COZEN O'CONNOR

June 1, 2021

VIA EMAIL (DOJ-CPB@DOJ.NH.GOV)

Nicole H. Sprinzen
Direct Phone 202-471-3451
Direct Fax 202-499-2941
nsprinzen@cozen.com

Ann-Marie Luciano
Direct Phone 202-471-3420
Direct Fax 202-912-4820
aluciano@cozen.com

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

I write on behalf of our client, American Councils for International Education ("American Councils"), a not-for-profit organization that administers language study programs in the United States and internationally. Pursuant to N.H. Rev. Stat. Ann. § 359-C:19 *et seq.*, this letter is to inform you that American Councils recently discovered that a limited number of finalists in one of its programs received administrator-level viewing access to the web-based database it uses to collect and maintain records for applicants, finalists and participants in the programs it administers. On May 18, 2021, American Councils determined that the inadvertent access affected 24 New Hampshire individuals.

Immediately upon discovery of the issue, American Councils terminated all access to the Application Information System ("AIS") Forms database, thus ending the ability of any finalist to view any other individual's information in the database. The same evening it became aware of the issue, American Councils was able to provide the correct access to the finalists, and again enabled their access to the database (with the correct access). American Councils took additional steps to address the situation, including conducting an internal investigation as to the extent of access and the possible causes for the data exposure and taking measures to ensure that a similar situation will not occur in the future. Those measures included revising user profiles so that user access is the default access provided within the AIS Forms database and ensuring that applicants, finalists and participants cannot be given administrator-level access, and conducting refresher training for all American Councils personnel who administer the database as to the occurrence of this situation and the correct access to provide program applicants, finalists and participants.

American Councils determined that the data exposure occurred between April 21-28, 2021. The program finalists were inadvertently given administrator-level view access, rather than user access that would allow them to upload their own application-related documents to the system but not view anyone else's records. With administrator-level view access, those participants had the ability to view all current and past applicant, finalist and participant records maintained in the database since 2009. The access enabled those individuals to view records and personal data belonging to other applicants, finalists and participants, including for New

Hampshire individuals, education records, medical records (including mental health records, where applicable), requests for accommodations (physical, health, visual, learning), insurance information, passport and visa records, naturalization records, birth certificates, bank account information, and other forms of government identification.

Of the 550 program finalists who received administrator-level view access, only 375 accessed the database during the period they had access. However, American Councils has not been able to determine whether those participants accessed records or data belonging to anyone other than themselves during that period, or what records or data they did access.

It is important to note that participant files and data are randomized in the AIS Forms database. During the limited exposure, a person viewing the data could not search, filter, or organize the files in question and participants were not grouped by program or last name. At no time did any of the finalists have the ability to edit any records in the database other than their own. Also, none of the finalists had access to any recommendations or application evaluations for any participants.

In addition, none of the finalists had access to any credit card information because American Councils does not collect payment information in the AIS Forms database. Information about participation in a program such as locations of programs and dates of program participation and travel was not available. Please also note that the data that was exposed is stored in the application intake portal, not the program management system. For these reasons, we remain confident that the risk of any misuse of these records is extremely low.

American Councils is committed to ensuring the privacy and security of the information of our applicants, participants, and finalists. American Councils is offering identity protection and credit monitoring services to those whose social security number or bank account number was affected by the incident (this includes only six New Hampshire individuals with a bank account number and no New Hampshire individuals with a social security number exposed) free of charge for one year. Attached for your reference is a sample of the notice to the affected individuals, which is being sent as expeditiously as possible via American Councils' electronic communication system through the AIS Forms database, which it uses routinely to communicate with these individuals.

If you have any questions, please contact me at (202) 471-3451.

Sincerely,

COZEN O'CONNOR

/s/ Nicole Sprinzen and /s/ Ann-Marie Luciano

By: Nicole H. Sprinzen and Ann-Marie Luciano

Cc: Lisa Choate, American Councils for International Education
Arseny Makaleev, American Councils for International Education

Enclosures

Sample Customer Notice and Reference Guide

TO: Name

Dear Name:

We value and respect the privacy of your information, which is why as a precautionary measure we are writing to inform you of a data exposure that occurred at American Councils for International Education (American Councils) between April 21-28, 2021.

What happened?

On April 28, 2021, American Councils became aware that a limited number of finalists in one of its programs received administrator-level viewing access to the web-based database it uses to collect and maintain records for applicants, finalists and participants in the programs it administers. That access enabled those individuals to view records and personal data belonging to other applicants, finalists and participants, including education records, medical records (including mental health records, where applicable), requests for accommodations (physical, health, visual, learning), insurance information, passport and visa records, naturalization records, birth certificates, and other government identification. We are providing you this notice because on May 18, 2021, we determined that your personal records were among those that were accessible, although we have not determined that your records have been viewed.

The program finalists were inadvertently given administrator-level view access, rather than user access that would allow them to upload their own application-related documents to the system but not view anyone else's records. With administrator-level view access, those participants had the ability to view all current and past applicant, finalist and participant records maintained in the database since 2009.

It is important to note that participant files and data are randomized in the Application Information System ("AIS") Forms database. During the limited exposure, a person viewing the data could not search, filter or organize the files

in question and participants were not grouped by program or last name. At no time did any of the finalists have the ability to edit any records in the database other than their own. Also, none of the finalists had access to any recommendations or application evaluations for any participants.

In addition, none of the finalists had access to any credit card information because American Councils does not collect payment information in the AIS Forms database. Information about participation in a program such as locations of programs and dates of program participation and travel was not available. Please also note that the data that was exposed is stored in the application intake portal, not the program management system. For these reasons, we remain confident that the risk of any misuse of these records is extremely low.

Of the 550 program finalists who received administrator-level view access, only 375 accessed the database during the period they had access. However, American Councils has not been able to determine whether those participants accessed records or data belonging to anyone other than themselves during that period, or what records or data they did access.

What steps did we take in response?

Immediately upon discovery of the issue, American Councils terminated all access to the AIS Forms database, thus ending the ability of any finalist to view any other individual's information in the database. American Councils took additional steps to address the situation, including conducting an internal investigation as to the extent of access and the possible causes for the data exposure and taking measures to ensure that a similar situation will not occur in the future.

Those measures include revising user profiles so that user access is the default access provided within the AIS Forms database and ensuring that applicants, finalists and participants cannot be given administrator-level access, and conducting refresher training for all American Councils personnel who administer the database as to the occurrence of this situation and the correct access to provide program applicants, finalists and participants.

What are your next steps?

You are not required to take any steps. However, the attached Reference

Guide provides information to help you protect your personal information.

We regret the occurrence of this situation. Please be assured that American Councils took prompt action to address it as soon as we became aware of it, including taking additional steps to ensure the security of current and past applicants, finalists and participants' information. Should you have further questions, you may contact American Councils at notice@americancouncils.org or (+1) 202-743-7527.

Yours sincerely,

Reference Guide (for Residents of the United States)

We encourage you to take the following steps:

What you can do to protect your information: You can enroll in a credit monitoring service. Many are available and are offered by companies like LifeLock, Experian, and other companies.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. Remain vigilant and monitor your account statements. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Place an initial fraud alert.
- Order your credit reports.
- Create an FTC Identity Theft Affidavit by submitting a report about the theft at http://www.ftc.gov/complaint or by calling the FTC.
- File a police report about the identity theft and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit with you when you file the police report.
- Your Identity Theft Report is your FTC Identity Theft Affidavit plus your police report. You may be able to use your Identity Theft Report to remove fraudulent information from your credit report, prevent companies from refurnishing fraudulent information to a consumer reporting agency, stop a company from collecting a debt that resulted from identity theft, place an extended seven-year fraud alert with consumer reporting

agencies, and obtain information from companies about accounts the identity thief opened or misused.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consumers Have The Right To Obtain A Security Freeze You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 7 years. See below for more details on placing a fraud alert on your credit file.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

How to Place A Security Freeze on Your Credit File. Placing, temporarily lifting, and removing a security freeze (also known as a "credit freeze") are free of charge. To place, temporarily lift, or remove a security freeze on/from your credit file, you must make a request with each of the three nationwide consumer reporting agency individually. For more information on security freezes, you may contact the three nationwide consumer reporting agencies as described below or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years

- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285 (Fraud Alert) 1-800-349-9960 (Credit Freeze)	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289 (Fraud Alert) 1-888-909-8872 (Credit Freeze)	www.transunion.com

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For Massachusetts Residents. You have the right to obtain a police report and request a free security freeze as described above. Placing a security freeze may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office

Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (Toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. You can obtain information from the Oregon Attorney General's Office about preventing identity theft. You can contact the Oregon Attorney General at:
Oregon Department of Justice
1162 Court St. NE
Salem, OR 97301
1-(877) 877-9392 (toll-free)
https://www.doj.state.or.us/

For Rhode Island Residents. You can obtain information from the Rhode Island Attorney General's Office about preventing identity theft. You can contact the Rhode Island Attorney General at:
Rhode Island Attorney General's Office
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.

- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.

- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.

- You have the right to ask for a credit score.

- You have the right to dispute incomplete or inaccurate information.

- Consumer reporting agencies 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 reports to be provided to employers.

- You may limit “prescreened” offers of credit and insurance you receive based on information in your credit report.

Sample Customer Notice and Reference Guide
Individuals with Bank Account No. or SS No.
With Credit Monitoring

TO: Name

Dear Name:

We value and respect the privacy of your information, which is why as a precautionary measure we are writing to inform you of a data exposure that occurred at American Councils for International Education (American Councils) between April 21-28, 2021.

What happened?

On April 28, 2021, American Councils became aware that a limited number of finalists in one of its programs received administrator-level viewing access to the web-based database it uses to collect and maintain records for applicants, finalists and participants in the programs it administers. That access enabled those individuals to view records and personal data belonging to other applicants, finalists and participants, including education records, medical records (including mental health records, where applicable), requests for accommodations (physical, health, visual, learning), insurance information, passport and visa records, naturalization records, birth certificates, bank account information, social security number, and other government identification. We are providing you this notice because on May 18, 2021, we determined that your personal records were among those that were accessible, although we have not determined that your records have been viewed.

The program finalists were inadvertently given administrator-level view access, rather than user access that would allow them to upload their own application-related documents to the system but not view anyone else's records. With administrator-level view access, those participants had the ability to view all current and past applicant, finalist and participant records maintained in the database since 2009.

It is important to note that participant files and data are randomized in the Application Information System ("AIS") Forms database. During the limited exposure, a person viewing the data could not search, filter or organize the files

in question and participants were not grouped by program or last name. At no time did any of the finalists have the ability to edit any records in the database other than their own. Also, none of the finalists had access to any recommendations or application evaluations for any participants.

In addition, none of the finalists had access to any credit card information because American Councils does not collect payment information in the AIS Forms database. Information about participation in a program such as locations of programs and dates of program participation and travel was not available. Please also note that the data that was exposed is stored in the application intake portal, not the program management system. For these reasons, we remain confident that the risk of any misuse of these records is extremely low.

Of the 550 program finalists who received administrator-level view access, only 375 accessed the database during the period they had access. However, American Councils has not been able to determine whether those participants accessed records or data belonging to anyone other than themselves during that period, or what records or data they did access.

What steps did we take in response?

Immediately upon discovery of the issue, American Councils terminated all access to the AIS Forms database, thus ending the ability of any finalist to view any other individual's information in the database. American Councils took additional steps to address the situation, including conducting an internal investigation as to the extent of access and the possible causes for the data exposure and taking measures to ensure that a similar situation will not occur in the future.

Those measures include revising user profiles so that user access is the default access provided within the AIS Forms database and ensuring that applicants, finalists and participants cannot be given administrator-level access, and conducting refresher training for all American Councils personnel who administer the database as to the occurrence of this situation and the correct access to provide program applicants, finalists and participants.

What are your next steps?

You are not required to take any steps. However, the attached Reference

Guide provides information to help you protect your personal information, and offers you one year of free credit monitoring.

We regret the occurrence of this situation. Please be assured that American Councils took prompt action to address it as soon as we became aware of it, including taking additional steps to ensure the security of current and past applicants, finalists and participants' information. Should you have further questions, you may contact American Councils at notice@americancouncils.org or (+1) 202-743-7527.

Yours sincerely,

Lisa Choate
Executive Vice President
American Councils for International Education

Reference Guide (for residents of the United States)

We encourage you to take the following steps:

Enroll in Identity Protection and Credit Monitoring Services; Access Identity Restoration Services if Needed.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one-year from the date of this letter.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration You will also find self-help tips and information about identity protection at this site.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks SM as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: **August 31, 2021** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your activation code: [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by August 31, 2021. Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

Additional details regarding your Experian IdentityWorks Membership: A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring**: Actively monitors Experian file for indicators of fraud.

- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.

- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.

- **Experian IdentityWorks ExtendCARETM**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.

- **$1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

    * Offline members will be eligible to call for additional reports quarterly after enrolling.

    ** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

What you can do to protect your information: There are actions you can consider taking to reduce the chances of identity theft or fraud. Please refer to www.ExperianIDWorks.com/restoration for this information, and refer to the additional steps below.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. Remain vigilant and monitor your account statements. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or

financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Place an initial fraud alert.
- Order your credit reports.
- Create an FTC Identity Theft Affidavit by submitting a report about the theft at http://www.ftc.gov/complaint or by calling the FTC.
- File a police report about the identity theft and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit with you when you file the police report.
- Your Identity Theft Report is your FTC Identity Theft Affidavit plus your police report. You may be able to use your Identity Theft Report to remove fraudulent information from your credit report, prevent companies from refurnishing fraudulent information to a consumer reporting agency, stop a company from collecting a debt that resulted from identity theft, place an extended seven-year fraud alert with consumer reporting agencies, and obtain information from companies about accounts the identity thief opened or misused.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consumers Have The Right To Obtain A Security Freeze You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 7 years. See below for more details on placing a fraud alert on your credit file.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

How to Place A Security Freeze on Your Credit File. Placing, temporarily lifting, and removing a security freeze (also known as a "credit freeze") are free of charge. To place, temporarily lift, or remove a security freeze on/from your credit file, you must make a request with each of the three nationwide consumer reporting agency individually. For more information on security freezes, you may contact the three nationwide consumer reporting agencies as described below or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285 (Fraud Alert) 1-800-349-9960 (Credit Freeze)	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289 (Fraud Alert) 1-888-909-8872 (Credit Freeze)	www.transunion.com

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division

200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For Massachusetts Residents. You have the right to obtain a police report and request a free security freeze as described above. Placing a security freeze may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (Toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. You can obtain information from the Oregon Attorney General's Office about preventing identity theft. You can contact the Oregon Attorney General at:
Oregon Department of Justice
1162 Court St. NE
Salem, OR 97301
1-(877) 877-9392 (toll-free)
https://www.doj.state.or.us/

For Rhode Island Residents. You can obtain information from the Rhode Island Attorney General's Office about preventing identity theft. You can contact the Rhode Island Attorney General at:
Rhode Island Attorney General's Office
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.

- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.

- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.

- You have the right to ask for a credit score.

- You have the right to dispute incomplete or inaccurate information.

- Consumer reporting agencies 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 reports to be provided to employers.

- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.