Southcentral Foundation

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

00001
00001
ACD1234
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

December 16, 2016

RE: Notice of Cyber Security Incident

Dear John Sample:

You are receiving this letter as part of Southcentral Foundation's (SCF) commitment to privacy. SCF takes customer-owner privacy very seriously and wants to ensure that you are made fully aware of a privacy and security incident regarding your protected health information.

What Happened? On October 18, 2016, SCF became aware that some employee email accounts might be accessible to persons outside the organization as a result of a cyber security attack.

What Action Was Taken By SCF? SCF immediately began to investigate the circumstances around the cyber security attack, in order to determine what happened and who may have been impacted. SCF engaged external computer forensic experts to assist with its investigation. The investigation determined that two SCF employees' email accounts were subject to unauthorized access. One email account was vulnerable from October 17, 2016 to October 18, 2016. The other email account was vulnerable from October 14, 2016 to October 18, 2016. As soon as SCF became aware the accounts were vulnerable, it disabled them to stop any further access.

What Information Was Involved? SCF reviewed the information in the email accounts and determined the accounts included, among other information, the protected health information of some SCF customer-owners. The information in the email accounts may include a combination of the following types of information related to you:

- Full name
- Medical record number
- Date of birth and age
- Address
- Phone number
- Social Security number
- Medicaid ID number
- Photographs
- Diagnosis information
- Treatment information
- Dates of service
- Provider name

Medical history
Tribal identification/membership card
Birth certificates
Health status information
Family members' names, relationships and phone numbers

What Is SCF Doing? SCF is working diligently to protect the privacy of its customer-owners and continues to investigate this incident.

SCF is sending you this notice because your protected health information may be at risk as a result of this incident. As an added precaution, SCF has established an account with AllClear ID that will protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-220-9457 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: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. 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 1-855-220-9457 using the following redemption code: Redemption Code.

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

What Can You Do? Please review the enclosed *Steps You Can Take To Protect Against Identity Theft And Fraud*, which provides the contact information of the major credit reporting agencies and government resources where you can obtain more information about fraud alerts and credit freezes. In addition, you can also enroll to receive the free credit monitoring and identity restoration services through AllClear ID.

The SCF Board of Directors, leadership and staff take the privacy and security of customer-owners' protected health information seriously and sincerely regret any inconvenience this situation may cause. SCF is taking appropriate action in an effort to prevent an incident like this from reoccurring. If you have any questions or concerns, you may contact our dedicated hotline at 1-855-220-9457, 5 a.m. to 5 p.m. Alaska Standard Time, Monday through Saturday (excluding U.S. holidays) or email SCF Corporate Compliance Department at scfcorporatecompliance@scf.cc.

Sincerely,

SOUTHCENTRAL FOUNDATION

Denise R. Morris

Denise R. Morris
Director, Corporate Compliance

Enclosure

STEPS YOU CAN TAKE TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your account statements, explanation of benefits forms, and monitoring your credit reports for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

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

At no charge, you can also have these credit bureaus place a "fraud alert" on your credit file. A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

You can also place a "security freeze" on your credit file that prohibits a credit reporting agency from releasing any information from your credit report without your written authorization, but it may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, the credit reporting agency cannot charge to place, lift or remove a security freeze. In all other cases, a credit agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. If you incur a cost to place a security freeze, please let us know. You must contact each of the credit reporting agencies separately to place a security freeze on your credit file:

Equifax Security Freeze	Experian Security Freeze	TransUnion LLC
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-685-1111	888-397-3742	888-909-8862
800-349-9960 (NY Residents)	www.experian.com/freeze/	freeze.transunion.com
www.freeze.equifax.com	center.html	

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. The FTC can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You have the right to file a police report if you 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 you have been a victim of identity theft. **Maryland residents** may contact the MD Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, www.oag.state.md.us, or 200 St. Paul Place, Baltimore, MD 21202. **North Carolina residents** may contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, www.ncdoj.com, or 9001 Mail Service Center, Raleigh, NC 27699. This notice was not delayed as a result of a law enforcement notification.

Southcentral Foundation

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

00002
ACD1234

07286
TO THE ESTATE OF JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

December 16, 2016

RE: Notice of Cyber Security Incident

To the Estate of John Sample:

You are receiving this letter as part of Southcentral Foundation's (SCF) commitment to privacy. SCF takes customer-owner privacy very seriously and wants to ensure that you are made fully aware of a privacy and security incident regarding your protected health information.

What Happened? On October 18, 2016, SCF became aware that some employee email accounts might be accessible to persons outside the organization as a result of a cyber security attack.

What Action Was Taken By SCF? SCF immediately began to investigate the circumstances around the cyber security attack, in order to determine what happened and who may have been impacted. SCF engaged external computer forensic experts to assist with its investigation. The investigation determined that two SCF employees' email accounts were subject to unauthorized access. One email account was vulnerable from October 17, 2016 to October 18, 2016. The other email account was vulnerable from October 14, 2016 to October 18, 2016. As soon as SCF became aware the accounts were vulnerable, it disabled them to stop any further access.

What Information Was Involved? SCF reviewed the information in the email accounts and determined the accounts included, among other information, the protected health information of some SCF customer-owners. The information in the email accounts may include a combination of the following types of information related to you:

Full name
Medical record number
Date of birth and age
Address
Phone number
Social Security number
Medicaid ID number
Photographs
Diagnosis information
Treatment information
Dates of service
Provider name

Medical history
Tribal identification/membership card
Birth certificates
Health status information
Family members' names, relationships and phone numbers

What Is SCF Doing? SCF is working diligently to protect the privacy of its customer-owners and continues to investigate this incident.

SCF is sending you this notice because your protected health information may be at risk as a result of this incident. As an added precaution, SCF has established an account with AllClear ID that will protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-220-9457 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: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. 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 1-855-220-9457 using the following redemption code: Redemption Code.

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

What Can You Do? Please review the enclosed *Steps You Can Take To Protect Against Identity Theft And Fraud*, which provides the contact information of the major credit reporting agencies and government resources where you can obtain more information about fraud alerts and credit freezes. In addition, you can also enroll to receive the free credit monitoring and identity restoration services through AllClear ID.

The SCF Board of Directors, leadership and staff take the privacy and security of customer-owners' protected health information seriously and sincerely regret any inconvenience this situation may cause. SCF is taking appropriate action in an effort to prevent an incident like this from reoccurring. If you have any questions or concerns, you may contact our dedicated hotline at 1-855-220-9457, 5 a.m. to 5 p.m. Alaska Standard Time, Monday through Saturday (excluding U.S. holidays) or email SCF Corporate Compliance Department at scfcorporatecompliance@scf.cc.

Sincerely,

SOUTHCENTRAL FOUNDATION

Denise R. Morris

Denise R. Morris
Director, Corporate Compliance

Enclosure

STEPS YOU CAN TAKE TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your account statements, explanation of benefits forms, and monitoring your credit reports for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

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

At no charge, you can also have these credit bureaus place a "fraud alert" on your credit file. A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

You can also place a "security freeze" on your credit file that prohibits a credit reporting agency from releasing any information from your credit report without your written authorization, but it may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, the credit reporting agency cannot charge to place, lift or remove a security freeze. In all other cases, a credit agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. If you incur a cost to place a security freeze, please let us know. You must contact each of the credit reporting agencies separately to place a security freeze on your credit file:

Equifax Security Freeze	Experian Security Freeze	TransUnion LLC
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-685-1111	888-397-3742	888-909-8862
800-349-9960 (NY Residents)	www.experian.com/freeze/	freeze.transunion.com
www.freeze.equifax.com	center.html	

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. The FTC can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You have the right to file a police report if you 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 you have been a victim of identity theft. **Maryland residents** may contact the MD Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, www.oag.state.md.us, or 200 St. Paul Place, Baltimore, MD 21202. **North Carolina residents** may contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, www.ncdoj.com, or 9001 Mail Service Center, Raleigh, NC 27699. This notice was not delayed as a result of a law enforcement notification.

Southcentral Foundation

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

07302
TO THE PARENT OR GUARDIAN OF
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

00003
ACD1234

December 16, 2016

RE: Notice of Cyber Security Incident

Dear Parent or Guardian of John Sample:

You are receiving this letter as part of Southcentral Foundation's (SCF) commitment to privacy. SCF takes customer-owner privacy very seriously and wants to ensure that you are made fully aware of a privacy and security incident regarding your protected health information.

What Happened? On October 18, 2016, SCF became aware that some employee email accounts might be accessible to persons outside the organization as a result of a cyber security attack.

What Action Was Taken By SCF? SCF immediately began to investigate the circumstances around the cyber security attack, in order to determine what happened and who may have been impacted. SCF engaged external computer forensic experts to assist with its investigation. The investigation determined that two SCF employees' email accounts were subject to unauthorized access. One email account was vulnerable from October 17, 2016 to October 18, 2016. The other email account was vulnerable from October 14, 2016 to October 18, 2016. As soon as SCF became aware the accounts were vulnerable, it disabled them to stop any further access.

What Information Was Involved? SCF reviewed the information in the email accounts and determined the accounts included, among other information, the protected health information of some SCF customer-owners. The information in the email accounts may include a combination of the following types of information related to you:

Full name
Medical record number
Date of birth and age
Address
Phone number
Social Security number
Medicaid ID number
Photographs
Diagnosis information
Treatment information
Dates of service
Provider name

Medical history
Tribal identification/membership card
Birth certificates
Health status information
Family members' names, relationships and phone numbers

What Is SCF Doing? SCF is working diligently to protect the privacy of its customer-owners and continues to investigate this incident.

SCF is sending you this notice because your protected health information may be at risk as a result of this incident. As an added precaution, SCF has established an account with AllClear ID that will protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-220-9457 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: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. 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 1-855-220-9457 using the following redemption code: Redemption Code.

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

What Can You Do? Please review the enclosed *Steps You Can Take To Protect Against Identity Theft And Fraud*, which provides the contact information of the major credit reporting agencies and government resources where you can obtain more information about fraud alerts and credit freezes. In addition, you can also enroll to receive the free credit monitoring and identity restoration services through AllClear ID.

The SCF Board of Directors, leadership and staff take the privacy and security of customer-owners' protected health information seriously and sincerely regret any inconvenience this situation may cause. SCF is taking appropriate action in an effort to prevent an incident like this from reoccurring. If you have any questions or concerns, you may contact our dedicated hotline at 1-855-220-9457, 5 a.m. to 5 p.m. Alaska Standard Time, Monday through Saturday (excluding U.S. holidays) or email SCF Corporate Compliance Department at scfcorporatecompliance@scf.cc.

Sincerely,

SOUTHCENTRAL FOUNDATION

Denise R. Morris

Denise R. Morris
Director, Corporate Compliance

Enclosure

STEPS YOU CAN TAKE TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your account statements, explanation of benefits forms, and monitoring your credit reports for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

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

At no charge, you can also have these credit bureaus place a "fraud alert" on your credit file. A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

You can also place a "security freeze" on your credit file that prohibits a credit reporting agency from releasing any information from your credit report without your written authorization, but it may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit reporting agency with a valid police report, the credit reporting agency cannot charge to place, lift or remove a security freeze. In all other cases, a credit agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. If you incur a cost to place a security freeze, please let us know. You must contact each of the credit reporting agencies separately to place a security freeze on your credit file:

Equifax Security Freeze	Experian Security Freeze	TransUnion LLC
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-685-1111	888-397-3742	888-909-8862
800-349-9960 (NY Residents)	www.experian.com/freeze/	freeze.transunion.com
www.freeze.equifax.com	center.html	

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them. The FTC can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You have the right to file a police report if you 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 you have been a victim of identity theft. **Maryland residents** may contact the MD Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, www.oag.state.md.us, or 200 St. Paul Place, Baltimore, MD 21202. **North Carolina residents** may contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, www.ncdoj.com, or 9001 Mail Service Center, Raleigh, NC 27699. This notice was not delayed as a result of a law enforcement notification.

Southcentral Foundation Takes Measures to Protect Customer-Owner Information from Cyber Security Attack

As part of Southcentral Foundation's (SCF) commitment to customer-owner privacy, SCF provided notice of a privacy and security issue regarding certain patients' protected health information on Dec. 16, 2016.

What Happened? On Oct. 18, 2016 SCF became aware that some employee email accounts might be accessible to persons outside the organization as a result of a cyber security attack.

What Action Was Taken by SCF? SCF immediately began to investigate the circumstances around the cyber security attack, in order to determine what happened and who may have been impacted. SCF engaged external computer forensic experts to assist with its investigation. The investigation determined that two SCF employee email accounts were subject to unauthorized access. One email account was vulnerable from Oct. 17-18, 2016. The other email account was vulnerable from Oct. 14-18, 2016. As soon as SCF became aware the accounts were vulnerable, it disabled them to stop any further access.

What Information Was Involved? SCF reviewed the information in the email accounts and determined the accounts included, among other information, the protected health information of some SCF customer-owners. The information in the email accounts may include a combination of the following types of information for impacted customer-owners:

- Full name
- Medical record number
- Date of birth and age
- Address
- Phone number
- Social Security number
- Medicaid ID number
- Photographs
- Diagnosis information
- Treatment information
- Dates of service
- Provider name
- Medical history
- Tribal identification/Membership card
- Birth certificates
- Health status information
- Family members' names, relationships, and phone numbers

What is SCF Doing? SCF is working diligently to protect the privacy of its customer-owners and continues to investigate this incident.

SCF has sent notice to all individuals whose protected health information may be at risk as a result of this incident. As an added precaution, SCF is offering all potentially impacted individuals access to credit monitoring and identity theft protection services with AllClear ID.

What Can You Do? Please review the *Steps You Can Take To Protect Against Identity Theft and Fraud*, which provides the contact information of the major credit reporting agencies and government resources where you can obtain more information about fraud alerts and credit freezes. In addition, those who are impacted can also enroll to receive the free credit monitoring and identity restoration services through AllClear ID.

The SCF Board of Directors, leadership, and staff take the privacy and security of customer-owners' protected health information seriously and sincerely regret any inconvenience this situation may cause. SCF is taking appropriate action in an effort to prevent an incident like this from reoccurring. If you have any questions or concerns, you may contact SCF's dedicated hotline at 1-855-220-9457, 5 a.m. to 5 p.m. Alaska Standard Time, Monday through Saturday (excluding U.S. holidays) or email SCF's Corporate Compliance Department at scfcorporatecompliance@scf.cc.

STEPS YOU CAN TAKE TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

While SCF continues to investigate, customer-owners may take direct action to further protect against possible identity theft or financial loss.

SCF encourages customer-owners to remain vigilant against incidents of identity theft and financial loss by reviewing account statements, explanation of benefits forms, and monitoring credit reports for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-680-7289
www.transunion.com

At no charge, customer-owners can also have these credit bureaus place a "fraud alert" on their credit file. A "fraud alert" will tell creditors to take additional steps to verify a customer-owner's identity prior to granting credit in the customer-owner's name; however, because it tells creditors to follow certain procedures to protect the customer-owner, it may also delay the customer-owner's ability to obtain credit while the credit bureaus verify the customer-owner's identity. As soon as one credit bureau confirms the fraud alert, the others are notified to place fraud alerts on the customer-owner's files. Customer-owners may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on their credit report.

Customer-owners can also place a "security freeze" on their credit file to prohibit a credit reporting agency from releasing any information from their credit report without their written authorization, but it may delay, interfere with, or prevent the timely approval of any requests for new credit. If a customer-owner has been a victim of identity theft and provides the credit reporting agency with a valid police report, the credit reporting agency cannot charge to place, lift, or remove a security freeze. In all other cases, a credit agency may charge a fee to place, temporarily lift, or permanently remove a security freeze. Customer-owners must contact each of the credit reporting agencies separately to place a security freeze on their credit file:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
1-800-685-1111
800-349-9960 (NY Residents)

Experian Security Freeze
PO Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion LLC
PO Box 2000
Chester, PA 19022
1-888-909-8862

www.freeze.equifax.com	www.experian.com/freeze/center.html	www.freeze.transunion.com

Customer-owners can further educate themselves regarding identity theft, fraud alerts, security freezes, and the steps they can take to protect themselves by contacting the state attorney general or the Federal Trade Commission (FTC). The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

Instances of known or suspected identity theft should be reported to law enforcement, the state attorney general, and the FTC. Customer-owners have the right to file a police report if they experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, customer-owners will likely need to provide some kind of proof that they have been a victim of identity theft. **Maryland residents** may contact the MD Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, www.oag.state.md.us, or 200 St. Paul Place, Baltimore, MD 21202. **North Carolina residents** may contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, www.ncdoj.com, or 9001 Mail Service Center, Raleigh, NC 27699.

This notice was not delayed as a result of a law enforcement notification.