

**BakerHostetler**

**RECEIVED**

**FEB 04 2020**

**CONSUMER PROTECTION**

**Baker&Hostetler LLP**

811 Main Street  
Suite 1100  
Houston, TX 77002-6111

T 713.751.1600  
F 713.751.1717  
[www.bakerlaw.com](http://www.bakerlaw.com)  
Will Daugherty  
direct dial: 713.646.1321  
[wdaugherty@bakerlaw.com](mailto:wdaugherty@bakerlaw.com)

January 31, 2020

**VIA OVERNIGHT MAIL**

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

*Re: Supplemental Incident Notification*

Dear Attorney General MacDonald:

We are writing on behalf of our client, Golden Entertainment, Inc. (“Golden”), to provide an update regarding a security incident that was reported to your office on November 7, 2019.

As explained in the notice to your office, on November 7, 2019, Golden provided notice to one New Hampshire resident pursuant to N.H. Rev. Stat. Ann. § 359-C:20 in connection with an incident involving unauthorized access to some Golden employees’ email accounts. Since then, Golden continued to work diligently to identify address information for individuals whose personal information was identified in emails and attachments that may have been accessible in the accounts. Additionally, Golden’s investigation uncovered two additional employee email accounts with unauthorized access. The unauthorized access occurred for all of the employees’ accounts identified in Golden’s investigation at various times between May 30, 2019 and October 6, 2019. The investigation was not able to determine which emails or attachments, if any, were accessed by the unauthorized person. Out of an abundance of caution, Golden conducted a comprehensive review of the emails and attachments in these employees’ email accounts and, on January 3, 2020, determined that an email or an attachment to an email in the email accounts may have contained the personal information of some New Hampshire residents.

Today, Golden is beginning to send notification letters via First-Class mail to the 10 additional New Hampshire residents whose address information was recently located and whose personal information was found in the additional accounts. The accounts contained the name, Social Security number, and driver’s license number of the 10 New Hampshire residents. The total number of New Hampshire residents notified in connection with this incident is 11. This

January 31, 2020

Page 2

notice is being provided in accordance with N.H. Rev. Stat. Ann. § 359-C:20<sup>1</sup>. Enclosed is a sample copy of the letter. Additionally, for individuals whose personal information was identified in the employees' email accounts for whom Golden lacks sufficient information to determine the mailing addresses, Golden is providing substitute notice by issuing a press release and posting a notification on its website. A copy of the press release and website message are enclosed. Golden is also emailing individuals for whom it does not have a mailing address and for whom Golden has an email address. Golden is offering one year of complimentary credit monitoring and identity theft protection services through Experian to individuals whose Social Security Number or driver's license number were contained in the email accounts involved. Golden also established a call center for the individuals to call with any questions regarding the incident.

To help prevent this type of incident from happening in the future, Golden is implementing additional safeguards and technical measures, including multi-factor authentication, and is providing additional training to employees.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Will Daugherty  
Partner

Enclosure

---

<sup>1</sup> This report does not waive Golden's objection that New Hampshire lacks personal jurisdiction over Golden.



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

Golden Entertainment, Inc. ("Golden Entertainment") takes the privacy and security of personal information very seriously. We are writing to inform you about an incident we recently identified and addressed that may have involved some of your information. This letter explains the incident, measures we have taken, and some steps you can take in response.

Our investigation into an email phishing incident determined that an unauthorized individual obtained access to some employees' email accounts. Upon first learning of the incident, we immediately took steps to secure the email accounts, launched an investigation, and a cybersecurity firm was engaged to assist. Findings from our investigation indicate that an unauthorized individual obtained access to the email accounts at various times between May 30, 2019 and October 6, 2019. The investigation was not able to determine which emails or attachments, if any, were accessed by the unauthorized person. Out of an abundance of caution, Golden Entertainment conducted a comprehensive review of the emails and attachments in the employees' email accounts and, on <<b2b\_text\_4 (date of discovery variable)>>, determined that an email or an attachment to an email in the email accounts contained some of your personal information, including your <<b2b\_text\_1 (variable data elements)>><<b2b\_text\_5 (variable data elements)>>.

We wanted to make you aware of our findings and assure you that we take this type of incident very seriously. As a precaution, **we are offering you a complimentary one-year membership of Experian's® IdentityWorks™ Credit 3B**. This product provides you with identity detection and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the additional information provided in the following pages.**

We regret this incident occurred and apologize for any inconvenience. To help prevent this type of incident from happening in the future, we are implementing additional safeguards and technical measures, and are providing additional training to our employees. If you have any questions about this matter, please call 1-855-946-0123 Monday through Friday between 9:00 a.m. and 6:30 p.m. EST.

Sincerely,

A handwritten signature in black ink, appearing to read "Sharon DiAmbrosio".

Sharon DiAmbrosio  
Associate Vice President, Human Resources

## Activate IdentityWorks Credit 3B Now in Three Easy Steps

- Ensure that you **enroll by:** <>**b2b\_text\_2 (Date)>** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** <>**Member ID>**

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-288-8057** by <>**b2b\_text\_2 (Date)>**. Be prepared to provide engagement number <>**b2b\_text\_3 (Engagement #)>** as proof of eligibility for the identity restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** 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.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>  
or call 877-288-8057 to register with the activation code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

\* 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.

## Additional Steps You Can Take

Regardless of whether you choose to take advantage of the complimentary credit monitoring, we remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

**If you are a resident of Maryland, New York, or North Carolina**, you may contact and obtain information from your state attorney general at:

- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us)
- *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>
- *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/>
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)

**If you are a resident of Maryland**, the mailing address of Golden Entertainment, Inc. is 6595 S Jones Blvd Las Vegas, NV 89118.

**If you are a resident of West Virginia**, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

**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](http://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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

# Golden Entertainment, Inc. Announces Data Security Incident

---

NEWS PROVIDED BY

**Golden Entertainment, Inc.** →

Jan 31, 2020, 22:20 ET

---

LAS VEGAS, Jan. 31, 2020 /PRNewswire/ -- Golden Entertainment, Inc. ("Golden Entertainment") is notifying some of our customers, employees, and vendors of an incident involving unauthorized access to some of our employees' email accounts that we recently addressed. This notice explains the incident, measures we have taken, and some steps you can take in response.

Golden Entertainment's investigation into an email phishing incident determined that an unauthorized individual obtained access to some employees' email accounts. Golden Entertainment immediately took steps to secure the email accounts, launched an investigation, and a cybersecurity firm was engaged to assist. Findings from Golden Entertainment's investigation indicate that an unauthorized individual obtained access to the email accounts at various times between May 30, 2019 and October 6, 2019. The investigation was unable to determine which emails or attachments, if any, were accessed by the unauthorized person. Out of an abundance of caution, Golden Entertainment conducted a comprehensive review of the emails and attachments in the employees' email accounts and, on October 8, 2019 and January 3, 2020, determined that an email or an attachment to an email in the email accounts contained personal information of some of our customers, employees, and vendors, including names, Social Security numbers, passport numbers, government ID numbers, driver's license numbers, dates of birth, usernames, passwords, payment card numbers, expiration dates, card security codes (CVV), financial account numbers, routing numbers, health insurance information, and health or treatment information.

Golden Entertainment takes the security of personal information very seriously. To date, we have no evidence that any information has been misused, but we wanted to make our customers, employees, and vendors whose information was contained in the email accounts aware of our findings. On November 7, 2019, we began mailing letters to individuals whose information was involved and continued to mail letters through January 31, 2020, as we found additional addresses and identified additional email accounts involved. Golden Entertainment has also established a dedicated call center to answer questions about this matter. If you believe your information was involved and have not received a letter by February 7, 2020, please call 1-855-946-0123, Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time.

It is always advisable to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. As a precaution, Golden Entertainment is also offering individuals whose Social Security number or driver's license number was involved complementary credit monitoring and identity protection services.

Golden Entertainment regrets this incident occurred and apologizes for any inconvenience. To help prevent this type of incident from happening in the future, Golden Entertainment is implementing additional safeguards and technical measures as well as providing additional phishing-awareness training to our employees.

For more information, please visit <http://goldenent.com/emailsecurityincident>.

SOURCE Golden Entertainment, Inc.

#### Related Links

<http://www.goldenent.com>

[\*\*California Residents Click Here\*\*](#)

**NOTICE OF DATA SECURITY INCIDENT**

January 31, 2020

Golden Entertainment, Inc. (“Golden Entertainment”) is notifying some of our customers, employees, and vendors of an incident involving unauthorized access to some of our employees’ email accounts that we recently addressed. This notice explains the incident, measures we have taken, and some steps you can take in response.

Our investigation into an email phishing incident determined that an unauthorized individual obtained access to some employees’ email accounts. Upon first learning of the incident, we immediately took steps to secure the email accounts, launched an investigation, and a cybersecurity firm was engaged to assist. Findings from our investigation indicate that an unauthorized individual obtained access to the email accounts at various times between May 30, 2019 and October 6, 2019. The investigation was not able to determine which emails or attachments, if any, were accessed by the unauthorized person. Out of an abundance of caution, we conducted a comprehensive review of the emails and attachments in the employees’ email accounts and, on October 8, 2019 and January 3, 2020, determined that an email or an attachment to an email in the email accounts contained names, Social Security numbers, passport numbers, government ID numbers, driver’s license numbers, dates of birth, usernames, passwords, payment card numbers, expiration dates, card security codes (CVV), financial account numbers, routing numbers, health insurance information, and health or treatment information.

Golden Entertainment takes the security of personal information very seriously. To date, we have no evidence that any information has been misused, but we wanted to make our customers, employees, and vendors whose personal information was contained in the email accounts aware of our findings. On November 7, 2019, we began mailing letters to individuals whose personal information was involved and continued to mail letters through January 31, 2020, as we found additional addresses and identified additional email accounts involved. Golden Entertainment has also established a dedicated call center to answer questions about this matter.

It is always advisable to remain vigilant to remain for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. Information on additional steps you can take in response is provided below this message. As a precaution, Golden Entertainment is also offering individuals whose Social Security number or driver’s license number was involved complementary credit monitoring and identity protection services.

We regret this incident occurred and apologize for any inconvenience. To help prevent this type of incident from happening in the future, we are implementing additional safeguards and technical measures as well as providing additional phishing-awareness training to our employees. If you have questions or believe your information was potentially involved, please call 1-855-946-0123, Monday through Friday, between 9:30 a.m. to 6:30 p.m., Eastern Time.

## **ADDITIONAL STEPS YOU CAN TAKE**

It is always advisable to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized activity on your financial account, contact your financial institution immediately. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111  
*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  
*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

**If you are a resident of Connecticut, Maryland, Massachusetts, New York, or North Carolina**, you may contact and obtain information from your state attorney general at:

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag)
- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, <http://www.oag.state.md.us>
- *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, <http://www.mass.gov/ago/contact-us.html>
- New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>
- New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/>
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)

**If you are a resident of Maryland**, the mailing address of Golden Entertainment, Inc. is 6595 S Jones Blvd Las Vegas, NV 89118.

**If you are a resident of West Virginia**, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (“PIN”) or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

**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](http://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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.