Cuddl Duds

123456

Return Mail Processing
P.O. Box 90
Claysburg, PA 16625-0090

123456

##C5633-L03-0123456
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN US 12345-6789

January 26, 2017

RE: Notice of Data Breach

Dear Sample A Sample:

Cuddl Duds is writing regarding a recent data security incident that may impact certain payment card information used by you at our e-commerce website. We wanted to provide you with information about this incident, our response, and steps you can take to prevent fraud, should you feel it necessary to do so.

What Happened? On or around December 1, 2016, we received reports of suspicious activity from our third party e-commerce partner. We immediately began to investigate these reports to identify what happened and what information was impacted. Third-party computer forensic investigators were retained to assist with the investigation into what happened and what data was impacted. The investigation initially identified suspicious files on the system. In an abundance of caution, all user passwords were reset as this incident was initially determined to impact only name, address, email address, and encrypted passwords. Further investigation identified a malicious code inserted into the e-commerce website. Upon identifying the malicious code, Cuddl Duds and its partner quickly took steps to remove the code and prevent further unauthorized access. A review of the code determined that it was capable of collecting information provided by customers on the checkout page of Cuddl Duds.

What Information Was Involved? Cuddl Duds's investigation has revealed that the malicious code collected demographic and credit card information entered on our e-commerce site checkout page between March 1, 2015 and December 1, 2016. The information collected included the cardholder's name, shipping address, billing address, email address, card number, card type, expiration date, and CVV. If you were a registered user at our site, your login and password would also have been collected. All user passwords were changed in December after the discovery of the files.

What We Are Doing: We take this incident, and information security, very seriously at Cuddl Duds. We are diligently investigating this incident, with the assistance of third-party forensic experts. We have removed the malicious code, and changed system account passwords so that credit and debit cards used to purchase products from our website after December 1, 2016 are not at risk. We are currently taking steps to further enhance the security of our systems to better protect

against future incidents of this kind. Additionally, we are providing written notice of this incident to those who may be impacted so that they can take steps to prevent possible fraud. We will also be notifying applicable state regulators about this incident.

What You Can Do: You can stay vigilant by reviewing your credit card statements for any suspicious charges. You can also review the enclosed Steps You Can Take to Protect Against Identity Theft and Fraud, which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft. If you use the same username and password at other sites, we recommend that you change the passwords for any other accounts you have that share the same username and or password.

For More Information: We sincerely regret any inconvenience or concern this incident may have caused you. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. You may call the assistance line at (844) 373-9985, Monday through Friday, 9:00 a.m. to 5:00 p.m. E.S.T (excluding U.S. holidays). You may also contact questions@cuddlduds.com with questions or concerns regarding this incident.

Sincerely,

David Komar

David Komar
Principal

123456

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit 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.

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

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
https://www.freeze.equifax.com		

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service

Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. **For Rhode Island residents**, Attorney General can be contacted at (401) 274-4400, http://www.riag.ri.gov/, or 150 South Main Street, Providence, RI 02903. Approximately 73 Rhode Island residents may be impacted by this incident. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or 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 they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

ON GOSSAMER®

123456

Return Mail Processing
P.O. Box 90
Claysburg, PA 16625-0090

123456

##C5633-L01-0123456
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN US 12345-6789

January 26, 2017

RE: Notice of Data Breach

Dear Sample A Sample:

On Gossamer is writing regarding a recent data security incident that may impact certain payment card information used by you at our e-commerce website. We wanted to provide you with information about this incident, our response, and steps you can take to prevent fraud, should you feel it necessary to do so.

What Happened? On or around December 1, 2016, we received reports of suspicious activity from our third party e-commerce partner. We immediately began to investigate these reports to identify what happened and what information was impacted. Third-party computer forensic investigators were retained to assist with the investigation into what happened and what data was impacted. The investigation initially identified suspicious files on the system. In an abundance of caution, all user passwords were reset as this incident was initially determined to impact only name, address, email address, and encrypted passwords. Further investigation identified a malicious code inserted into the e-commerce website. Upon identifying the malicious code, On Gossamer and its partner quickly took steps to remove the code and prevent further unauthorized access. A review of the code determined that it was capable of collecting information provided by customers on the checkout page of On Gossamer.

What Information Was Involved? On Gossamer's investigation has revealed that the malicious code collected demographic and credit card information entered on our e-commerce site checkout page between March 1, 2015 and December 1, 2016. The information collected included the cardholder's name, shipping address, billing address, email address, card number, card type, expiration date, and CVV. If you were a registered user at our site, your login and password would also have been collected. All user passwords were changed in December after the discovery of the files.

What We Are Doing: We take this incident, and information security, very seriously at On Gossamer. We are diligently investigating this incident, with the assistance of third-party forensic experts. We have removed the malicious code, and changed system account passwords so that credit and debit cards used to purchase products from our website after December 1, 2016 are not at risk. We are currently taking steps to further enhance the security of our systems to better protect

against future incidents of this kind. Additionally, we are providing written notice of this incident to those who may be impacted so that they can take steps to prevent possible fraud. We will also be notifying applicable state regulators about this incident.

What You Can Do: You can stay vigilant by reviewing your credit card statements for any suspicious charges. You can also review the enclosed Steps You Can Take to Protect Against Identity Theft and Fraud, which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft. If you use the same username and password at other sites, we recommend that you change the passwords for any other accounts you have that share the same username and or password.

For More Information: We sincerely regret any inconvenience or concern this incident may have caused you. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. You may call the assistance line at (844) 373-9985, Monday through Friday, 9:00 a.m. to 5:00 p.m. E.S.T (excluding U.S. holidays). You may also contact questions@ongossamer.com with questions or concerns regarding this incident.

Sincerely,

David Komar

David Komar
Principal

123456

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit 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.

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

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
https://www.freeze.equifax.com		

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service

Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. **For Rhode Island residents**, Attorney General can be contacted at (401) 274-4400, http://www.riag.ri.gov/, or 150 South Main Street, Providence, RI 02903. Approximately 73 Rhode Island residents may be impacted by this incident. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or 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 they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

Le Mystère

123456

Return Mail Processing
P.O. Box 90
Claysburg, PA 16625-0090

123456

##C5633-L02-0123456
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN US 12345-6789

January 26, 2017

RE: Notice of Data Breach

Dear Sample A Sample:

Le Mystère is writing regarding a recent data security incident that may impact certain payment card information used by you at our e-commerce website. We wanted to provide you with information about this incident, our response, and steps you can take to prevent fraud, should you feel it necessary to do so.

What Happened? On or around December 1, 2016, we received reports of suspicious activity from our third party e-commerce partner. We immediately began to investigate these reports to identify what happened and what information was impacted. Third-party computer forensic investigators were retained to assist with the investigation into what happened and what data was impacted. The investigation initially identified suspicious files on the system. In an abundance of caution, all user passwords were reset as this incident was initially determined to impact only name, address, email address, and encrypted passwords.Further investigation identified a malicious code inserted into the e-commerce website. Upon identifying the malicious code, Le Mystère and its partner quickly took steps to remove the code and prevent further unauthorized access. A review of the code determined that it was capable of collecting information provided by customers on the checkout page of Le Mystère.

What Information Was Involved? Le Mystère's investigation has revealed that the malicious code collected demographic and credit card information entered on our e-commerce site checkout page between March 1, 2015 and December 1, 2016. The information collected included the cardholder's name, shipping address, billing address, email address, card number, card type, expiration date, and CVV. If you were a registered user at our site, your login and password would also have been collected. All user passwords were changed in December after the discovery of the files.

What We Are Doing: We take this incident, and information security, very seriously at Le Mystère. We are diligently investigating this incident, with the assistance of third-party forensic experts. We have removed the malicious code, and changed system account passwords so that credit and debit cards used to purchase products from our website after December 1, 2016 are not at risk. We are currently taking steps to further enhance the security of our systems to better protect

against future incidents of this kind. Additionally, we are providing written notice of this incident to those who may be impacted so that they can take steps to prevent possible fraud. We will also be notifying applicable state regulators about this incident.

What You Can Do: You can stay vigilant by reviewing your credit card statements for any suspicious charges. You can also review the enclosed Steps You Can Take to Protect Against Identity Theft and Fraud, which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft. If you use the same username and password at other sites, we recommend that you change the passwords for any other accounts you have that share the same username and or password.

For More Information: We sincerely regret any inconvenience or concern this incident may have caused you. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. You may call the assistance line at (844) 373-9985, Monday through Friday, 9:00 a.m. to 5:00 p.m. E.S.T (excluding U.S. holidays). You may also contact questions@lemystere.com with questions or concerns regarding this incident.

Sincerely,

David Komar

David Komar
Principal

123456

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit 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.

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

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
https://www.freeze.equifax.com		

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service

Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. **For Rhode Island residents**, Attorney General can be contacted at (401) 274-4400, http://www.riag.ri.gov/, or 150 South Main Street, Providence, RI 02903. Approximately 73 Rhode Island residents may be impacted by this incident. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or 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 they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

CAROLE HOCHMAN

123456

Return Mail Processing
P.O. Box 90
Claysburg, PA 16625-0090

123456

##C5633-L04-0123456
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN US 12345-6789

January 26, 2017

RE: Notice of Data Breach

Dear Sample A Sample:

Carole Hochman is writing regarding a recent data security incident that may impact certain payment card information used by you at our e-commerce website. We wanted to provide you with information about this incident, our response, and steps you can take to prevent fraud, should you feel it necessary to do so.

What Happened? On or around December 1, 2016, we received reports of suspicious activity from our third party e-commerce partner. We immediately began to investigate these reports to identify what happened and what information was impacted. Third-party computer forensic investigators were retained to assist with the investigation into what happened and what data was impacted. The investigation initially identified suspicious files on the system. In an abundance of caution, all user passwords were reset as this incident was initially determined to impact only name, address, email address, and encrypted passwords. Further investigation identified a malicious code inserted into the e-commerce website. Upon identifying the malicious code, Carole Hochman and its partner quickly took steps to remove the code and prevent further unauthorized access. A review of the code determined that it was capable of collecting information provided by customers on the checkout page of Carole Hochman.

What Information Was Involved? Carole Hochman's investigation has revealed that the malicious code collected demographic and credit card information entered on our e-commerce site checkout page between March 1, 2015 and December 1, 2016. The information collected included the cardholder's name, shipping address, billing address, email address, card number, card type, expiration date, and CVV. If you were a registered user at our site, your login and password would also have been collected. All user passwords were changed in December after the discovery of the files.

What We Are Doing: We take this incident, and information security, very seriously at Carole Hochman. We are diligently investigating this incident, with the assistance of third-party forensic experts. We have removed the malicious code, and changed system account passwords so that credit and debit cards used to purchase products from our website after December 1, 2016 are not at risk. We are currently taking steps to further enhance the security of our systems to better protect

against future incidents of this kind. Additionally, we are providing written notice of this incident to those who may be impacted so that they can take steps to prevent possible fraud. We will also be notifying applicable state regulators about this incident.

What You Can Do: You can stay vigilant by reviewing your credit card statements for any suspicious charges. You can also review the enclosed Steps You Can Take to Protect Against Identity Theft and Fraud, which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft. If you use the same username and password at other sites, we recommend that you change the passwords for any other accounts you have that share the same username and or password.

For More Information: We sincerely regret any inconvenience or concern this incident may have caused you. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. You may call the assistance line at (844) 373-9985, Monday through Friday, 9:00 a.m. to 5:00 p.m. E.S.T (excluding U.S. holidays). You may also contact questions@carolehochman.com with questions or concerns regarding this incident.

Sincerely,

David Komar

David Komar
Principal

123456

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit 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.

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

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
https://www.freeze.equifax.com		

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service

Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. **For Rhode Island residents**, Attorney General can be contacted at (401) 274-4400, http://www.riag.ri.gov/, or 150 South Main Street, Providence, RI 02903. Approximately 73 Rhode Island residents may be impacted by this incident. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or 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 they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.