Holland & Knight

800 17th Street, Suite 1100 | Washington, DC 20006 | T 202.955.3000 | F 202.955.5564
Holland & Knight LLP | www.hklaw.com

STATE OF NH
DEPT OF JUSTICE
2017 MAR 29 AM 10: 10

Christopher G. Cwalina
Partner
202-469-5230
chris.cwalina@hklaw.com

March 28, 2017

Attorney General Joseph Foster
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice Pursuant to New Hampshire Statute § 359-C:19

Dear Attorney General Foster:

Pursuant to New Hampshire Statute section 359-C:19, we are writing on behalf of Daytona State College ("DSC") to notify you of a potential unauthorized acquisition of personal information involving approximately thirteen (13) New Hampshire residents.

On or around March 10, 2017, DSC discovered that certain financial aid records for applicants to DSC for 2016-2017 enrollment were accessed. This population includes New Hampshire residents. We believe the incident occurred in January 2017, and is related to another incident that month that DSC became aware of on February 19, 2017.[1] Our investigation into this matter is ongoing; however, at this time, we believe the incident was the result of certain insecure practices by one of DSC's third-party vendors.

At this time, we believe the data at issue includes information contained on students' Free Application for Federal Student Aid (FAFSA) form, which includes name, address, Social Security number, date of birth, driver's license number, and salary information. For dependent students, parent or guardian information, including their name, address, Social Security number, date of birth, and salary information, was also included on the FAFSA form.

DSC is currently not aware of any confirmed misuse of the financial information contained on the FAFSA forms. However, in an abundance of caution and in an effort to protect its students and their parents/guardians, DSC is notifying all potentially impacted students, and all potentially impacted

[1] On March 3, 2017, DSC mailed a letter to all individuals who received a 2016 W-2 regarding this incident; however, no residents of your state are believed to have been impacted.

parents/guardians for whom DSC was able to ascertain a mailing address, to provide information and steps to help protect their information.

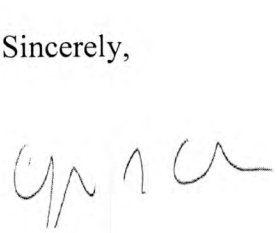
DSC is offering one year of identity protection services, at no cost, to all affected students and parents/guardians. The details of these services and instructions for how to enroll, as well as information regarding additional steps individuals can take to help protect their information, were provided to these individuals in the notice letter that was sent on or around March 24-27, 2017. Enclosed please find a copy of this correspondence.

Below is the contact information for Brian T. Babb, Executive Vice President and General Counsel at DSC:

Brian T. Babb, Executive Vice President and General Counsel
Daytona State College
Building 100, Room 402R
1200 W. International Speedway Blvd.
Daytona Beach, FL 32114
(386) 506-4457

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,



Christopher G. Cwalina

STATE OF NH
DEPT OF JUSTICE

2017 MAR 29 AM 10: 10

[DATE]

«FIRST_NAME» «LAST_NAME»
«ADDRESS_LINE1»
«ADDRESS_LINE2»
«CITY» «ST» «ZIP»

RE: IMPORTANT DATA SECURITY NOTIFICATION

Dear «FIRST_NAME» «LAST_NAME»:

We are writing to let you know about a data security incident discovered in March 2017, involving information from your 2016-2017 financial aid application for Daytona State College (DSC), and to recommend steps that you can take to help protect your information.

We are offering you free identity protection services with Experian, as further detailed in this letter. **Your activation code to enroll in the services is [CODE].** Additional information and enrollment instructions are provided below.

What Happened

We recently discovered that your Free Application for Federal Student Aid (FAFSA) information was involved in a security incident at DSC. We believe the incident was the result of certain insecure practices by one of our third-party vendors. While we discovered this incident in March 2017, we believe the incident occurred in January 2017. DSC is currently not aware of any misuse of the financial information contained on your FAFSA Form.

We are sending this notification to you because we take very seriously the protection of our students' information, regret that this occurred, and want to recommend steps you can take to protect your information.

What Information Was Involved

We believe the information at risk includes information contained on your FAFSA form, which includes your name, address, Social Security number, date of birth, driver's license number, and salary information.

Some students also list their parent/s or guardian's information on the FAFSA. For these students, DSC will also try to reach their parents/guardians to notify them of this incident, but if you fall into this category, we also ask you to let your parents or guardians know about this incident, as we may not be able to identify their home address.

What We Are Doing

DSC is continuing to investigate the security incident and cooperating fully with law enforcement authorities. Meanwhile, we have provided steps below that you can take to help protect your information. DSC is making available to you free identity protection services for one year, as described below. If your FAFSA form contained your parent/s' or guardian/s' information, DSC is also providing them with the free identity protection services, at no charge.

What You Can Do

To prevent and detect misuse of your information, we strongly encourage you to take the preventative measures outlined in this letter.

(1) IRS Protective Measures

As mentioned, DSC is currently not aware that your financial information has been misused. However, below are some immediate steps you may consider taking with respect to your tax return. You may want to file an IRS Form 14039, Identity Theft Affidavit (available at https://www.irs.gov/pub/irs-pdf/f14039.pdf) and, in the event you have not done so already, **complete your 2016 tax filing process as soon as possible**. Even if you have **already filed** your 2016 tax return, we still suggest you file an IRS Form 14039, Identity Theft Affidavit because it will be good for three years. Follow the instructions in the Affidavit.

Language you can use on the Identity Theft Affidavit regarding why you are filing the form is as follows:

> *"My information was recently involved in a data security incident at Daytona State College. My Free Application for Federal Student Aid (FAFSA) form is believed to have been compromised, which included information, such as my name, address, Social Security number, date of birth, driver's license number, salary information, and tax withholdings for 2016."*

If the IRS or your tax preparer advises that a fraudulent tax return has been filed in your name, you should still continue to pay your taxes and file your return, but you will have to file a paper return, along with IRS Form 14039 (Identity Theft Affidavit) attached to the top. The return should be mailed to the address that you would use if mailing a return, which is included in the instructions for paper filings.

The IRS does not initiate contact with taxpayers by email, text or social media to request personal information. The IRS recommends that you respond immediately to any ***written*** IRS notice by calling the number provided in the notice.

You can obtain additional information regarding taxpayer identity theft on the IRS website, at https://www.irs.gov/Individuals/Identity-Protection and https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft, or by calling the IRS at 1-800-908-4490. For information about your state return, visit your state revenue agency's web site at http://www.taxadmin.org/state-tax-agencies.

We also recommend that you notify your accountant and/or tax preparer of this incident.

(2) Identity Protection Services

DSC is providing you with identity protection services with Experian. We recommend that you **activate your one-year membership of Experian IdentityWorks℠** and take the additional steps laid out in this letter. Experian's product helps to reduce your risk and helps you protect yourself by alerting you to identity theft and potentially unauthorized transactions.

To start monitoring your personal information, please follow the steps below:

1. Ensure that you **enroll by**: **March 25, 2018** (Your code will not work after this date.)
2. **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcreditone
3. Provide your **activation code**. Your individual activation code is included on the first page of this letter. Please refer to the beginning of this letter for your code.

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks℠ online, please contact Experian's customer care team at (866) 318-2317 by March 25, 2018. Be prepared to provide **engagement number DB01007** as proof of eligibility for the identity restoration services by Experian.

In addition to a one-year membership Experian IdentityWorks℠, DSC is also providing you with Experian's Identity Restoration services. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer of Identity Restoration assistance is available to you for one-year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Additional details regarding your 12-MONTH EXPERIAN IDENTITYWORKS℠ Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks℠.

You can contact Experian **immediately** regarding any fraud issues, and you will have access to the following features once you enroll in Experian IdentityWorks℠:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for fraud indicators.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

You can also find additional information from Experian at www.ExperianIDWorks.com/restoration.

For More Information

We have attached information regarding additional actions you can take to help reduce the chances of identity theft or fraud on your account as well as resources to obtain additional information about identity theft and ways to protect yourself.

Questions and Concerns

We sincerely apologize for any inconvenience and encourage you to take advantage of the Experian services. We have contracted with experts at Experian to provide you with support related to this incident. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact this free service at (866) 318-2317.

Sincerely,

Ken Matthews
Associate Vice President for Enrollment Services
Daytona State College
Building 100, Room 210-C
1200 W. International Speedway Blvd.
Daytona Beach, FL 32114

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➢ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	**Experian**	**TransUnion**
PO Box 740241	PO Box 4500	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

➢ PLACE AN EXTENDED FRAUD ALERT ON YOUR CREDIT FILE

You may also want to consider contacting the credit reporting companies and asking them to place an extended fraud alert. If you are a victim of identity theft and have created an Identity Theft Report, you can place an extended fraud alert on your credit file. It stays in effect for 7 years. When you place an extended alert, you can get 2 free credit reports within 12 months from each of the 3 nationwide credit reporting companies, and the credit reporting companies must take your name off marketing lists for prescreened credit offers for 5 years, unless you ask them to put your name back on the list.

➢ SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call 877-322-8228.
Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, contact your insurer at the

number on the statement. If you do not receive regular explanation of benefits statements, contact your provider to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **BE ON THE LOOKOUT FOR PHISHING SCHEMES**

We recommend that you be on the lookout for suspicious emails. Specifically, watch for phishing schemes, which are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator.

Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (look for misspellings in the email address). It is also important that you check the recipient's email address to ensure it is legitimate.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft. If you believe a fraudulent tax return has been filed in your name, we recommend that you contact the Internal Revenue Service at the below information.

The U.S. Department of Education's Office of Inspector General also maintains a website describing steps students may take if they suspect they are a victim of identity theft at http://www.ed.gov/about/offices/list/oig/misused/idtheft.html and http://www.ed.gov/about/offices/list/oig/misused/victim.html.

Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Internal Revenue Service, 1111 Constitution Ave NW #5480, Washington, DC 20224, 1-800-908-4490, www.irs.gov/identitytheft

For residents of Florida: You may also obtain information about preventing and avoiding identity theft from the Florida Office of the Attorney General:

Florida Office of the Attorney General, Consumer Protection Division
The Capitol PL-01, Tallahassee, FL 32399-1050, 1-866-966-7226,
http://www.myfloridalegal.com/contact.nsf/contact?Open&Section=Citizen_Services

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

STATE OF NH
DEPT OF JUSTICE
2017 MAR 29 AM 10: 10

[DATE]

«FIRST_NAME» «LAST_NAME»
«ADDRESS_LINE1»
«ADDRESS_LINE2»
«CITY» «ST» «ZIP»

RE: IMPORTANT DATA SECURITY NOTIFICATION

Dear «FIRST_NAME» «LAST_NAME»:

We are writing to let you know about a data security incident which was discovered in March 2017, involving information from your dependent's 2016-2017 financial aid application, and to recommend steps you can take to help protect your information.

We are offering you free identity protection services with Experian, as further detailed in this letter. **Your activation code to enroll in the services is [CODE].** Additional information and enrollment instructions are provided below.

What Happened

We recently discovered that your dependent's Free Application for Federal Student Aid (FAFSA) information was involved in a security incident at Daytona State College (DSC). The FAFSA form included your personal information. We believe the incident was the result of certain insecure practices by one of our third-party vendors. While we discovered this incident in March 2017, we believe the incident occurred in January 2017. DSC is currently not aware of any misuse of the financial information contained on your dependent's FAFSA Form.

We are sending this notification to you because we take very seriously the protection of our students' and their parents' information, regret that this occurred, and want to recommend steps you can take to protect your information.

What Information Was Involved

We believe the information at risk includes information contained on your dependent's FAFSA form, which may have included your name, address, Social Security number, date of birth, and salary information.

We have also notified your dependent about this incident.

What We Are Doing

DSC is continuing to investigate the security incident and cooperating fully with law enforcement authorities. Meanwhile, we have provided steps below that you can take to help protect your information. DSC is making available to you (and your dependent) free identity protection services for one year, as described below.

What You Can Do

To prevent and detect misuse of your information, we strongly encourage you to take the preventative measures outlined in this letter.

(1) IRS Protective Measures

As mentioned, DSC is currently not aware that your financial information has been misused. However, below are some immediate steps you may consider taking with respect to your tax return. You may want to file an IRS Form 14039, Identity Theft Affidavit (available at https://www.irs.gov/pub/irs-pdf/f14039.pdf) and, in the event you have not done so already, **complete your 2016 tax filing process as soon as possible**. Even if you have **already filed** your 2016 tax return, we still suggest you file an IRS Form 14039, Identity Theft Affidavit because it will be good for three years. Follow the instructions in the Affidavit.

Language you can use on the Identity Theft Affidavit regarding why you are filing the form is as follows:

> *"My information was recently involved in a data security incident at Daytona State College. My dependent's Free Application for Federal Student Aid (FAFSA) form is believed to have been compromised, which included information, such as my name, address, Social Security number, date of birth, salary information, and tax withholdings for 2016."*

If the IRS or your tax preparer advises that a fraudulent tax return has been filed in your name, you should still continue to pay your taxes and file your return, but you will have to file a paper return, along with IRS Form 14039 (Identity Theft Affidavit) attached to the top. The return should be mailed to the address that you would use if mailing a return, which is included in the instructions for paper filings.

The IRS does not initiate contact with taxpayers by email, text or social media to request personal information. The IRS recommends that you respond immediately to any ***written*** IRS notice by calling the number provided in the notice.

You can obtain additional information regarding taxpayer identity theft on the IRS website, at https://www.irs.gov/Individuals/Identity-Protection and https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft, or by calling the IRS at 1-800-908-4490. For information about your state return, visit your state revenue agency's web site at http://www.taxadmin.org/state-tax-agencies.

We also recommend that you notify your accountant and/or tax preparer of this incident.

(2) Identity Protection Services

DSC is providing you with identity protection services with Experian. We recommend that you **activate your one-year membership of Experian IdentityWorks℠** and take the additional steps laid out in this letter. Experian's product helps to reduce your risk and helps you protect yourself by alerting you to identity theft and potentially unauthorized transactions.

To start monitoring your personal information, please follow the steps below:

1. Ensure that you **enroll by**: **March 25, 2018** (Your code will not work after this date.)
2. **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcreditone
3. Provide your **activation code**. Your individual activation code is included on the first page of this letter. Please refer to the beginning of this letter for your code.

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks℠ online, please contact Experian's customer care team at (866) 318-2317 by March 25, 2018. Be prepared to provide **engagement number DB01007** as proof of eligibility for the identity restoration services by Experian.

In addition to a one-year membership Experian IdentityWorks℠, DSC is also providing you with Experian's Identity Restoration services. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer of Identity Restoration assistance is available to you for one-year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Additional details regarding your 12-MONTH EXPERIAN IDENTITYWORKS℠ Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks℠.

You can contact Experian **immediately** regarding any fraud issues, and you will have access to the following features once you enroll in Experian IdentityWorks℠:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for fraud indicators.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.

- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

You can also find additional information from Experian at www.ExperianIDWorks.com/restoration.

For More Information

We have attached information regarding additional actions you can take to help reduce the chances of identity theft or fraud on your account as well as resources to obtain additional information about identity theft and ways to protect yourself.

Questions and Concerns

We sincerely apologize for any inconvenience and encourage you to take advantage of the Experian services. We have contracted with experts at Experian to provide you with support related to this incident. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact this free service at (866) 318-2317.

Sincerely,

Ken Matthews
Associate Vice President for Enrollment Services
Daytona State College
Building 100, Room 210-C
1200 W. International Speedway Blvd.
Daytona Beach, FL 32114

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➢ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	**Experian**	**TransUnion**
PO Box 740241	PO Box 4500	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

➢ PLACE AN EXTENDED FRAUD ALERT ON YOUR CREDIT FILE

You may also want to consider contacting the credit reporting companies and asking them to place an extended fraud alert. If you are a victim of identity theft and have created an Identity Theft Report, you can place an extended fraud alert on your credit file. It stays in effect for 7 years. When you place an extended alert, you can get 2 free credit reports within 12 months from each of the 3 nationwide credit reporting companies, and the credit reporting companies must take your name off marketing lists for prescreened credit offers for 5 years, unless you ask them to put your name back on the list.

➢ SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call 877-322-8228.
Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, contact your insurer at the

number on the statement. If you do not receive regular explanation of benefits statements, contact your provider to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **BE ON THE LOOKOUT FOR PHISHING SCHEMES**

We recommend that you be on the lookout for suspicious emails. Specifically, watch for phishing schemes, which are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator.

Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (look for misspellings in the email address). It is also important that you check the recipient's email address to ensure it is legitimate.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft. If you believe a fraudulent tax return has been filed in your name, we recommend that you contact the Internal Revenue Service at the below information.

The U.S. Department of Education's Office of Inspector General also maintains a website describing steps students may take if they suspect they are a victim of identity theft at http://www.ed.gov/about/offices/list/oig/misused/idtheft.html and http://www.ed.gov/about/offices/list/oig/misused/victim.html.

Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Internal Revenue Service, 1111 Constitution Ave NW #5480, Washington, DC 20224, 1-800-908-4490, www.irs.gov/identitytheft

For residents of Florida: You may also obtain information about preventing and avoiding identity theft from the Florida Office of the Attorney General:

Florida Office of the Attorney General, Consumer Protection Division
The Capitol PL-01, Tallahassee, FL 32399-1050, 1-866-966-7226,
http://www.myfloridalegal.com/contact.nsf/contact?Open&Section=Citizen_Services

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov