

**LEWIS
BRISBOIS
BISGAARD
& SMITH LLP**
ATTORNEYS AT LAW

1055 Westlakes Drive, Suite 300
Berwyn, Pennsylvania 19312
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

JAMES E. PRENDERGAST
DIRECT DIAL: 215.977.4058
JIM.PRENDERGAST@LEWISBRISBOIS.COM

June 12, 2014

VIA U.S. MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Event

Dear Sir or Madam:

We represent SafetyFirst, 1055 Parsippany Blvd., Suite 204, Parsippany, NJ 07054, and are writing to notify you of a data security incident that compromised the security of personal information of four (4) New Hampshire residents. SafetyFirst's investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SafetyFirst does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

SafetyFirst assists corporations with maintaining certain records related to the corporation's commercial drivers. On April 2, 2014, SafetyFirst became aware that an FTP server used to back up certain clients' drivers' data was publicly accessible, resulting in unauthorized access to these clients' drivers' personal information. SafetyFirst immediately disconnected the FTP server to prevent further unauthorized access to the data on the server. SafetyFirst then launched an investigation into this matter to determine what information was exposed and how the server was being accessed. To assist with this investigation, SafetyFirst engaged the services of an independent forensics investigation firm.

As part of its investigation, the forensics investigation team analyzed forensics images of the affected server and reviewed all relevant log data. The forensics investigation team determined that

Attorney General Joseph Foster
June 12, 2014
Page 2

the information on the SafetyFirst FTP server became publicly accessible after a configuration error during a routine upgrade. SafetyFirst has been able to identify what information was accessed, when it was accessed and by what IP addresses. The information that was accessed includes the driver's name, Social Security number, driver's license number, medical examiner's certificate and certain medical information specifically related to its client's Federal Motor Carrier Safety Regulation compliance efforts.

Notice to New Hampshire Residents

On May 1, 2014, SafetyFirst began notifying affected clients that their employees' personal information was accessed without authorization. This notice was sent by letter attached to an email in substantially the same form as the letter attached here as Exhibit A. SafetyFirst has been asked by two of its clients to notify these clients affected employees on behalf of the affected client. SafetyFirst is providing affected employees, including four (4) New Hampshire residents, with written notice of this incident commencing on June 13, 2014, in substantially the same form as the letter attached here as Exhibit B.

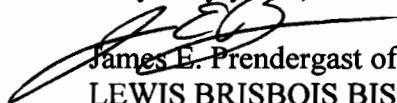
Other Steps Taken and To Be Taken

SafetyFirst takes this matter, and the security of the personal information in its care, seriously and has taken measures to ensure that this type of exposure does not occur again. These measures include an analysis of its systems and processes and implementing additional measures to secure personal information. SafetyFirst is no longer using the affected FTP server process for backups. SafetyFirst is also working with a third party IT expert to ensure that its other systems remain secure. In addition to providing written notice of this incident to affected individuals as described above, each affected individual is being offered access to one free year of credit monitoring and identity restoration services provided through AllClear ID. SafetyFirst is providing each individual with information on how to protect against identity theft and fraud. Further, SafetyFirst is providing written notice of this incident to the other state regulators and consumer reporting agencies where required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-977-4058.

Very truly yours,



James E. Prendergast of
LEWIS BRISBOIS BISGAARD & SMITH LLP

JEP:lpt

cc: SafetyFirst Systems, Inc.

Exhibit A

CLIENT NOTICE TEMPLATE

Dear NAME,

I am writing to inform you of a recent incident that may affect the security of your drivers' personal information.

On April 2, 2014, SafetyFirst became aware that an FTP server used to back up your drivers' data was publicly accessible, resulting in unauthorized access to your drivers' personal information. SafetyFirst immediately disconnected the FTP server to prevent further unauthorized access to the data on the server. SafetyFirst then launched an investigation into this matter to determine what information was exposed and how the server was being accessed. To assist with this investigation, SafetyFirst engaged the services of an independent forensics investigation firm.

As part of its investigation, the forensics investigation team analyzed forensics images of the affected server and reviewed all relevant log data. The forensics investigation team determined that the information on the SafetyFirst FTP server became publicly accessible after a configuration error during a routine upgrade. We have also been able to identify what information was accessed, when it was accessed and by what IP addresses.

Our investigation into this incident has determined that CLIENT data was first accessed on DATE and last accessed on DATE. Enclosed with this letter is a list of CLIENT drivers whose personal information was accessed. This list also indicates what personal information was accessed for each driver. We have no evidence at this time of any fraud or identity theft resulting from the inadvertent exposure of your drivers' personal information.

In addition to working with a forensics investigation team, SafetyFirst has also reached out to certain websites that may have indexed or cached the accessed CLIENT data. SafetyFirst has requested that these websites remove the content to prevent further unauthorized accesses to the CLIENT data. SafetyFirst has received confirmation from these websites that CLIENT data has been removed.

The security of our clients' and their employees' personal information is our first priority. We deeply regret this incident and any inconvenience this may cause your or your drivers. We are doing everything possible to safeguard the personal information hosted on SafetyFirst's network and to prevent this type of incident from happening in the future. If you have any questions about the information in this letter or if you would like to discuss this matter further, please contact me at EMAIL ADDRESS or by phone at XXX-XXX-XXXX.

Sincerely,

Paul Farrell

Exhibit B

First Name Last Name
Address
City, State Zip

Dear First Name Last Name,

I am contacting you regarding a data security incident that has occurred at SafetyFirst¹ that may potentially have exposed your personal information – including your name, [client_def1]– to others without authorization. Please be assured that SafetyFirst has taken this incident seriously and is committed to taking every step necessary to address the incident, protect your identity, and ensure that the incident does not occur again.

By way of background, on April 2, 2014, SafetyFirst became aware that an FTP server used to back up drivers' data was publicly accessible, resulting in unauthorized access to your personal information. SafetyFirst immediately disconnected the FTP server to prevent further unauthorized access to the data on the server and launched an investigation, via an independent forensics investigation firm, to determine what information was exposed and how the server was being accessed. The forensics investigation team determined that the information on the SafetyFirst FTP server became publicly accessible after a configuration error during a routine upgrade, and that your personal information was accessed without authorization. We have no evidence, however, that this information has been misused.

We have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. You are automatically eligible to use this service – there is no action required on your part. If a problem arises, simply call [redacted] and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling [redacted] using the following redemption code:

Please note: Additional steps may be required by you in order to set up your security factors and activate your secure phone alerts.

You may also take action directly to further protect against possible identity theft or other financial loss. We encourage you to review your account statements regularly, and to monitor your credit

¹ As you may know, SafetyFirst assists companies, including [client_def2] with maintaining records on its drivers.

reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below. Information regarding security freezes is also available from these agencies.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-ID-THEFT (877-438-4338); TTY: 866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

We sincerely apologize for this incident, regret any inconvenience it may cause you and encourage you to take advantage of the identity protection service outlined in this letter. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact our confidential hotline between 9 a.m. and 9 p.m. EST at ~~XXX-XXX-XXXX~~.

Sincerely,