BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Patrick H. Haggerty
direct dial: 513.929.3412
phaggerty@bakerlaw.com

December 19, 2018

VIA OVERNIGHT MAIL

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol St.
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

I am writing on behalf of our client, GoldSilver LLC ("GoldSilver"), to notify you of a security incident involving eight (8) New Hampshire residents.

On November 20, 2018, GoldSilver was alerted to a potential security incident in which an attacker demanded an extortion payment or he would release certain customer information obtained from GoldSilver's systems. GoldSilver immediately took steps to secure the system, investigate the credibility of the claim, and engage a forensic computer security firm to assist in the investigation. GoldSilver also requested assistance from the FBI. The investigation determined that an unauthorized person obtained access to a database containing certain customer records between September 28, 2018 and November 20, 2018. GoldSilver conducted a thorough review of the contents of the database and determined that it contained certain customers' information, including the names and financial account numbers for eight (8) New Hampshire residents.

On December 19, 2018, GoldSilver will begin mailing notification letters to the New Hampshire residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20, via United States First-Class mail, in substantially the same form as the enclosed letter.[1] GoldSilver is also providing a telephone number for all notified individuals to call with any questions they may have.

[1] This report does not waive GoldSilver's objection that New Hampshire lacks personal jurisdiction regarding the company related to this matter.

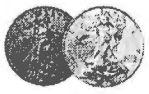
To help prevent something like this from happening in the future, GoldSilver is implementing additional procedures to further expand and strengthen the security of its systems.

Please contact me if you have any questions regarding this matter.

Sincerely,

Patrick H. Haggerty
Partner

Enclosure



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

I am sorry. Regrettably, I am writing to inform you of a recent incident that may have involved your information. This notice describes the incident, outlines the measures we have taken in response, and advises you on steps you can take to further protect your information.

At GoldSilver LLC, we place an extremely high value on maintaining the integrity and security of our customers' information. However, as you are aware, nearly all companies in America and around the world are under constant cyberattack and security incidents occur all too often.

On November 20, 2018, we were alerted to a potential security incident in which a foreign-based attacker demanded an extortion payment or he would release certain customer information obtained from our systems. We immediately took steps to secure the system, investigate the credibility of the claim, and engage a forensic computer security firm to assist in the investigation. We also requested assistance from the FBI.

The investigation determined that an unauthorized person obtained access to a database containing certain customer records between September 28, 2018 and November 20, 2018. We conducted a thorough review of the contents of the database and determined that it contained some of your information, including your name, email address, country and/or state, an encrypted password, <<Variable Data>>. The database may have also contained the partial payment card numbers and your physical address. No full payment card information was accessible, as we store only the partial cards.

All passwords to GoldSilver.com have been deactivated, and access to your account requires access to your email account as a second authentication step until a new password is set. Even though passwords on the system were in encrypted form, if you use the same password for other accounts, we encourage you to change those passwords immediately.

We encourage you to remain vigilant to the possibility of fraud by reviewing your financial statements and credit reports for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. You should also review the additional information on the following pages on ways to protect yourself.

I sincerely apologize for any concern or inconvenience this incident may cause. As a result of this incident, GoldSilver is implementing additional procedures to further expand and strengthen the security of our systems. If you have questions about this matter, please email security@goldsilver.com, or call (888) 319-8166, Monday through Friday between 9:00 am and 5:00 pm Eastern Time.

Sincerely,

Michael R Maloney
Founder

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you to remain 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:

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
Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

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

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, www.oag.state.md.us, 1-888-743-0023 (toll-free when calling within Maryland) or
410-576-6300 (for calls originating outside Maryland)

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or toll-free at 1-877-566-7226

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.

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 number 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 number 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 – Experian, TransUnion and Equifax – 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're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're 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. And you must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.