

July 2, 2013

Attorney General Michael A. Delaney  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

**Re: Champlain College — Supplemental Notice of Data Security Event**

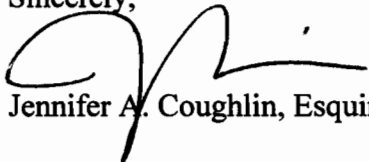
Dear Sir or Madam:

We represent Champlain College (“College”), P.O. Box 670 Burlington, VT 05402-0670. On May 31, 2013, we provided notice to your office of an incident potentially affecting the security of one thousand and eleven (1,011) New Hampshire residents’ personal information. A copy of our May 31, 2013 notice to you is attached to this letter as *Exhibit A*.

On June 7, 2013, the College’s investigation, as well as the investigation of the independent, third-party computer forensic experts Kivu Consulting, Inc. identified an additional one hundred and fifty-nine (159) New Hampshire residents whose name and Social Security number were stored on the portable storage device. On or about July 5, 2013, the College will send these New Hampshire residents written notice in substantially the same form as the sample notice attached to this letter as *Exhibit B*. The College is offering each individual access to one (1) free year of identity monitoring and restoration services. The College is also providing each individual with information on how to protect against identity theft and fraud. The College is also supplementing its notice of this incident to other state regulators and to the national consumer reporting agencies.

Should you have any questions regarding this supplemental notification or other aspects of the data security event, please contact us at 215-358-5134.

Sincerely,



Jennifer A. Coughlin, Esquire

cc: Champlain College

Attachments

# ***EXHIBIT A***



Jennifer A. Coughlin  
D: 215.358.5134  
jcoughlin@nidhlaw.com

518 Township Line Road  
Suite 300  
Blue Bell, PA 19422  
P: 215.358.5100  
F: 215.358.5101

May 31, 2013

Attorney General Michael A. Delaney  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

**Re: Champlain College — Notice of Data Security Event**

Dear Sir or Madam:

We represent Champlain College ("College"), P.O. Box 670 Burlington, VT 05402-0670, and are writing to notify you of a data event that may have compromised the security of personal information of one thousand and eleven (1,011) New Hampshire residents. The College'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, the College does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

**Nature of the Data Security Event**

On or about March 18, 2013, the College discovered a portable storage device connected to an unattended computer in a College computer lab. The College immediately commenced an internal investigation to determine the contents of the drive. The College retained independent forensic experts, Kivu Consulting, Inc. ("Kivu"), to assist in its investigation and in identifying the contents of the portable storage device. The College retained privacy and data security legal counsel to assist with its investigation of, and response to, this incident. These investigations are ongoing; however, it appears that the portable storage device contained the name and Social Security Number of certain College applicants and College students.

**Notice to New Hampshire Residents**

Although the investigations are ongoing, it appears that the personal information of one thousand and eleven (1,011) New Hampshire residents was stored on the portable storage device. The

College is providing these New Hampshire residents with written notice of this incident on or about May 31, 2013, in substantially the same form as the letter attached here as *Exhibit A*.

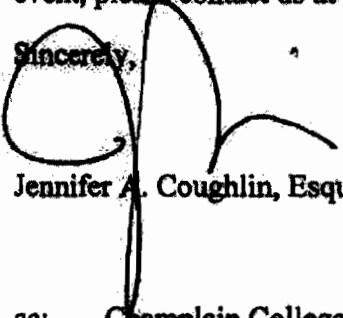
#### **Other Steps Taken and To Be Taken**

In addition to providing written notice of this incident to all affected individuals as described above, the College posted notice of this incident and Frequently Asked Questions on its website. Each affected individual is being offered access to one (1) free year of credit monitoring services and identity restoration services. The College is also providing each individual with information on how to protect against identity theft and fraud. The College is providing written notice of this incident to other state and international regulators, and to the national consumer reporting agencies.

#### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-358-5134.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jennifer A. Coughlin', written over the word 'Sincerely,'.

Jennifer A. Coughlin, Esquire

cc: Champlain College

# EXHIBIT A



Return mail will be processed by: IBC  
P.O. Box 1624  
Fort Mill, SC 29716  
PO #121844A

1 1 00000001 270388

# CHAMPLAIN COLLEGE

163 South Willard Street  
Burlington, Vermont 05402-0670



May 31, 2013

Dear ,

Champlain College is writing to inform you of a recent incident that may affect the security of your personal information. We are unaware of any attempted or actual misuse of your personal information, but with an abundance of caution I am contacting you to make you aware of the incident and provide you with steps to monitor your identity, financial accounts, and credit, should you feel it is necessary to do so.

We take this matter, and the security of your personal information, very seriously and are committed to rectifying the situation as quickly as possible. We are working to make sure this type of incident does not happen again and that we live up to the expectations you have of us to safeguard your information.

In addition to launching our own internal investigation and retaining independent forensics experts, we have engaged privacy and data security legal counsel to assist with our investigation of, and response to, this incident. We are also adopting additional data collection and transfer protocols.

Our goal is to be forthcoming with the truth and to arm you with resources to prevent potential identity theft. While we believe there is little likelihood that your information will be misused as a result of this incident, we want to help you safeguard against identity theft. The remainder of this letter includes information that is not intended to scare you, but instead arm you with resources and information that may be of assistance.

## What happened?

On March 18, 2013, we discovered a portable storage device, used by the college's information systems department, was inadvertently left unattended in an on campus computer lab. We began an internal investigation and a review of the contents and use of the portable storage device. We also retained independent forensics experts to assist with our investigation. Although this investigation is currently ongoing, we've discovered that the portable storage device contained your name, Social Security number, and other information provided by you to the college's financial aid and admissions offices during the application process.

What can you do to protect your identity, financial accounts, and credit, should you feel it is necessary to do so?

First, Champlain College has retained First Watch Technologies, Inc. to provide you with one (1) free year of identity monitoring services. If you enroll, First Watch will monitor thousands of databases and hundreds of billions of records on your behalf to look for suspicious activity that could indicate the beginning steps of identity theft. If suspicious activity is found, First Watch will place a personal phone call to you (at the telephone number that you provide during enrollment) to determine if the suspicious activity is fraudulent. The First Watch ID service also includes up to \$25,000 of identity theft insurance with \$0 deductible, along with identity restoration coverage (certain limitations and exclusions may apply).

You must enroll to receive these services. To enroll, go to <http://www.firstwatchid.com> and take the following steps:

- Click on verification code on the upper right-hand corner of the First Watch ID homepage.
- Enter the appropriate information including your unique 12-digit verification code: .

The deadline to enroll in this service is August 29, 2013.

Second, 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 [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. First Watch provides you with easy access (<http://www.firstwatchid.com>) to this credit bureau service and suggests that every four months you request your free report from one of the three major credit bureaus. If you sign up, First Watch provides you with an email reminder service that notifies you every four months to request your report from the appropriate credit bureau.

Third, at no charge, you can also have the three 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 instructs creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. Once 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](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 6790  
Fullerton, CA 92834  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

Fourth, you may also obtain information on how to place a fraud alert or security freeze on your credit file from your state attorney general. You may obtain your state attorney general's contact information by contacting the local office of your state representative, and by visiting your state government's website. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, [www.ncdoj.gov](http://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](http://www.oag.state.md.us).

Finally, in addition to enrolling in the one free year of identity monitoring services we are offering and suggestions above, we encourage you to remain vigilant, review your account statements, and monitor your credit reports for suspicious or unauthorized activity.

You can further educate yourself on identity theft and the steps you can take to protect yourself, including placing a fraud alert or security freeze on your credit file, by contacting the Federal Trade Commission. The Federal Trade Commission can be reached at:

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
[www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)  
1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261

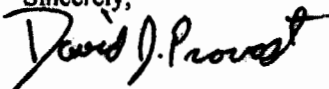
If you believe you are a victim of attempted or actual identity theft or fraud, we encourage you to take the following steps:

- 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.
- File a complaint with your state Attorney General.
- 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've made about the ID theft on the phone or in person. Use certified mail, return receipt requested, for all correspondence regarding the theft.
- Keep copies of all correspondence or forms relating to the suspicious activity, identity theft, or fraud.
- Keep the originals of supporting documentation, such as police reports and letters to and from creditors; send copies only.
- Keep old files, even if you believe the problem is resolved.

We apologize for any inconvenience or concern that this may have caused you. We have established a confidential, toll free inquiry line, staffed with professionals familiar with this incident trained in identity and credit protection and restoration and familiar with this incident, for you to call with any questions or concerns regarding this event or this letter. This confidential line can be reached Monday through Friday, 9:00 a.m. to 7:00 p.m. EST, at (866) 628-6618.

The situation does not appear to be malicious, but still serves as a learning opportunity for Champlain to better serve its students, applicants and their parents. We are committed to getting this right and keeping your information safe.

Sincerely,



David J. Provost  
Vice President of Finance and Administration  
Champlain College



Portsmouth, New Hampshire  
PO #121844A

# CHAMPLAIN COLLEGE

163 South Willard Street  
Burlington, Vermont 05402-0670



Parents or Guardians of

May 31, 2013

Dear Parent/Guardian of:

Champlain College is writing to inform you of a recent incident that may affect the security of your child's personal information. We are unaware of any attempted or actual misuse of your child's personal information, but with an abundance of caution I am contacting you to make you aware of the incident and provide you with steps to monitor your child's identity, financial accounts, and credit, should you feel it is necessary to do so.

We take this matter, and the security of your child's personal information, very seriously and are committed to rectifying the situation as quickly as possible. We are working to make sure this type of incident does not happen again and that we live up to the expectations you have of us to safeguard your child's information.

In addition to launching our own internal investigation and retaining independent forensics experts, we have engaged privacy and data security legal counsel to assist with our investigation of, and response to, this incident. We are also adopting additional data collection and transfer protocols.

Our goal is to be forthcoming with the truth and to arm you with resources to prevent potential identity theft. While we believe there is little likelihood that your child's information will be misused as a result of this incident, we want to help you safeguard your child against identity theft. The remainder of this letter includes information that is not intended to scare you, but instead arm you with resources and information that may be of assistance.

## What happened?

On March 18, 2013, we discovered a portable storage device, used by the college's information systems department, was inadvertently left unattended in an on campus computer lab. We began an internal investigation and a review of the contents and use of the portable storage device. We also retained independent forensics experts to assist with our investigation. Although this investigation is currently ongoing, we've discovered that the portable storage device contained your child's name, Social Security number, and other information provided by your child to the college's financial aid and admissions offices during the application process.

What can you do to protect your child's identity, financial accounts, and credit, should you feel it is necessary to do so?

First, Champlain College has retained First Watch Technologies, Inc. to provide you with the opportunity to enroll your child in its identity monitoring service product for 12 months at no cost to you. Once your child is enrolled, for one year, First Watch will monitor thousands of databases and hundreds of billions of records to look for suspicious activity that could indicate the beginning steps of identity theft. If suspicious activity is found, First Watch will place a personal phone call to you (at the telephone number that you provide) to determine if the suspicious activity is fraudulent. The First Watch ID service also includes up to \$25,000 of identity theft insurance coverage, with \$0 deductible, along with identity restoration coverage (however, certain limitations and exclusions may apply).

Additionally, First Watch will provide you with access to its "Child Protect" tool. Child Protect provides enhanced detection regarding whether your child's social security number is being used. You will be provided a Child Protect Score, which is different than your Identity Risk Score. If you receive a low score for your child, this indicates that First Watch did not detect the use of your child's Social Security number. If you receive a high score, this indicates that First Watch detected activity. Your child's Social Security number will not be recorded or shared.

In order to receive these services, you must enroll your child. To do so, go to <http://www.firstwatchid.com> and take the following steps:

- Click on verification code on the upper right-hand corner of the First Watch ID homepage; and
- Enter the appropriate information including your unique 12-digit verification code: .

The deadline to enroll in this service is August 29, 2013.



Second, under U.S. law, you are entitled to obtain, on behalf of your child, one free credit report annually from each of the three major credit bureaus, so long as the bureau maintains a file on your child. To order your child's free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your child's credit report. First Watch provides you with easy access (<http://www.firstwatchid.com>) to this credit bureau service, and suggests that, every four months, you request your child's free report from one of the three major credit bureaus. First Watch provides you with an email reminder service, if you sign-up, that notifies you every four months to request your child's report from the appropriate credit bureau.

Third, at no charge, you can also have the three credit bureaus place a "fraud alert" on your child's file, if one exists, that alerts creditors to take additional steps to verify your child's identity prior to granting credit in your child's name. Note, however, that because a fraud alert instructs creditors to follow certain procedures to protect your child, it may also delay your child's ability to obtain credit while the agency verifies your child's identity. Once one credit bureau confirms the fraud alert, the others are notified to place a fraud alert on your child's file. Should you wish to place a fraud alert, or should you have any questions regarding your child's 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](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 6790  
Fullerton, CA 92834  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

Fourth, you may also obtain information on how to place a fraud alert or security freeze on your child's credit file from your state attorney general. You may obtain your state attorney general's contact information by contacting the local office of your state representative, and by visiting your state government's website. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, [www.ncdoj.gov](http://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](http://www.oag.state.md.us).

Finally, in addition to enrolling your child in the one free year of identity monitoring services we are offering and the suggestions above, we encourage you to remain vigilant, review your child's account statements, and monitor your child's credit reports for suspicious or unauthorized activity.

You can further educate yourself on identity theft and the steps you can take to protect and your child, including placing a fraud alert or security freeze on your child's credit file, by contacting the Federal Trade Commission. The Federal Trade Commission can be reached at:

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
[www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)  
1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261

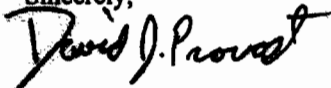
If you believe that you, or your child, are a victim of attempted or actual identity theft or fraud, we encourage you to take the following steps:

- 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.
- File a complaint with your state Attorney General.
- 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've made about the ID theft on the phone or in person, using certified mail, return receipt requested, for all correspondence regarding the theft.
- Keep copies of all correspondence or forms relating to the suspicious activity, identity theft, or fraud.
- Keep the originals of all supporting documentation, such as police reports and letters to and from creditors; send copies only.
- Keep old files, even if you believe that the problem is resolved.

We apologize for any inconvenience or concern that this may have caused you. We have established a confidential, toll free inquiry line, staffed with professionals familiar with this incident trained in identity and credit protection and restoration and familiar with this incident, for you to call with any questions or concerns regarding this event or this letter. This confidential line can be reached Monday through Friday, 9:00 a.m. to 7:00 p.m. EST, at (866) 628-6618.

The situation does not appear to be malicious, but still serves as a learning opportunity for Champlain to better serve its students, applicants and their parents. We are committed to getting this right and keeping your information safe.

Sincerely,



David J. Provost  
Vice President of Finance and Administration  
Champlain College

# EXHIBIT B



Return mail will be processed by: IBC  
P.O. Box 1624  
Fort Mill, SC 29716 3 3 00000998 015221  
PO #121846A

# CHAMPLAIN COLLEGE

163 South Willard Street  
Burlington, Vermont 05402-0670



July 5, 2013

Dear \_\_\_\_\_

Champlain College is writing to inform you of a recent incident that may affect the security of your personal information. We are unaware of any attempted or actual misuse of your personal information, but with an abundance of caution I am contacting you to make you aware of the incident and provide you with steps to monitor your identity, financial accounts, and credit, should you feel it is necessary to do so.

We take this matter, and the security of your personal information, very seriously and are committed to rectifying the situation as quickly as possible. We are working to make sure this type of incident does not happen again and that we live up to the expectations you have of us to safeguard your information.

In addition to launching our own internal investigation and retaining independent forensics experts, we have engaged privacy and data security legal counsel to assist with our investigation of, and response to, this incident. We are also adopting additional data collection and transfer protocols.

**Our goal is to be forthcoming with the truth and to arm you with resources to prevent potential identity theft.** While we believe there is little likelihood that your information will be misused as a result of this incident, we want to help you safeguard against identity theft. The remainder of this letter includes information that is not intended to scare you, but instead arm you with resources and information that may be of assistance.

## What happened?

On March 18, 2013, we discovered a portable storage device, used by the college's information systems department, was inadvertently left unattended in an on campus computer lab. We began an internal investigation and a review of the contents and use of the portable storage device. We also retained independent forensics experts to assist with our investigation. On June 7, 2013, we confirmed that the portable storage device contained your name, Social Security number, and other information provided by you to the college's financial aid and admissions offices during the application process.

**What can you do to protect your identity, financial accounts, and credit, should you feel it is necessary to do so?**

First, Champlain College has retained First Watch Technologies, Inc. to provide you with one (1) free year of identity monitoring services. If you enroll, First Watch will monitor thousands of databases and hundreds of billions of records on your behalf to look for suspicious activity that could indicate the beginning steps of identity theft. If suspicious activity is found, First Watch will place a personal phone call to you (at the telephone number that you provide during enrollment) to determine if the suspicious activity is fraudulent. The First Watch ID service also includes up to \$25,000 of identity theft insurance with \$0 deductible, along with identity restoration coverage (certain limitations and exclusions may apply).

You must enroll to receive these services. To enroll, go to <http://www.firstwatchid.com> and take the following steps:

- Click on verification code on the upper right-hand corner of the First Watch ID homepage.
- Enter the appropriate information including your unique 12-digit verification code:

The deadline to enroll in this service is September 9, 2013.

Second, 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 [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. First Watch provides you with easy access (<http://www.firstwatchid.com>) to this credit bureau service and suggests that every four months you request your free report from one of the three major credit bureaus. If you sign up, First Watch provides you with an email reminder service that notifies you every four months to request your report from the appropriate credit bureau.

Third, at no charge, you can also have the three 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 instructs creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. Once 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](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 6790  
Fullerton, CA 92834  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

Fourth, you may also obtain information on how to place a fraud alert or security freeze on your credit file from your state attorney general. You may obtain your state attorney general's contact information by contacting the local office of your state representative, and by visiting your state government's website. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, [www.ncdoj.gov](http://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](http://www.oag.state.md.us).

Finally, in addition to enrolling in the one free year of identity monitoring services we are offering and suggestions above, we encourage you to remain vigilant, review your account statements, and monitor your credit reports for suspicious or unauthorized activity.

You can further educate yourself on identity theft and the steps you can take to protect yourself, including placing a fraud alert or security freeze on your credit file, by contacting the Federal Trade Commission. The Federal Trade Commission can be reached at:

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
[www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)  
1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261

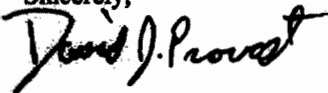
If you believe you are a victim of attempted or actual identity theft or fraud, we encourage you to take the following steps:

- 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.
- File a complaint with your state Attorney General.
- 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've made about the ID theft on the phone or in person. Use certified mail, return receipt requested, for all correspondence regarding the theft.
- Keep copies of all correspondence or forms relating to the suspicious activity, identity theft, or fraud.
- Keep the originals of supporting documentation, such as police reports and letters to and from creditors; send copies only.
- Keep old files, even if you believe the problem is resolved.

We apologize for any inconvenience or concern that this may have caused you. We have established a confidential, toll free inquiry line, staffed with professionals familiar with this incident trained in identity and credit protection and restoration and familiar with this incident, for you to call with any questions or concerns regarding this event or this letter. This confidential line can be reached Monday through Friday, 9:00 a.m. to 7:00 p.m. EST, at (866) 628-6618.

The situation does not appear to be malicious, but still serves as a learning opportunity for Champlain to better serve its students, applicants and their parents. We are committed to getting this right and keeping your information safe.

Sincerely,



David J. Provost  
Vice President of Finance and Administration  
Champlain College