



SIDLEY AUSTIN LLP
 1501 K STREET, N.W.
 WASHINGTON, D.C. 20005
 +1 202 736 8000
 +1 202 736 8711 FAX

ctbrown@sidley.com
 +1 202 736 8465

BEIJING	HONG KONG	SHANGHAI
BOSTON	HOUSTON	SINGAPORE
BRUSSELS	LONDON	SYDNEY
CENTURY CITY	LOS ANGELES	TOKYO
CHICAGO	NEW YORK	WASHINGTON, D.C.
DALLAS	PALO ALTO	
GENEVA	SAN FRANCISCO	

FOUNDED 1866

May 15, 2017

RECEIVED

MAY 16 2017

CONSUMER PROTECTION

The Honorable Gordon MacDonald
 New Hampshire Department of Justice
 33 Capitol Street
 Concord, New Hampshire 03301

Dear Attorney General MacDonald:

We write on behalf of our client the University of New Mexico Foundation (the "Foundation") to inform you of a data security incident involving the personal information maintained by the Foundation. This includes information of one annuitant, business information of one vendor, and donation information of thirty-three donors that are New Hampshire residents.

In mid-April, 2017, the Foundation discovered that an unauthorized individual had gained access to the Foundation's network through an account with its managed services provider. While the investigation is ongoing, the Foundation understands that the intrusion through the managed services provider's credentials may have began on or around February 16, 2017. With the managed services provider's administrative privileges, the unauthorized individual may have had access to certain systems that contained personal information of the Foundation's employees, annuitants, vendors, and donors.

The Foundation, with assistance from the managed services provider, took immediate steps to lock down the impacted server and terminate the intruder's access. The Foundation also began an investigation to understand the scope of the incident, reported the incident to federal law enforcement and is fully cooperating with their investigation.

Information that may have been available include names, contact information, social security numbers and/or EINs, dates of birth, bank account and routing numbers, and other information maintained for employment purposes, for vendor business purposes, or for annuitant accounts. Donor information that may have been available includes names, contact information, donation amount, and the checking and routing information displayed on donation checks.

The investigation is ongoing. On May 15, 2017, the Foundation is providing notification to approximately 23,000 of its employees, vendors, annuitants, and donors out of an abundance of caution because their personal information was available through the affected systems. This includes one annuitant, one vendor, and thirty-three donors that are New Hampshire residents. As a precautionary measure, the Foundation is also providing one year of credit monitoring and identity theft protection services to potentially affected individuals through AllClear ID, as described in the attached sample notice letter.



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

Respectfully submitted,

Colleen Theresa Brown

Colleen Theresa Brown



FOUNDATION

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 15, 2017

NOTICE OF DATA BREACH

Dear John Sample,

We are writing to tell you about a situation that may have exposed some of your personal information. We take the protection of your information very seriously and are contacting you directly to explain the circumstances, steps we are taking in response, and resources we are making available to you.

What Happened?

In mid-April, 2017, we discovered that an unauthorized individual had gained access to our network through an account with our security services provider. This unauthorized individual may have had access to certain systems that contained personal information of our donors. While our investigation is ongoing, we are providing this notice out of an abundance of caution to alert you to the incident because information about you was available through the affected system.

What Information Was Involved?

Information that may have been available includes names, contact information, donation amount, and the checking and routing information displayed on your donation checks. While this information should not typically be sufficient to grant access to your accounts with your financial institutions, we place a high priority on the confidentiality of our donor information, and wanted to alert you to this incident so that you may be vigilant against phishing attempts or other fraudulent requests, and to monitor your accounts for any suspicious activity.

What We Are Doing.

Upon discovery of the incident, the Foundation and its security provider immediately took steps to secure the system and block the intruder's access, and began an investigation to understand the scope of the incident. That investigation is still ongoing. The Foundation also reported the incident to federal law enforcement and is fully cooperating with their investigation.

What You Can Do.

We want to make you aware of steps you may take to guard against potential identity theft or fraud. Please review the enclosed Information about Identity Theft Protection about what you can do.

As an added precaution, we have arranged to have AllClear ID provide credit monitoring and identity repair services for twelve months at no cost to you. AllClear ID is a leading national provider of cyber security and identity theft protection services. The AllClear ID identity repair services require no further action and you may use them at any time during the next twelve months. You must take additional steps to sign up for credit monitoring.

Please be advised that this credit monitoring is being offered out of an abundance of caution to comply with guidance in certain states, and is not intended to suggest that recipients of the offer are at any substantial risk of harm.



01-03-1-00

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-412-7152 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: You must take additional steps to sign up for credit monitoring. This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-877-412-7152 using the following redemption code: Redemption Code. You will need to expressly authorize AllClear ID to activate credit monitoring. This includes providing AllClear ID with your redemption code and verifying your identity.

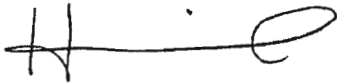
Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

For More Information.

Please know that, as a friend of the University and the Foundation, your wellbeing and safety are important to us. We take the security and confidentiality of our donor information seriously. If you have further questions or concerns about this incident, you can find more information by calling our hotline at 1-877-412-7152.

We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

A handwritten signature in black ink, appearing to read "H. Nemcik". The signature is fluid and cursive, with a large loop at the end.

Henry Nemcik
President and Chief Executive Officer
UNM Foundation
Two Woodward Ctr
700 Lomas NE, Ste 108
Albuquerque, NM 87102

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

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.

Federal Trade Commission, Identity Theft Clearinghouse

600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov and www.ftc.gov/idtheft. You can also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.pdf>.

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/idtheft/index.htm
Or contact the Identity Theft Unit directly:
2000 St. Paul Place, 16th Floor, Baltimore, MD 21202, 410-567-6491

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

For residents of Vermont: You may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <http://www.atg.state.vt.us>.

Suggestions if You Are a Victim of Identity Theft:

- *File a police report.* Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- *Contact the U.S. Federal Trade Commission (FTC).* The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.
- *Keep a record of your contacts.* Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity



theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In other situations, the cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.*

Because the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below.

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Twelve months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for twelve months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - o Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
 - o Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------



FOUNDATION

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00002
ACD1234

21928
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 15, 2017

NOTICE OF DATA BREACH

Dear John Sample,

We are writing to tell you about a situation that may have exposed some of your personal information. We take the protection of your information very seriously and are contacting you directly to explain the circumstances, steps we are taking in response, and resources we are making available to you.

What Happened?

In mid-April, 2017, we discovered that an unauthorized individual had gained access to our network through an account with our security services provider. This unauthorized individual may have had access to certain systems that contained your personal information. While our investigation is ongoing, we are providing this notice out of an abundance of caution to alert you to the incident because information about you was available through the affected system.

What Information Was Involved?

Information that may have been available includes names, contact information, Social Security numbers and/or EINs, date of birth, bank account and routing numbers, and other information maintained for employment purposes or to support your employer, annuitant or business relationship with the University of New Mexico Foundation.

What We Are Doing.

Upon discovery of the incident, the Foundation and its security provider immediately took steps to secure the system and block the intruder's access, and began an investigation to understand the scope of the incident. That investigation is still ongoing. The Foundation also reported the incident to federal law enforcement and is fully cooperating with their investigation.

What You Can Do.

We want to make you aware of steps you may take to guard against potential identity theft or fraud. Please review the enclosed Information about Identity Theft Protection about what you can do.

As an added precaution, we have arranged to have AllClear ID provide credit monitoring and identity repair services for twelve months at no cost to you. AllClear ID is a leading national provider of cyber security and identity theft protection services. The AllClear ID identity repair services require no further action and you may use them at any time during the next twelve months. You must take additional steps to sign up for credit monitoring.

Please be advised that this credit monitoring is being offered out of an abundance of caution to comply with guidance in certain states, and is not intended to suggest that recipients of the offer are at any substantial risk of harm.



01-03-2-00

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-412-7152 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: You must take additional steps to sign up for credit monitoring. This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-877-412-7152 using the following redemption code: Redemption Code. You will need to expressly authorize AllClear ID to activate credit monitoring. This includes providing AllClear ID with your redemption code and verifying your identity.

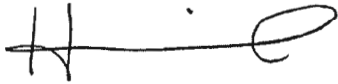
Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

For More Information.

Please know that, as a friend of the University and the Foundation, your wellbeing and safety are important to us. We take the security and confidentiality of your information seriously. If you have further questions or concerns about this incident, you can find more information by calling our hotline at 1-877-412-7152.

We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

A handwritten signature in black ink, appearing to read "H. Nemcik". The signature is fluid and cursive, with a large loop at the end.

Henry Nemcik
President and Chief Executive Officer
UNM Foundation
Two Woodward Ctr
700 Lomas NE, Ste 108
Albuquerque, NM 87102

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

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.

Federal Trade Commission, Identity Theft Clearinghouse

600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov and www.ftc.gov/idtheft You can also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.pdf>.

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/idtheft/index.htm
Or contact the Identity Theft Unit directly:
2000 St. Paul Place, 16th Floor, Baltimore, MD 21202, 410-567-6491

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

For residents of Vermont: You may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <http://www.atg.state.vt.us>.

Suggestions if You Are a Victim of Identity Theft:

- *File a police report.* Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- *Contact the U.S. Federal Trade Commission (FTC).* The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.
- *Keep a record of your contacts.* Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity



theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In other situations, the cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.*

Because the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Twelve months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for twelve months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
 - o Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
 - o Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------