Meepos & Company

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

00001
ACD1234

00001
JOHN
SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

July 3, 2017

Re: Notice of Data Breach

Dear John:

We are writing to make you aware of a recent data privacy incident that may affect the security of some of your information. You are receiving this notice because you are a partner or shareholder in a ***business*** entity for which you receive a K-1. **We have not been made aware of any misuse of personal information besides the fraudulent filing of certain individual tax returns using information from *individual* tax clients**. While your information is located in a module of our tax software for which there is no evidence of access, we take this incident very seriously and, in an abundance of caution, we are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? On May 19, 2017, Meepos & Company ("Meepos") received reports of issues with certain clients' 2016 tax filings. Meepos immediately launched an investigation and has been working diligently, with the assistance of third party forensic investigators, to determine what caused the issues and whether other clients may be affected. Through the investigation, Meepos determined that an unauthorized actor or actors gained access to certain parts of Meepos's network due to a misconfiguration of our two-factor password authentication and, as a result, may have had access to personal information for certain Meepos clients in our tax filing system, including documents that may be associated with our business client tax filings. After discovering the unauthorized access, we immediately worked with our IT professionals to identify the access point, quarantined the affected system and completed enterprise wide password changes to better prevent further unauthorized access to our systems. We also immediately contacted the IRS to alert them of the situation in order to stop the issuance of any fraudulent refunds. The investigation has determined that the unauthorized actor(s) may have had access to Meepos's system beginning on February 24, 2017, although the first known access to tax information and fraudulent filings did not occur until May 2017.

What Information Was Involved? The information relating to you that was present on the affected systems would be located in documents attached to your business' tax filings and may include the following categories of information: (1) name; (2) address; and (3) Social Security number or employer identification number.

What We Are Doing. We consulted with specialists in the data privacy and security field, including computer forensic experts, to assist in our investigation. We continue to work closely with them to better understand and appropriately respond to the incident. We are working to guide all affected clients through the process of resolving any issues with their tax accounts and are in regular direct contact with the IRS. Additionally, we have reported this incident to state tax agencies, the FBI and will be notifying certain state Attorneys General as required by law. We work with third party IT professionals to ensure measures are in place to protect the security of information in our possession, including verification that our two-factor password authentication is properly functioning.

The confidentiality, privacy, and security of information in our systems is one of our highest priorities. In recent years we have implemented a number of additional security protocols with the assistance of our professional IT consultants such as installing software to encrypt email attachments containing sensitive data, requiring two-factor authentication on our computers and additional layers of passwords to access client information in software programs. We are incredibly discouraged that this intrusion happened despite our efforts. In discussions with our contact at the IRS, we have learned that this is part of a wide-reaching and ongoing epidemic affecting the entire accounting industry on a national level. CPA firms are contacting the IRS regarding similar incidents on a near daily basis. We vow to re-double our efforts as part of an ongoing commitment to the security of personal information in our care and are working with data security professionals to review our existing security measures and to implement additional safeguards.

As an added precaution, we are offering you access to 24 months of identity restoration and credit monitoring services through AllClear ID at no cost to you. We encourage you to enroll in these services, as we are not able to act on your behalf to do so. More information on the services being offered and information on how to enroll can be found in the enclosed "Steps You Can Take to Protection Your Information."

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information" for additional steps you can take to better protect against the potential misuse of your personal information. You can also enroll to receive the free credit monitoring and identity restoration services we are offering at no cost to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at 1-855-259-6476. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

RH Meepos

Robert Meepos, CPA
Managing Partner

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Credit Monitoring and Identity Restoration. As an added precaution, we have arranged to have AllClear ID protect your identity for 24 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 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-259-6476 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 1-855-259-6476 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.

We encourage you to enroll in the credit monitoring services we are offering, at no cost to you, as we are not able to act on your behalf to enroll you in the credit monitoring service.

Monitor Your Accounts.

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free 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.

Fraud Alerts. 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 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. 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. Fees vary based on where you live, but commonly range from $3 to $15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze/place-credit-freeze

Contact the IRS. You can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. 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); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Meepos is located at 409 Washington Blvd., Marina del Rey, California 90292.

For New Mexico residents, we encourage you to review your rights pursuant to the Fair Credit Reporting act by visiting: www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Meepos & Company

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

00827
00002
ACD1234
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

July 3, 2017

Re: Notice of Data Breach

Dear John Sample:

Following up on the preliminary notice we previously sent to your attention, we are writing to provide you with more information on the recent data privacy incident. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? On May 19, 2017, Meepos & Company ("Meepos") received reports of issues with certain clients' 2016 tax filings. Meepos immediately launched an investigation and has been working diligently, with the assistance of third party forensic investigators, to determine what caused the issues and whether other clients may be affected. Through the investigation, Meepos determined that an unauthorized actor or actors gained access to certain parts of Meepos's network due to a misconfiguration of our two-factor password authentication and, as a result, had access to information in our tax filing program, including your personal information. After discovering the unauthorized access, we immediately worked with our IT professionals to identify the access point, quarantined the affected system and completed enterprise wide password changes to better prevent further unauthorized access to our systems. We also immediately contacted the IRS to alert them of the situation in order to stop the issuance of any fraudulent refunds. The investigation has determined that the unauthorized actor(s) may have had access to Meepos's system beginning on February 24, 2017, although the first known access to tax information and fraudulent filings did not occur until May 2017.

What Information Was Involved? The information relating to you that was present on the affected systems may include the following categories of information: (1) name; (2) address; (3) Social Security number (4) wage/income information; (5) date of birth; and (6) bank account information if a specific account was provided for direct deposit or electronic payment purposes (bank account and routing number).

What We Are Doing. We consulted with specialists in the data privacy and security field, including computer forensic experts, to assist in our investigation. We continue to work closely with them to better understand and appropriately respond to the incident. We are working to guide all affected clients through the process of resolving any issues with their tax accounts and are in regular direct contact with the IRS. Additionally, we have reported this incident to state tax agencies, the FBI and will be notifying certain state Attorneys General as required by law. We work with third party IT professionals to ensure measures are in place to protect the security of information in our possession, including verification that our two-factor password authentication is properly functioning.

The confidentiality, privacy, and security of information in our systems is one of our highest priorities. In recent years we have implemented a number of additional security protocols with the assistance of our professional IT consultants such as installing software to encrypt email attachments containing sensitive data, requiring two-factor authentication on our computers and additional layers of passwords to access client information in software programs. We are incredibly

discouraged that this intrusion happened despite our efforts. In discussions with our contact at the IRS, we have learned that this is part of a wide-reaching and ongoing epidemic affecting the entire accounting industry on a national level. CPA firms are contacting the IRS regarding similar incidents on a near daily basis. We vow to re-double our efforts as part of an ongoing commitment to the security of personal information in our care and are working with data security professionals to review our existing security measures and to implement additional safeguards.

We have not been made aware of any misuse of personal information besides the fraudulent filing of certain individual tax returns in an attempt to collect refunds (which were largely unsuccessful, based on subsequent correspondence with the IRS). As an added precaution, we are offering you access to 24 months of identity restoration and credit monitoring services through AllClear ID at no cost to you. We encourage you to enroll in these services, as we are not able to act on your behalf to do so. More information on the services being offered and information on how to enroll can be found in the enclosed "Steps You Can Take to Protection Your Information."

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information" for additional steps you can take to better protect against the potential misuse of your personal information. You can also enroll to receive the free credit monitoring and identity restoration services we are offering at no cost to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at 1-855-259-6476. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

RH Meepos

Robert Meepos, CPA
Managing Partner

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Credit Monitoring and Identity Restoration. As an added precaution, we have arranged to have AllClear ID protect your identity for 24 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 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-259-6476 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 1-855-259-6476 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.

We encourage you to enroll in the credit monitoring services we are offering, at no cost to you, as we are not able to act on your behalf to enroll you in the credit monitoring service.

Monitor Your Accounts.

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free 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.

Fraud Alerts. 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 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. 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. Fees vary based on where you live, but commonly range from $3 to $15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze/place-credit-freeze

Contact the IRS. You can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. 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); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Meepos is located at 409 Washington Blvd., Marina del Rey, California 90292.

For New Mexico residents, we encourage you to review your rights pursuant to the Fair Credit Reporting act by visiting: www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Meepos & Company

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

00003
ACD1234

00975
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

July 3, 2017

Re: Notice of Data Breach

Dear John Sample:

We are writing to make you aware of a recent data privacy incident that may affect the security of some of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? On May 19, 2017, Meepos & Company ("Meepos") received reports of issues with certain clients' 2016 tax filings. Meepos immediately launched an investigation and has been working diligently, with the assistance of third party forensic investigators, to determine what caused the issues and whether other clients may be affected. Through the investigation, Meepos determined that an unauthorized actor or actors gained access to certain parts of Meepos's network due to a misconfiguration of our two-factor password authentication and, as a result, may have had access to personal information for certain Meepos clients in our tax filing system. After discovering the unauthorized access, we immediately worked with our IT professionals to identify the access point, quarantined the affected system and completed enterprise wide password changes to better prevent further unauthorized access to our systems. We also immediately contacted the IRS to alert them of the situation in order to stop the issuance of any fraudulent refunds. The investigation has determined that the unauthorized actor(s) may have had access to Meepos's system beginning on February 24, 2017, although the first known access to tax information and fraudulent filings did not occur until May 2017.

What Information Was Involved? Meepos has your data because one of our tax preparers utilized the Meepos accounting system to file your 2015 or 2016 tax return. The information relating to you that was present on the affected systems may include the following categories of information: (1) name; (2) address; (3) Social Security number (4) wage/income information; (5) date of birth; and (6) bank account information if a specific account was provided for direct deposit or electronic payment purposes (bank account and routing number).

What We Are Doing. We consulted with specialists in the data privacy and security field, including computer forensic experts, to assist in our investigation. We continue to work closely with them to better understand and appropriately respond to the incident. We are working to guide all affected clients through the process of resolving any issues with their tax accounts and are in regular direct contact with the IRS. Additionally, we have reported this incident to state tax agencies, the FBI and will be notifying certain state Attorneys General as required by law. We work with third party IT professionals to ensure measures are in place to protect the security of information in our possession, including verification that our two-factor password authentication is properly functioning.

The confidentiality, privacy, and security of information in our systems is one of our highest priorities. In recent years we have implemented a number of additional security protocols with the assistance of our professional IT consultants such as installing software to encrypt email attachments containing sensitive data, requiring two-factor authentication on our

computers and additional layers of passwords to access client information in software programs. We are incredibly discouraged that this intrusion happened despite our efforts. In discussions with our contact at the IRS, we have learned that this is part of a wide-reaching and ongoing epidemic affecting the entire accounting industry on a national level. CPA firms are contacting the IRS regarding similar incidents on a near daily basis. We vow to re-double our efforts as part of an ongoing commitment to the security of personal information in our care and are working with data security professionals to review our existing security measures and to implement additional safeguards.

We have not been made aware of any misuse of personal information besides the fraudulent filing of certain individual tax returns in an attempt to collect refunds (which were largely unsuccessful, based on subsequent correspondence with the IRS). As an added precaution, we are offering you access to 24 months of identity restoration and credit monitoring services through AllClear ID at no cost to you. We encourage you to enroll in these services, as we are not able to act on your behalf to do so. More information on the services being offered and information on how to enroll can be found in the enclosed "Steps You Can Take to Protection Your Information."

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information" for additional steps you can take to better protect against the potential misuse of your personal information. You can also enroll to receive the free credit monitoring and identity restoration services we are offering at no cost to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at 1-855-259-6476. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

RH Meepos

Robert Meepos, CPA
Managing Partner

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Credit Monitoring and Identity Restoration. As an added precaution, we have arranged to have AllClear ID protect your identity for 24 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 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-259-6476 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 1-855-259-6476 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.

We encourage you to enroll in the credit monitoring services we are offering, at no cost to you, as we are not able to act on your behalf to enroll you in the credit monitoring service.

Monitor Your Accounts.

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free 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.

Fraud Alerts. 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 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. 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. Fees vary based on where you live, but commonly range from $3 to $15. 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. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze/place-credit-freeze

Contact the IRS. You can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. 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); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Meepos is located at 409 Washington Blvd., Marina del Rey, California 90292.

For New Mexico residents, we encourage you to review your rights pursuant to the Fair Credit Reporting act by visiting: www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.