund (“JWJEF”) that may have involved your child’s personal information. JWJEF takes the privacy and security of all personal information in its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your child’s personal information.

What Happened? We recently learned that your child’s information may have been involved in a data security incident. On August 11, 2022, we discovered JWJEF’s credit cards had been misused. Upon further investigation, we also determined that the employees involved also had access to some employment records. We took immediate steps to revoke the employees’ permissions to the network and promptly launched an investigation. In so doing, we engaged independent digital forensics and incident response experts to help us determine what happened and to identify any information that may have been accessed without authorization. Although your child’s personal information may have been involved in the incident, which is the reason for this notification, we have no reason to believe that this information has been misused.

What Information Was Involved? The information involved may include your child’s first and last name, date of birth, mailing address, and Social Security number.

What Are We Doing? As soon as we discovered this incident, we took the immediate steps described above. In addition, we are working to minimize the risk of a similar incident occurring in the future. We also notified law enforcement about this incident and will continue to cooperate with any investigation they are conducting.

To help relieve concerns you may have following this incident, we have secured the services of IDX to provide identity theft protection services for your family (2 adults and up to 5 minors) at no cost to you for 24 months. IDX is a global leader in identity risk mitigation and response. The identity monitoring services include 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 or your family’s identity is compromised.

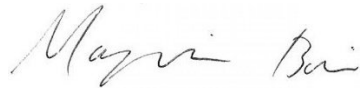
Visit <https://app.idx.us/account-creation/protect> to activate the identity monitoring services. You have until February 28, 2023 to activate your child’s identity monitoring services. Please use the enrollment code listed above.

What You Can Do: We encourage you to activate the identity monitoring services we are making available through IDX. Please also review the enclosed “Steps You Can Take to Protect Your Child’s Information” included with this letter. It describes additional steps you can take to help protect your child, including recommendations regarding identity theft protection.

For More Information: If you have questions or need assistance, please call IDX at 1-800-939-4170 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). IDX call center representatives are fully versed on this incident and can answer any questions that you may have.

Please know that we take this matter very seriously and deeply regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in cursive script, reading "Mackenzie Baris". The ink is dark and the signature is fluid.

Mackenzie Baris
Deputy Director
Jobs With Justice Education Fund
1150 Connecticut Avenue NW, Suite 200
Washington, DC 20036

(Enclosure)

Steps You Can Take to Protect Your Child's Information

Review Any Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review statements from your child's accounts closely. 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 should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Personal Information of a Minor: You can request that each of the three national consumer reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the consumer reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies is below.

Security Freeze: You may place a free credit freeze for minors under age 16. By placing a security freeze, someone who fraudulently acquires the minor's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the 3 national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, the minor will not be able to borrow money, obtain instant credit, or get a new credit card until the freeze is temporarily lifted or permanently removed. You must separately place a security freeze on the minor's credit file with each credit reporting agency. There is no charge to place, lift, or remove a security freeze on the minor's credit files. In order to place a security freeze, you may be required to provide the credit reporting agency with information that identifies you and/or the minor, including birth or adoption certificate, Social Security card, and government issued identification card.

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on the minor's credit report. An initial fraud alert is free and will stay on the minor's credit file for at least one year. This informs creditors of possible fraudulent activity within the minor's report and requests that the creditor contact you prior to establishing any accounts in the minor's name. To place a fraud alert, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center

Raleigh, NC 27699

ncdoj.gov

1-877-566-7226

Rhode Island Attorney General

150 South Main Street

Providence, RI 02903

<http://www.riag.ri.gov>riag.ri.gov

1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW

Washington, DC 20001

oag.dc.gov

1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in the minor's file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.