



Phillips Lytle LLP

Via Fax 617-973-8799 and Mail

May 7, 2008

Office of Consumer Affairs
and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116
Attention: Maureen Tobin

Re: Bryant & Stratton College, Inc.

Dear Ms. Tobin:

In response to your letter dated today requesting additional information regarding the matter referenced above, please be advised that the number of Massachusetts residents potentially affected by the data security breach outlined in Bryant & Stratton College's letter to your office is three (3).

C

Steps taken and plans to take relating to the incident are outlined in the letter Bryant & Stratton College and SunGard Higher Education sent to all potentially affected individuals, a copy of which was provided to you. Bryant & Stratton College is continuing to work with SunGard Higher Education to review and enhance the policies and procedures governing access to and use of personal information.

O

P

If you have any additional questions, please do not hesitate to contact me.

Y

Very truly yours,

Phillips Lytle LLP

By

Sharon Prise Azurin

cc: Office of Attorney General
Martha Coakley (via fax (617) 727-3265 and mail)

SPAse Doc # 01-2215840.1

Sharon Prise Azurin
Direct 716 847 7088 sazurin@phillipslytle.com

ATTORNEYS AT LAW

June XX, 2008

[Name]
[Address]

Dear [Name],

According to Bryant & Stratton College's records, you are a Massachusetts resident. As a follow up to our letter to you dated April 24, 2008 (copy attached for your reference), we are writing to provide you with additional information to help protect yourself from the possible misuse of your personal information as outlined by Massachusetts law G.L. ch. 93H.

Please be advised that you have the right to obtain a police report in connection with any fraudulent activity that may incur with respect to your credit. In addition to the precautionary steps outlined in our first letter to you, you may also wish to consider placing a security freeze on your credit files. Please review the attached document entitled "Security Freeze Information" which explains how a consumer in Massachusetts may request a security freeze, the necessary information a consumer will need to provide when requesting a security freeze, and any fees required to be paid in connection with placing, temporarily lifting or removing a security freeze.

Please feel free to call the toll-free information line established at 866.520.2408 with any questions or concerns and to visit the website created at www.sungardhe.com/laptoptheft.

As you know, SunGard Higher Education and Bryant & Stratton take this theft and the protection of confidential information very seriously. Bryant & Stratton continues to work with SunGard Higher Education to review and enhance the policies and procedures governing access to and use of personal information.

Sincerely,

Brian Maddocks
Chief Executive Officer
SunGard Higher Education

John Staschak
Chief Executive Officer
Bryant & Stratton College

Doc # 01-2222459.1

Thursday, April 24, 2008

Your eight digit personal identification code: [PIDIM]

[FIRST] [LAST]
[STREET]
[STREET 2 – SKIP IF BLANK]
[CITY] [STATE] [ZIP]

Dear [FIRST] [LAST],

We are writing to inform you of the theft of a laptop computer that may put your personal information at risk. While we do not believe that identity theft was the motive behind the incident, we wanted to inform you of the circumstances and let you know of the precautions you can take.

The laptop that was stolen belonged to a consultant at SunGard Higher Education, a software company that has provided IT services to Bryant & Stratton College ("Bryant & Stratton") for a number of years. The theft occurred on March 13, 2008 and was immediately reported to law enforcement but the laptop has not been recovered. The matter continues to be under investigation. The laptop was protected with a strong password to prevent access to the operating system. After an analysis of backup data, SunGard Higher Education found that the stolen laptop contained data from projects with Bryant & Stratton. Bryant & Stratton received notification of this security breach on April 14, 2008. Security teams from Bryant & Stratton and SunGard Higher Education then worked together to further analyze and verify the data.

We are writing to you because the analysis indicated that the stolen laptop contained your personal information. We determined that your name, address and Social Security number were included in the data. Although we believe the laptop was stolen for the value of the hardware rather than the data, we recommend that you take steps to protect yourself from the possible misuse of your personal information.

A website has been created at www.sungardhe.com/laptoptheft to provide you with information on how to protect your identity. We recommend you visit the site and take the precautionary steps outlined to help guard yourself against potential identity theft. For example, we recommend that you carefully review your credit card, debit card and banking/financial institution(s) statements for any suspicious and/or unauthorized activity. You should consider contacting your credit card, debit card and/or banking/financial institution to report that your Social Security number may have been compromised and consider closing or shutting down your account(s) and opening a new account with a new PIN, security code or password. You are also encouraged to request a copy of your credit report. You are entitled to receive one free report per year from each of the three main consumer reporting companies:

- Equifax – 800.525.6285 or www.equifax.com, P.O. Box 740241, Atlanta, Georgia 30374-0241
- Experian – 888.397.3742 or www.experian.com, P.O. Box 9532, Allen, Texas 75013
- TransUnion – 800.680.7289 or www.tuc.com, Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, California 92834-6790

If you believe that fraudulent activity has occurred, you might also want to contact the Social Security Administration fraud line at 800-269-0271 or www.ssa.gov. Another helpful resource is to contact the Federal Trade Commission website regarding identity theft: <http://www.consumer.gov/idtheft> for guidance and tools or call toll free at 1-877-IDTHEFT (1-877-438-4338). Your state of residence may also have information available on-line or otherwise.

A toll-free information line has also been established at 866.520.2408 to address your questions and concerns. As a precaution, to help you detect any possible misuse of your data, credit monitoring will be provided, at no cost to you, for a period of one year. ConsumerInfo.com, Inc., an Experian® company has been selected to provide you with this service. This credit monitoring product known as Triple AlertSM will identify and notify you of key changes in your three national credit reports that may indicate fraudulent activity.

Your complimentary 12 month membership includes:

- Monitoring all three credit files with Experian, Equifax® and TransUnion® – everyday
- Email alerts of key changes indicating possible fraudulent activity – within 24 hours
- Monthly "No Hit" alerts, if applicable
- Dedicated team of fraud resolution representatives for victims of identity theft
- \$25,000 identity theft insurance with no deductible*

*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York.

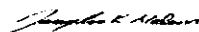
You need to contact the help desk at 866.520.2408 to obtain your credit monitoring activation code. You will be asked to provide the help desk the eight-digit personal identification code which appears above your name in the address block on this letter to obtain your code.

Once you have your code, please visit <http://partner.consumerinfo.com/start> and enter the activation code. You will be instructed on how to initiate your online membership.

You have until August 1, 2008 to activate this membership, which will then continue for 12 full months. We encourage you to activate your credit monitoring membership quickly.

SunGard Higher Education and Bryant & Stratton take this theft and the protection of confidential information very seriously. Bryant & Stratton continues to work with SunGard Higher Education to review and enhance the policies and procedures governing access to and use of personal information. SunGard Higher Education has taken immediate action and sincerely regrets that this incident occurred. SunGard Higher Education apologizes to Bryant & Stratton, to you, and the entire Bryant & Stratton community for the inconvenience this incident may cause.

Sincerely,



Douglas K. Nelson
Vice President
SunGard Higher Education



John J. Staschak
President & CEO
Bryant & Stratton College

SECURITY FREEZE INFORMATION

Any consumer in Massachusetts may place a security freeze on his or her credit report by sending a request in writing, by mail to all credit reporting agencies. The credit reporting agency is not allowed to charge a fee to victims or their spouses for placing, removing for a specific period or party, or removing a security freeze on a credit report. To prove you are a victim, you must also send to the credit reporting agency a valid copy of a police report. All other consumers must pay a \$5 fee for each placing, temporary lifting or removing of a security freeze. A security freeze shall prohibit, with certain specific exceptions, the credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. The freeze goes into effect three (3) business days from receipt of the consumer's letter by the credit reporting agency.

To obtain more detailed information on how to place a security freeze on your credit reports, see below.

HOW TO "FREEZE" YOUR CREDIT FILES

A security freeze means that your file cannot be shared with potential creditors. A security freeze can help prevent identity theft. Most businesses will not open credit accounts without first checking a consumer's credit history. If your credit files are frozen, even someone who has your name and Social Security number probably would not be able to obtain credit in your name. A security freeze is free to identity theft victims who have a police report, investigative report or a complaint to a law enforcement agency concerning identity theft.

How do I place a security freeze?

To place a freeze, you must write to each of the three credit bureaus. Credit bureaus charge a \$5 fee, unless you are a victim or victim's spouse who sends a copy of your police report concerning identity theft.

Write to *all* three addresses below and include the information that follows:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
P.O. Box 6790
Fullerton, CA 92834-6790

For each, you must:

- Send a letter by mail;

- Provide your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth;
- If you have moved in the past 5 years, supply the addresses where you have lived over the prior 5 years.
- Provide proof of current address such as a current utility bill or phone bill
- Send a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
- If you are not a victim, include payment by check, money order or credit card (Visa, Master Card, American Express, or Discover cards only.)

How long does it take for a security freeze to be in effect?

After 3 business days from receiving your letter, the credit reporting agencies listed above will place a freeze providing credit reports to potential creditors.

After 5 business days from receiving your letter to place a freeze on your account, the credit reporting agencies will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep this PIN or password in a safe place.

Can I open new credit accounts if my files are frozen?

Yes. You can have a security freeze lifted for a specific temporary period of time. This is done at no charge for victims. For non-victims, however, there is a \$5 charge for either temporarily lifting the security freeze for a specific period of time or allowing a specific creditor to access your credit report. The steps to do so are as follows:

- Contact the credit reporting agencies above.
- The manner by which you contact them is determined by them, but it may be by way of telephone, fax or over the Internet.
- You must provide proper identification;
- You must provide your unique PIN or password;
- And, if you are requesting to open your credit to a third party or for a specific period of time, you must provide to whom or during what time period your credit report will be accessible.

How long does it take for a security freeze to be lifted?

Credit bureaus must lift a freeze no later than three (3) business days from receiving your request.

What will a creditor who requests my file see if it is frozen?

A creditor will see a message or a code indicating the file is frozen.

Can a creditor get my credit score if my file is frozen?

No. A creditor who requests your file from one of the three credit bureaus will only get a message or a code indicating that the file is frozen.

Can I order my own credit report if my file is frozen?

Yes.

Can anyone see my credit file if it is frozen?

When you have a security freeze on your credit file, certain entities still have access to it. Your report can still be released to your existing creditors or to collection agencies acting on their own behalf. They can use it to review or collect on your account. Other creditors may also use your information to make offers of credit. Government agencies may also have access in response to a court or administrative order, a subpoena, or a search warrant.

Do I have to freeze my file with all three credit bureaus?

Yes. Different credit issuers may use different credit bureaus. If you want to stop your credit file from being viewed, you must freeze it with Equifax, Experian, and Trans Union.

Will a freeze lower my credit score?

No.

Can an employer do a background check on my credit file?

No. You would have to lift the freeze to allow a background check, just as you would to apply for credit. The process for lifting the freeze is described above.

Does freezing my file mean that I won't receive pre-approved credit offers?

No. You can stop the pre-approved credit offers by calling 888-5OPTOUT (888-567-8688). Or you can do this online at www.optoutprescreen.com. This will stop most of the offers, the ones that go through the credit bureaus. It's good for five years or you can make it permanent.

What law requires security freezes?

The law on security freezes in Massachusetts was passed as HB 4144 during the 2007 legislative session.

Before using these template letters, please read the entire document for complete information.

SAMPLE FREEZE LETTER TO EQUIFAX

Date

Equifax
Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Dear Equifax:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one:

I have included my payment of \$5 to freeze my credit file.

OR

I am an identity theft victim or victim's spouse and a copy of my police report showing identity theft is enclosed.

Yours Truly,

Your Name.

SAMPLE FREEZE LETTER TO TRANS UNION

Date

**Trans Union Security Freeze
P.O. Box 6790
Fullerton, CA 92834-6790**

Dear Trans Union:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one:

I have included my payment of \$5 to freeze my credit file.

OR

I am an identity theft victim or victim's spouse and a copy of my police report showing identity theft is enclosed.

Yours Truly,

Your name

SAMPLE FREEZE LETTER TO EXPERIAN

Date

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Dear Experian:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one:

I have included my payment of \$5 to freeze my credit file.

OR

I am an identity theft victim or victim's spouse and a copy of my police report showing identity theft is enclosed.

Yours Truly,

Your name

IDENTITY THEFT

In order to better protect yourself, it is helpful to know some of the ways identity thefts can occur. Thieves:

- Steal wallets and purses containing personal identification and credit/bank cards.
- Steal mail, including bank and credit card statements, pre-approved credit offers, new checks and tax information
- Complete a change of address form to divert mail to another location.
- Rummage through trash, or the trash of businesses, for personal data in a practice known as “dumpster diving”
- Find personal information in homes
- Use personal information individuals share on the Internet
- Send e-mail posing as legitimate companies or government agencies with which individuals do business.
- Get information from the workplace in a practice known as “business record theft” by stealing files out of offices where a person is a customer, employee, patient or student, bribing an employee who has access to personal files, or “hacking” into electronic files.

HOW TO AVOID IDENTITY THEFT

All consumers should take the following steps to prevent identity theft from occurring:

- Review Credit Reports from each of the three major credit bureaus once a year.
- Place passwords on your credit card, bank and phone accounts.
- Secure personal information in your home.
- Ask about information security procedures in your workplace.
- Don't carry your social security card with you; leave it in a secure place.
- Don't give out your social security number unless it is absolutely necessary; ask to use other types of identifiers when possible.
- Don't give out personal information over the phone, through the mail or over the internet unless you have initiated the contact or are sure you know with whom you are dealing.
- Guard your mail and trash from theft.
- Destroy offers of credit received in the mail that you do not respond to; you may choose to opt-out of receiving free offers of credit.
- Carry only the identification information and the number of credit/debit cards that you actually need.
- Pay attention to your billing cycles—follow up with creditors if bills do not arrive on time.
- Be wary of promotional scams.
- Keep your purse or wallet in a safe place at work.
- Notify your credit card company if you are planning to travel out of state.

WHAT TO DO IF YOU ARE A VICTIM OF IDENTITY THEFT

If you are a victim of identity theft, or believe you may be a victim, it is important that you take the following steps:

- Place a fraud alert on your credit reports and review your credit reports
- Place a security freeze on your credit reports.
- Close any accounts that have been tampered with or opened fraudulently.
- File a police report and ask for a copy for your records
- File a complaint with the Federal Trade Commission and the Attorney General's Office.
- Write down the name of anyone you talk to, what s/he told you, and the date of the conversation.
- Follow-up in writing with all contacts you have made about the identity theft on the phone or in person. Use certified mail, return receipt requested, for all correspondence regarding identity theft.
- Keep all copies of all correspondence or forms relating to identity theft.
- Keep the originals of supporting documentation, like police reports and letters to and from creditors; send copies only.
- Keep old files, even if you believe the problem is resolved. If it happens again, you will be glad you did.