Nelson Mullins

Nelson Mullins Riley & Scarborough LLP
Attorneys and Counselors at Law
Atlantic Station / 201 17th Street, NW / Suite 1700 / Atlanta, GA 30363
Tel: 404.322.6000 Fax: 404.322.6033
www.nelsonmullins.com

July 1, 2011

VIA FIRST CLASS MAIL

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

Re: Data Breach Notification

Dear Attorney General Delaney:

We write to inform you of a recent data security incident on behalf of our client, StudentCity.com, Inc. ("StudentCity"). StudentCity recognized on June 9, 2011 that it was beginning to receive a pattern of reports from a very small number of students that credit card accounts that were used for purchases through StudentCity were subsequently being used to conduct fraudulent transactions. The information contained in the affected database contained the following information about StudentCity customers: name, credit card number and passport number (not specified by applicable New Hampshire R.S. Section 359-C:19, but included as information we want our customers to know). Note, however, that in the great majority of cases, passport number and credit card number were not included in the same record. Note further, that all credit card information was encrypted, but the investigation has revealed that the encryption was broken in some cases.

StudentCity has determined that the breach of security described above may have affected the names, credit card numbers and passport numbers of 266 residents in your state. Our client is providing written notification by U.S. first class mail to all affected residents of Missouri to the last home address our client has on record, and a sample of our notification letters are enclosed. There are multiple forms of letters to address the specific type of information compromised in each case, to allow for specific guidance on risks and steps to be taken that will be most helpful to each individual.

StudentCity immediately contacted its credit card processor, which could detect no issues. Nevertheless, StudentCity did the following: (1) immediately took steps to protect all customer data that might have been compromised; (2) immediately began sending urgent emails to its customers instructing them to check their bank statements on June 11, 2011, so that they could take proactive and preventative action to protect themselves in the event of a compromise,

(3) immediately began an intensive internal investigation on June 9, 2011; (4) immediately contacted the nation's top forensics specialist for credit card breaches that StudentCity could identify (Chris Novak of Verizon Business) on June 10, 2011, and brought Verizon Business to StudentCity's offices to begin its intensive investigation on June 13, 2011; (5) immediately notified the U.S. Secret Service to assist in the investigation; and (6) immediately informed its merchant bank and all the credit card brands that it accepts of the suspected issue.

StudentCity has also set up a website and a call center staffed by Identity Theft Guard Solutions, LLC ("ID Experts") to offer assistance, and identity restoration services, education and insurance to all students and parents impacted through ID Experts for one full year at no cost. Furthermore, StudentCity is taking extraordinary steps to assure that such incidents cannot happen in the future. It will not be collecting credit card information at all; such information will all be collected by a processor whose sole job is the secure collection and processing of credit card information. Passport numbers will be destroyed following the trips for which they are needed, and will be stored only with strong encryption.

Very truly yours,

Jon Neiditz

cc: StudentCity.com, Inc.
Enclosures

[Name]
[Address]
[City, State Zip]

To Speak to ID Experts, Please Call
1-800-555-555
Or Visit: www.example.com
Your Membership Code: [ID Experts will insert]

Dear [Name],

I hope you have received previous emails from me informing you about the attack on StudentCity's system. As soon as we realized something might be wrong, we began telling students about it so that they could protect themselves. This is the formal letter promised in the emails that spells out what we know now, and tells you more about what you can do to protect yourself and how we are trying to help.

On June 9, we began to figure out that we might have a problem based on some reports we were receiving from students. We immediately contacted our credit card processor, which could detect no issues. However, we immediately (1) protected all customer data that might have been compromised; (2) began sending urgent emails to our customers instructing them to check their bank statements on June 11, so that they could take proactive and preventive action to protect themselves in the event of a compromise, (3) began an intensive internal investigation on June 9; (4) contacted the nation's top forensics specialists for credit card breaches that we could identify on June 10, and brought them to our offices on June 13, to begin their own intensive investigation; (5) notified the U.S. Secret Service to get their assistance in the investigation; and (6) informed our merchant bank and all the credit card brands that we accept of the suspected issue.

As soon as we knew, we confirmed to you that your name and credit card information might have been compromised. The personal information was encrypted, but the encryption appears to have been broken in some cases. Going forward, we can promise you that we will no longer face any risk of a credit card compromise, because we will not be collecting your credit card information at all; it will all be collected by a processor whose sole job is the secure collection and processing of credit card information.

Again, we need to stress the importance of having your card cancelled and reissued. When credit card information is breached, the best protection remains reissue of the card. So to protect yourself from the possibility of unauthorized charges, if you have not already done so, we recommend that ***you contact your credit card issuer immediately by calling the toll-free number located on the back of your card or on your monthly statement, tell them you have received this letter, and ask them to cancel and reissue the card.*** You should tell your credit card issuer that your account may have been compromised and review all charges on your account for potentially fraudulent activity. We also recommend that you change your web account password immediately.

We are also offering identity theft protection services through ID Experts®, a data breach and recovery services expert. We have contracted with ID Experts to provide you with a website answering most questions at www.MyIDExperts.com, with general call-center counseling services, and with fully managed recovery services which will include: 12 months of a $20,000 insurance reimbursement policy, exclusive educational materials and access to fraud resolution representatives. With this protection, ID Experts will help you resolve issues if your identity is compromised. You may register for the free ID Experts identity monitoring services or get answers to frequently asked questions at www.MyIDExperts.com, or by calling **1-866-384-9362**.

To learn more about these services and to ensure the safety of your personal information, we encourage you review the information located at www.MyIDExperts.com, or to call ID Experts at 1-866-384-9362. Representatives from ID Experts have been fully versed on the incident and can answer any questions or concerns you may have regarding protection of your personal information. They are available to assist with general information or enrollment in the program and services Monday through Friday from 8am-8pm Eastern Time by calling 1-866-384-9362. Also, remember that answers to frequently asked questions can be found at www.MyIDExperts.com,

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the following access code when calling or enrolling on the website, so please do not discard this letter.

Your Membership Code: [ID Experts will insert individual codes]

We sincerely regret any inconvenience or concern that this matter may have caused you. Thank you for your patience and understanding while we work together to protect your information.

Sincerely,

Jacqui Lewis
Company

(Enclosure)

Recommended Steps to help Protect your Identity

Please Note: No one is allowed to place a fraud alert on your credit report except for you, please follow the instructions below to place the alert.

By immediately taking the following simple steps, you can help prevent your information from being misused.

1. Website: Go to www.MyIDExperts.com, review the Frequently Asked Questions and, if you want, follow the instructions for enrollment. If you do not have Internet access, you can also call 1-866-384-9362 to enroll over the phone. Once you have completed your enrollment, you will receive a welcome letter either by mail or by email if you provide an email address when you sign up. The welcome letter will detail the components of your membership. It will direct you to the exclusive ID Experts' Member Website where you will find other valuable educational information.

2. Telephone: Contact ID Experts at 1-866-384-9362 to gain additional information about this event and to talk with knowledgeable representatives about the appropriate steps to take to protect your credit record.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. You can receive free credit reports by placing fraud alerts and through your credit monitoring. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled with ID Experts, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with ID Experts, you will be contacted by a member of the Recovery Department who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Experts Recovery Advocate who will work on your behalf to identify, stop, and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting

1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

1-888-397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

6. Security Freeze: By placing a freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze is no more than $10 for each credit reporting bureau for a total of $30. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the Federal Trade Commission, there is no charge to place the freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following:

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

For North Carolina Residents:
Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400

For all other US Residents:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502

[Name]
[Address]
[City, State Zip]

To Speak to ID Experts, Please Call
1-800-555-555
Or Visit: www.example.com
Your Membership Code: [ID Experts will insert]

Dear [Name],

I hope you have received previous emails from me informing you about the attack on StudentCity's system. As soon as we realized something might be wrong, we began telling students about it so that they could protect themselves. This is the formal letter promised in the emails that spells out what we know now and tells you more about what you can do to protect yourself, and how we are trying to help.

On June 9, we began to figure out that we might have a problem based on some reports we were receiving from students. We immediately contacted our credit card processor, which could detect no issues. However, we immediately (1) protected all customer data that might have been compromised; (2) began sending urgent emails to our customers instructing them to check their bank statements on June 11, so that they could take proactive and preventive action to protect themselves in the event of a compromise, (3) began an intensive internal investigation on June 9; (4) contacted the nation's top forensics specialists for credit card breaches that we could identify on June 10, and brought them to our offices to begin their intensive investigation on June 13, (5) notified the U.S. Secret Service to get their assistance in the investigation; and (6) informed our merchant bank and all the credit card brands that we accept of the suspected issue.

The investigation is currently ongoing, but we have determined that there was a database breach in the StudentCity system. Your name and passport information *may* have been compromised, but our investigation has also proven that **your credit card information WAS NOT COMPROMISED.** Going forward, we can promise you that we will no longer face any risk of a credit card compromise, because we will not be collecting your credit card information at all; it will all be collected by a processor whose sole job is the secure collection and processing of credit card information. Moreover, we will destroy passport numbers after you travel with us, and more securely encrypt your information while we need to keep it.

A passport number alone does not allow anyone access to your identity or financial information. As long as you physically have your passport, you should be fine. However, we also understand your concerns about fraud charges and potential identity theft and have therefore established the resources discussed below.

We are offering identity theft protection services through ID Experts®, a data breach and recovery services expert. We have contracted with ID Experts to provide you with a website answering most questions at www.MyIDExperts.com, with general call-center counseling services, and with fully managed recovery services which will include: 12 months of a $20,000 insurance reimbursement policy, exclusive educational materials and access to fraud resolution representatives. With this protection, ID Experts will help you resolve issues if your identity is compromised. You may register for the free ID Experts identity monitoring services or get answers to frequently asked questions at www.MyIDExperts.com, or by calling **1-866-384-9362**.

To learn more about these services and to ensure the safety of your personal information, we encourage you review the information located at www.MyIDExperts.com, or to call ID Experts at 1-866-384-9362. Representatives from ID Experts have been fully versed on the incident and can answer any questions or concerns you may have regarding protection of your personal information. They are available to assist with general information or enrollment in the program and services Monday through Friday from 8am-8pm Eastern Time by calling 1-866-384-9362. Also, remember that answers to frequently asked questions can be found at www.MyIDExperts.com,

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the following access code when calling or enrolling on the website, so please do not discard this letter.

Your Membership Code: [ID Experts will insert individual codes]

We sincerely regret any inconvenience or concern that this matter may have caused you. Thank you for your patience and understanding while we work together to protect your information.

Sincerely,

Jacqui Lewis
Company

(Enclosure)

Recommended Steps to help Protect your Identity

Please Note: No one is allowed to place a fraud alert on your credit report except for you, please follow the instructions below to place the alert.

By immediately taking the following simple steps, you can help prevent your information from being misused.

1. Website: Go to www.MyIDExperts.com, review the Frequently Asked Questions and, if you want, follow the instructions for enrollment. If you do not have Internet access, you can also call 1-866-384-9362 to enroll over the phone. Once you have completed your enrollment, you will receive a welcome letter either by mail or by email if you provide an email address when you sign up. The welcome letter will detail the components of your membership. It will direct you to the exclusive ID Experts' Member Website where you will find other valuable educational information.

2. Telephone: Contact ID Experts at 1-866-384-9362 to gain additional information about this event and to talk with knowledgeable representatives about the appropriate steps to take to protect your credit record.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. You can receive free credit reports by placing fraud alerts and through your credit monitoring. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled with ID Experts, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with ID Experts, you will be contacted by a member of the Recovery Department who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Experts Recovery Advocate who will work on your behalf to identify, stop, and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting

1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

1-888-397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

6. Security Freeze: By placing a freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze is no more than $10 for each credit reporting bureau for a total of $30. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the Federal Trade Commission, there is no charge to place the freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following:

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

For North Carolina Residents:
Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400

For all other US Residents:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502

[Name]
[Address]
[City, State Zip]

To Speak to ID Experts, Please Call
1-800-555-555
Or Visit: www.example.com
Your Membership Code: [ID Experts will insert]

Dear [Name],

I hope you have received previous emails from me informing you about the attack on StudentCity's system. As soon as we realized something might be wrong, we began telling students about it so that they could protect themselves. This is the formal letter promised in the emails that spells out what we know now and tells you more about what you can do to protect yourself, and how we are trying to help.

On June 9, we began to figure out that we might have a problem based on some reports we were receiving from students. We immediately contacted our credit card processor, which could detect no issues. However, we immediately (1) protected all customer data that might have been compromised; (2) began sending urgent emails to our customers instructing them to check their bank statements on June 11, so that they could take proactive and preventive action to protect themselves in the event of a compromise, (3) began an intensive internal investigation on June 9; (4) contacted the nation's top forensics specialists for credit card breaches that we could identify on June 10, and brought them to our offices to begin their intensive investigation on June 13; (5) notified the U.S. Secret Service to get their assistance in the investigation; and (6) informed our merchant bank and all the credit card brands that we accept of the suspected issue.

As soon as we knew, we confirmed to you that your name and credit card information might have been compromised, to enable you to take prompt action to protect your account against fraud. The credit card information was encrypted, but the encryption appears to have been broken in some cases. Going forward, we can promise you that we will no longer face any risk of a credit card compromise, because we will not be collecting your credit card information at all; it will all be collected by a processor whose sole job is the secure collection and processing of credit card information.

Again, we need to stress the importance of having your card cancelled and reissued. When credit card information is breached, the best protection remains reissue of the card. So to protect yourself from the possibility of unauthorized charges, if you have not already done so, we recommend that ***you contact your credit card issuer immediately by calling the toll-free number located on the back of your card or on your monthly statement, tell them you have received this letter, and ask them to cancel and reissue the card.*** You should tell your credit card issuer that your account may have been compromised and review all charges on your account for potentially fraudulent activity. We also recommend that you change your credit card web account password immediately.

We now know that your passport number may also have been compromised. Even if it were compromised, we do not expect that theft to cause you any harm or inconvenience. However, going forward we will destroy passport numbers after you travel with us, and more securely encrypt your information while we need to keep it.

A passport number alone does not allow anyone access to your identity or financial information. As long as you physically have your passport, you should be fine. However, we also understand your concerns

about fraud charges and potential identity theft and have therefore established the resources discussed below.

We are offering identity theft protection services through ID Experts®, a data breach and recovery services expert. We have contracted with ID Experts to provide you with a website answering most questions at www.MyIDExperts.com, with general call-center counseling services, and with fully managed recovery services which will include: 12 months of a $20,000 insurance reimbursement policy, exclusive educational materials and access to fraud resolution representatives. With this protection, ID Experts will help you resolve issues if your identity is compromised. You may register for the free ID Experts identity monitoring services or get answers to frequently asked questions at www.MyIDExperts.com, or by calling **1-866-384-9362**.

To learn more about these services and to ensure the safety of your personal information, we encourage you review the information located at www.MyIDExperts.com, or to call ID Experts at 1-866-384-9362. Representatives from ID Experts have been fully versed on the incident and can answer any questions or concerns you may have regarding protection of your personal information. They are available to assist with general information or enrollment in the program and services Monday through Friday from 8am-8pm Eastern Time by calling 1-866-384-9362. Also, remember that answers to frequently asked questions can be found at www.MyIDExperts.com,

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the following access code when calling or enrolling on the website, so please do not discard this letter.

Your Membership Code: [ID Experts will insert individual codes]

We sincerely regret any inconvenience or concern that this matter may have caused you. Thank you for your patience and understanding while we work together to protect your information.

Sincerely,

Jacqui Lewis
Company

(Enclosure)

Recommended Steps to help Protect your Identity

Please Note: No one is allowed to place a fraud alert on your credit report except for you, please follow the instructions below to place the alert.

By immediately taking the following simple steps, you can help prevent your information from being misused.

1. Website: Go to www.MyIDExperts.com, review the Frequently Asked Questions and, if you want, follow the instructions for enrollment. If you do not have Internet access, you can also call 1-866-384-9362 to enroll over the phone. Once you have completed your enrollment, you will receive a welcome letter either by mail or by email if you provide an email address when you sign up. The welcome letter will detail the components of your membership. It will direct you to the exclusive ID Experts' Member Website where you will find other valuable educational information.

2. Telephone: Contact ID Experts at 1-866-384-9362 to gain additional information about this event and to talk with knowledgeable representatives about the appropriate steps to take to protect your credit record.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. You can receive free credit reports by placing fraud alerts and through your credit monitoring. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled with ID Experts, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with ID Experts, you will be contacted by a member of the Recovery Department who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Experts Recovery Advocate who will work on your behalf to identify, stop, and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting

1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

1-888-397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

6. Security Freeze: By placing a freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze is no more than $10 for each credit reporting bureau for a total of $30. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the Federal Trade Commission, there is no charge to place the freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following:

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

For North Carolina Residents:
Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400

For all other US Residents:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502