



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

April 12, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Harrison, Mauro, & Morgan, P.A. (“HMM”) located at 568 High Street Burlington, NJ 08016, and are writing to notify your office of an incident that may affect the security of certain personal information relating to seven (7) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, HMM does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

In February 2022, HMM became aware that an unusual number of tax returns were getting rejected by the Internal Revenue Service (“IRS”). In response, HMM launched an investigation, with the assistance of a third-party information technology (“IT”) specialist, which determined that an unauthorized actor gained accessed to their external cloud storage system. An extensive scan was done of HMM’s internal systems and there were no indications of any unauthorized access. HMM then commenced an extensive review of the files stored on that system to determine whether sensitive information may have been present there at the time of the incident. On March 21, 2022, the investigation confirmed that the system contained sensitive information.

The information that could have been subject to unauthorized access includes name, and Social Security number.

Notice to Maryland Residents

On or about April 12, 2022, HMM began providing written notice of this incident to seven (7) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, HMM moved quickly to investigate and respond to the incident, assess the security of HMM systems, and identify potentially affected individuals. Further, HMM notified the IRS and all relevant state tax authorities regarding the event. HMM is providing access to credit monitoring services for 1 year, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

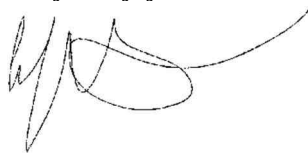
Additionally, HMM is providing impacted individuals with guidance on how to better protect against identity theft and fraud. HMM is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

HMM is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

A handwritten signature in black ink, appearing to read 'GJB', with a long, sweeping horizontal line extending to the right.

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB /mep
Enclosure

EXHIBIT A



Return to IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 12, 2022

<<Variable Header – CA Only>>

Dear <<First Name>> <<Last Name>>,

Harrison, Mauro, & Morgan P.A. is writing to inform you of a recent data privacy event that may involve some of your personal information. We take this event seriously and are providing you with information about the event and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? In February 2022, Harrison, Mauro, & Morgan became aware that an unusual number of tax returns were getting rejected by the Internal Revenue Service (“IRS”). In response, Harrison, Mauro, & Morgan launched an investigation, with the assistance of a third-party information technology (“IT”) specialist, which determined that an unauthorized actor gained access to their external cloud storage system. An extensive scan was done of Harrison, Mauro, & Morgan’s internal systems and there were no indications of any unauthorized access. Harrison, Mauro, & Morgan then commenced an extensive review of the files stored on that system to determine whether sensitive information may have been present there at the time of the incident. On March 21, 2022, the investigation confirmed that the system contained sensitive information.

What Information Was Involved? The information involved was limited to 2020 tax return information including your Name, <<Data Elements>>. As stated above, some tax returns have been rejected by the IRS as duplicate returns because of this incident. To date, we are unaware of any other attempted misuse of this information as a result of this incident and are sending this notice out of an abundance of caution.

What We Are Doing in Response? The security of information in our care is among our highest priorities. In addition to launching an internal investigation into this incident, we are reviewing our existing policies and procedures and will implement additional safeguards, as needed. In an abundance of caution, we are notifying you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. Additionally, we are offering you access to complimentary credit monitoring, fraud consultation, and identity theft restoration services through IDX.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity. You may also review the information contained in the attached “Steps You Can Take to Protect Personal Information.” There you will also find more information on the 12 months of credit monitoring and identity protection services we are making available to you. While Harrison, Mauro, & Morgan will cover the cost of these services, you will need to complete the activation process.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-903-3648, Monday through Friday, 9 am – 9 pm Eastern Time.

Sincerely,

A handwritten signature in dark ink that reads "Harrison, Mauro + Morgan, CPAs". The script is cursive and fluid, with the company name written in a slightly larger and more formal hand than the first name.

Harrison, Mauro, & Morgan

(Enclosure)



STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time. Please note the deadline to enroll is July 12, 2022.

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

May 24, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

Our office represents Harrison, Mauro, & Morgan, P.A. (“HMM”) located at 568 High Street Burlington, NJ 08016. We write to supplement the April 12, 2022 notice to your office concerning an incident that may affect the privacy of personal information related to certain Maryland residents. Our prior submission is attached as ***Exhibit A***. By providing this notice, HMM does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Since providing the initial notice, HMM continued its extensive internal review of the files that may have been subject to unauthorized access. HMM has now completed its review and identified all individuals that could have been impacted by the incident. On May 24th, HMM provided notice of this incident to an additional five (5) Maryland residents. The information related to these residents includes name, and Social Security number. Notice is being provided in substantially the same form as the letter attached as ***Exhibit B***.

HMM is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for 24 months, through IDX at no cost to the individuals. Additionally, HMM is providing impacted individuals with guidance on how to better protect against identity theft and fraud. HMM is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and

Office of the Attorney General

May 24, 2022

Page 2

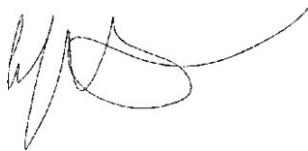
monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

HMM is providing written notice of this incident to relevant state regulators, as necessary, and has provided notice to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

A handwritten signature in black ink, appearing to read 'GJB', with a long, sweeping horizontal line extending to the right.

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB /mep

Enclosure

EXHIBIT A

From: Tony Alvarez
Sent: Tuesday, April 12, 2022 4:35 PM
To: idtheft@oag.state.md.us
Cc: John Mullen; Gregory Bautista; Marybeth Peluzzo
Subject: Harrison, Mauro & Morgan, P.A. - Notice of Data Event - MD
Attachments: HM&M - Notice of Data Event - MD.docx.PDF

Dear Sir or Madam,

Please see attached notice of data event.

Regards,
Tony

Tony Alvarez
Attorney
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, PA 19333
(267) 930-1710 - Office
(484) 226-5253 - Mobile
talvarez@mullen.law
<https://www.mullen.law/>

This email may be an attorney-client communication or otherwise confidential and privileged. If you are not the intended recipient, or received it in error, do not review or copy. Please immediately notify the sender and permanently delete/destroy the email and attachments.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

April 12, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Harrison, Mauro, & Morgan, P.A. (“HMM”) located at 568 High Street Burlington, NJ 08016, and are writing to notify your office of an incident that may affect the security of certain personal information relating to seven (7) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, HMM does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

In February 2022, HMM became aware that an unusual number of tax returns were getting rejected by the Internal Revenue Service (“IRS”). In response, HMM launched an investigation, with the assistance of a third-party information technology (“IT”) specialist, which determined that an unauthorized actor gained access to their external cloud storage system. An extensive scan was done of HMM’s internal systems and there were no indications of any unauthorized access. HMM then commenced an extensive review of the files stored on that system to determine whether sensitive information may have been present there at the time of the incident. On March 21, 2022, the investigation confirmed that the system contained sensitive information.

The information that could have been subject to unauthorized access includes name, and Social Security number.

Notice to Maryland Residents

On or about April 12, 2022, HMM began providing written notice of this incident to seven (7) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, HMM moved quickly to investigate and respond to the incident, assess the security of HMM systems, and identify potentially affected individuals. Further, HMM notified the IRS and all relevant state tax authorities regarding the event. HMM is providing access to credit monitoring services for 1 year, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

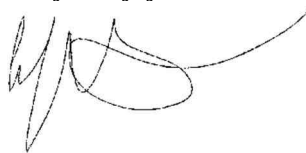
Additionally, HMM is providing impacted individuals with guidance on how to better protect against identity theft and fraud. HMM is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

HMM is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

A handwritten signature in black ink, appearing to read 'GJB', with a long, sweeping horizontal line extending to the right.

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB /mep
Enclosure

EXHIBIT A

To the April 12, 2022 notice



Return to IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 12, 2022

<<Variable Header – CA Only>>

Dear <<First Name>> <<Last Name>>,

Harrison, Mauro, & Morgan P.A. is writing to inform you of a recent data privacy event that may involve some of your personal information. We take this event seriously and are providing you with information about the event and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? In February 2022, Harrison, Mauro, & Morgan became aware that an unusual number of tax returns were getting rejected by the Internal Revenue Service (“IRS”). In response, Harrison, Mauro, & Morgan launched an investigation, with the assistance of a third-party information technology (“IT”) specialist, which determined that an unauthorized actor gained access to their external cloud storage system. An extensive scan was done of Harrison, Mauro, & Morgan’s internal systems and there were no indications of any unauthorized access. Harrison, Mauro, & Morgan then commenced an extensive review of the files stored on that system to determine whether sensitive information may have been present there at the time of the incident. On March 21, 2022, the investigation confirmed that the system contained sensitive information.

What Information Was Involved? The information involved was limited to 2020 tax return information including your Name, <<Data Elements>>. As stated above, some tax returns have been rejected by the IRS as duplicate returns because of this incident. To date, we are unaware of any other attempted misuse of this information as a result of this incident and are sending this notice out of an abundance of caution.

What We Are Doing in Response? The security of information in our care is among our highest priorities. In addition to launching an internal investigation into this incident, we are reviewing our existing policies and procedures and will implement additional safeguards, as needed. In an abundance of caution, we are notifying you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. Additionally, we are offering you access to complimentary credit monitoring, fraud consultation, and identity theft restoration services through IDX.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity. You may also review the information contained in the attached “Steps You Can Take to Protect Personal Information.” There you will also find more information on the 12 months of credit monitoring and identity protection services we are making available to you. While Harrison, Mauro, & Morgan will cover the cost of these services, you will need to complete the activation process.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-903-3648, Monday through Friday, 9 am – 9 pm Eastern Time.

Sincerely,

A handwritten signature in dark ink that reads "Harrison, Mauro + Morgan, CPAs". The script is cursive and fluid, with the company name and credentials clearly legible.

Harrison, Mauro, & Morgan

(Enclosure)



STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time. Please note the deadline to enroll is July 12, 2022.

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

EXHIBIT B



Return to IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

May 24, 2022

<<Variable Header – CA Only>>

Dear <<First Name>> <<Last Name>>,

Harrison, Mauro, & Morgan P.A. is writing to inform you of a recent data privacy event that may involve some of your personal information. We take this event seriously and are providing you with information about the event and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? In February 2022, Harrison, Mauro, & Morgan became aware that an unusual number of tax returns were getting rejected by the Internal Revenue Service (“IRS”). In response, Harrison, Mauro, & Morgan launched an investigation, with the assistance of a third-party information technology (“IT”) specialist, which determined that an unauthorized actor gained access to their external cloud storage system. An extensive scan was done of Harrison, Mauro, & Morgan’s internal systems and there were no indications of any unauthorized access. Harrison, Mauro, & Morgan then commenced an extensive review of the files stored on that system to determine whether sensitive information may have been present there at the time of the incident. On May 4, 2022, the investigation confirmed that the system contained sensitive information.

What Information Was Involved? The information involved was limited to 2020 tax return information including your Name, <<Data Elements>>. As stated above, some tax returns have been rejected by the IRS as duplicate returns because of this incident. To date, we are unaware of any other attempted misuse of this information as a result of this incident and are sending this notice out of an abundance of caution.

What We Are Doing in Response? The security of information in our care is among our highest priorities. In addition to launching an internal investigation into this incident, we are reviewing our existing policies and procedures and will implement additional safeguards, as needed. In an abundance of caution, we are notifying you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. Additionally, we are offering you access to complimentary credit monitoring, fraud consultation, and identity theft restoration services through IDX.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity. You may also review the information contained in the attached “Steps You Can Take to Protect Personal Information.” There you will also find more information on the <<12 / 24>> months of credit monitoring and identity protection services we are making available to you. While Harrison, Mauro, & Morgan will cover the cost of these services, you will need to complete the activation process.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-833-903-3648, Monday through Friday, 9 am – 9 pm Eastern Time.

Sincerely,

A handwritten signature in cursive script that reads "Harrison, Mauro + Morgan, CPA's". The ink is dark and the handwriting is fluid.

Harrison, Mauro, & Morgan

(Enclosure)



STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-903-3648 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time. Please note the deadline to enroll is July 12, 2022.

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.