

BakerHostetler

RECEIVED

FEB 23 2019

CONSUMER PROTECTION

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

February 25, 2019

VIA OVERNIGHT MAIL

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

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Evergreen Alliance Golf Limited L.P., d/b/a Arcis Golf, to notify your office of a security incident involving New Hampshire residents.¹

After Arcis Golf received a report suggesting that there may have been unauthorized access to data from payment cards that were legitimately used at certain Arcis Golf locations, Arcis Golf immediately launched an investigation and engaged a leading computer security firm to assist. On January 16, 2019, findings from the investigation identified the operation of malware designed to access payment card data from cards used on point-of-sale (POS) devices at certain Arcis Golf locations. The malware was designed to search for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the POS devices. It is possible that data from cards used at the locations involved may have been accessed between August 15, 2018 and February 4, 2019.

Arcis Golf maintains the name and mailing address for some of its guests who visit an Arcis Golf property and use a payment card, but not for every guest, depending on the purpose for which the card is used. As a result, Arcis Golf is able to determine that at least four (4) New Hampshire residents used a payment cards at one of the Arcis Golf locations involved in this incident, and Arcis Golf is mailing notification letters to such residents for whom it maintains mailing information. An example of the notification letter is enclosed. With regard to guests for which Arcis Golf maintains no mailing information, Arcis Golf is providing substitute notice under N.H. Rev. Stat. § 359-C:20, by posting a statement on its website that includes a list of locations involved and by issuing a press release. Copies of

¹ This report is not a waiver of any objection that New Hampshire lacks personal jurisdiction over Arcis Golf.

February 25, 2019

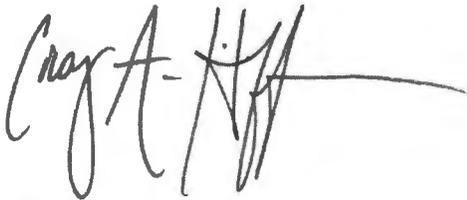
Page 2

the press release and website notice are enclosed. Notification is being provided without unreasonable delay.

During the investigation, Arcis Golf worked with cyber security experts to remove the malware and deploy an endpoint security tool to devices across its network. Arcis Golf continues to partner with the cyber security firm to evaluate ways to enhance its network security measures. In addition, Arcis Golf continues to support law enforcement's investigation and is working with the payment card networks so that the banks that issue payment cards can be made aware of the incident and initiate heightened monitoring.

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

Sincerely,

A handwritten signature in black ink, appearing to read "Craig A. Hoffman", with a long horizontal line extending to the right.

Craig Hoffman
Partner

Enclosure

[Arcis Golf Letterhead]

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<Date>>

<<City>><<State>><<Zip>>

<<Country>>

Dear <<Name 1>>:

At Arcis Golf, we value the relationship we have with our members and understand the importance of protecting personal information. We are writing to inform you that we recently identified and addressed an incident that may have involved your payment card information. This notice explains the incident, measures we have taken in response, and some additional steps you may consider taking.

After we received a report suggesting that there may have been unauthorized access to data from payment cards that were legitimately used at certain Arcis Golf locations, the Company immediately launched an investigation and engaged a leading computer security firm to assist. On January 16, 2019, findings from the investigation identified the operation of malware designed to access payment card data from cards used on point-of-sale (POS) devices at certain Arcis Golf locations. The malware was designed to search for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the POS devices. It is possible that data from cards used at the locations involved may have been accessed between August 15, 2018 and February 4, 2019. We are notifying you because you used a payment card ending in <<<Last 4 of Card Number>>> at one of the identified locations during this time period.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized credit card charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

During the investigation, we worked with cyber security experts to remove the malware and deploy an endpoint security tool to devices across our network. We continue to partner with the cyber security firm to evaluate ways to enhance our security measures. In addition, we are working with the payment card networks so that the banks that issue payment cards can be made aware of the incident and initiate heightened monitoring.

We regret that this incident occurred and apologize for any inconvenience. If you have questions regarding this incident, you can call 877-734-5504 Monday through Friday between the hours of 8:00 a.m. and 8:00 p.m. CST.

Sincerely,

[Signature]

Scott Siddons
General Counsel
Arcis Golf

ADDITIONAL STEPS YOU CAN TAKE

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 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, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, 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 Centre, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Connecticut, Maryland, 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, 1-860-808-5318, www.ct.gov/ag
- *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
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

If you are a resident of Massachusetts, please note that pursuant to Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

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 90 days. 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.

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.

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
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, 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 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 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 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 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. 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.

News Release

Media contact:
Karen Moraghan
Hunter Public Relations
kmoraghan@hunter-pr.com
(908) 963-6013

Arcis Golf Notifies Guests of Payment Card Incident

DALLAS, TX (February 22, 2019) – Evergreen Alliance Golf Limited, L.P. d/b/a Arcis Golf (“Arcis Golf” or “the Company”) has identified and taken measures to address a payment card security incident that may have affected cards used at its locations between August 15, 2018 and February 4, 2019. This press release explains the incident, the measures Arcis Golf has taken, and some steps that members and guests can take in response.

After Arcis Golf received a report suggesting that there may have been unauthorized access to data from payment cards that were legitimately used at certain Arcis Golf locations, Arcis Golf immediately launched an investigation and engaged a leading computer security firm to assist. On January 16, 2019, findings from the investigation identified the operation of malware designed to access payment card data from cards used on point-of-sale (POS) devices at certain Arcis Golf locations. The malware was designed to search for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the POS devices. It is possible that data from cards used at the locations involved may have been accessed between August 15, 2018 and February 4, 2019. A list of the Arcis Golf locations involved is available at www.arcisgolf.com/paymentcardincident. In addition to this notice, Arcis Golf will be mailing a notification letter to those individuals that Arcis Golf has a mailing address for and could determine that they used their card at one of the locations involved during the time frame of the incident.

Arcis Golf reminds members and guests that it is always advisable to remain vigilant to the possibility of fraud by reviewing payment card statements for any unauthorized activity. Members and guests should immediately report any unauthorized charges to the card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card.

During the investigation, Arcis Golf worked with cyber security experts to remove the malware and deploy an endpoint security tool to devices across its network. Arcis Golf continues to partner with the cyber security firm to evaluate ways to enhance its security measures. In addition, Arcis Golf is working with the payment card networks so that the banks that issue payment cards can be made aware of the incident and initiate heightened monitoring on the affected cards.

Arcis Golf regrets that this incident occurred and apologizes for any inconvenience. For more information, members and guests can visit www.arcisgolf.com/paymentcardincident or call 877-734-5504 Monday through Friday between the hours of 8:00 a.m. and 8:00 p.m. CST.

ABOUT ARCIS GOLF

Recognized as one of the fastest-growing private companies in America, Arcis Golf is the premier operator of public and private golf clubs in the United States with a current portfolio of more than 60 properties in 15

states from coast to coast. An industry leader, providing dynamic direction and unrivaled amenities that complement diverse playing experiences, Arcis Golf is committed reinventing the golf and country club lifestyle experience to a level of excellence that exceeds all expectations. Arcis Golf's allocation of more than \$60 million in major capital improvements to its facilities has resulted in award-winning clubhouse transformations, golf course renovations, and other upgrades that represent part of Arcis Golf's industry-leading acquisition investment of \$400 million since its formation in July 2015. Arcis Golf is supported by Arcis Equity Partners, LLC, a private-equity firm dedicated to making equity and debt investments in the real estate and leisure sectors. Through strategic acquisitions that build and sustain Arcis Golf as a leader in upscale golf and lifestyle experiences, the complete Arcis Golf portfolio benefits from the commitment of Arcis Equity Partners, LLC. Capitalizing on the resources developed to support its growing portfolio, Arcis Golf also provides professional management services to third-party owners under its Arcis Advantage division. Location: 4851 Lyndon B Johnson Fwy, Suite 600 Dallas, Texas 75244. Phone: (214) 722-6000. Website: www.arcisgolf.com

Website Notice

Will appear on: www.arcisgolf.com/paymentcardincident

Arcis Golf Reports Findings from Investigation of Payment Card Incident

California residents click [here](#). [LINK]

Arcis Golf has identified and taken measures to address a payment card security incident that may have affected cards used at its locations between August 15, 2018 and February 4, 2019. This notice explains the incident, measures we have taken to address the security issues, and some steps you can take in response.

After we received a report suggesting that there may have been unauthorized access to data from payment cards that were legitimately used at certain Arcis Golf locations, the Company immediately launched an investigation and engaged a leading computer security firm to assist. On January 16, 2019, findings from the investigation identified the operation of malware designed to access payment card data from cards used on point-of-sale (POS) devices at certain Arcis Golf locations. The malware was designed to search for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the POS devices. It is possible that data from cards used at the locations involved may have been accessed between August 15, 2018 and February 4, 2019. A list of the Arcis Golf locations involved is available [here](#). [LINK]

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized credit card charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

During the investigation, we worked with cyber security experts to remove the malware and deploy an endpoint security tool to devices across our network. We continue to partner with the cyber security firm to evaluate ways to enhance our security measures. In addition, we are working with the payment card networks so that the banks that issue payment cards can be made aware of the incident and initiate heightened monitoring.

We regret that this incident occurred and apologize for any inconvenience. If you have questions regarding this incident, you can call 877-734-5504 Monday through Friday between the hours of 8:00 a.m. and 8:00 p.m. CST.

ADDITIONAL STEPS YOU CAN TAKE

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 or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Confidential/Privileged: Prepared at Request of Counsel

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, 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 Centre, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Connecticut, Maryland, Massachusetts, 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, 1-860-808-5318, www.ct.gov/ag
- *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
- *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

If you are a resident of Massachusetts, note that pursuant to Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

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 90 days. 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.

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.

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
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, 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 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 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 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 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. 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.