



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

AUG 02 2021

CONSUMER PROTECTION

Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

July 28, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We continue to represent Paxton Media Group ("Paxton") located at 201 South 4th Street, Paducah, KY 42003, and write to supplement the notice provided to your Office on June 24, 2021, attached here as *Exhibit A*. By providing this notice, Paxton does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Based on ongoing data review, on June 28, 2021, the investigation identified additional personal information for certain individuals. The information affected related to New Hampshire residents includes Social Security number, financial account number and/or routing number, and health insurance information.

Per our prior notification to your Office, on June 24, 2021, Paxton began providing notice to potentially affected New Hampshire residents. Based on the ongoing data review, on July 28, 2021, Paxton will be providing written notice to an additional five (5) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit B*. Paxton will also be issuing notice of the incident to the media in all fifty (50) states and will be posting notice of this incident to the homepages of its relevant business units.

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773.

Very truly yours,

Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/shs

EXHIBIT A

STATE OF NH
DEPT OF JUSTICE
2021 AUG -2 PM 1:26



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

M. Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 24, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Paxton Media Group (“Paxton”) located at 201 South 4th Street, Paducah, KY 42003, and write to notify your Office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Paxton does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On March 20, 2021, Paxton identified suspicious activity on certain computer systems. Paxton immediately commenced an investigation to determine the full nature and scope of the incident and to secure its network. The investigation determined that Paxton was the target of a cyber-attack and that, in connection with the cyber event, an unauthorized actor was able to copy certain information from its system. This activity occurred sometime between February 26 and March 20, 2021. While the investigation into the affected information is ongoing, on May 25, 2021, the investigation determined that the relevant files contained personal information for certain individuals. The information affected related to the New Hampshire resident includes name and Social Security number.

Notice to New Hampshire Resident

On June 24, 2021, Paxton began providing written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. 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, Paxton moved quickly to investigate and respond to the incident, to assess the security its systems, and to determine the full scope of the information affected. Paxton has security measures in place to protect its systems and the information in its care and is implementing further technical safeguards.

Additionally, Paxton is providing impacted individuals with guidance on how to protect against identity theft and fraud. Paxton is also providing individuals whose Social Security number is affected with complimentary access to twelve (12) months of complimentary credit monitoring, as well as 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. In addition to notifying individuals and your Office, Paxton will be notifying the three major credit reporting agencies, Equifax, Experian, and TransUnion, as well as other relevant state regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773.

Very truly yours,

A handwritten signature in black ink, appearing to read "Alex Belton", with a long horizontal line extending to the right.

M. Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/shs
Enclosure

EXHIBIT A

To the June 24, 2021 submission



C/O IDX
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
(833) 909-3905
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

June 24, 2021

RE: Notice of Data <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>:

Paxton Media Group (“Paxton”) writes to inform you of an incident that may affect some of your information. We take this incident and the security of information in our care seriously and are providing you with an overview of the incident, our response, and steps you may take to better protect yourself, should you feel it appropriate to do so.

What Happened? On March 20, 2021, Paxton identified suspicious activity on certain computer systems in our environment. We immediately commenced an investigation to determine the full nature and scope of the incident and to secure our network. Through this investigation, we determined that Paxton was the target of a cyber-attack and that, in connection with the cyber event, an unauthorized actor was able to copy certain information from our system. This activity occurred sometime between February 26 and March 20, 2021.

What Information Was Involved? Based on the investigation, we conducted a thorough review of the affected data to identify the types of information stored there and to whom it related. On May 25, 2021, our review determined that your information was present in the affected data. This information included your <<Variable Text 2>>, and name.

What We Are Doing. We have security measures in place to protect our systems and the information in our possession and we have worked to add further technical safeguards to our environment. Following this incident, we took immediate steps to secure our systems against the attack and to conduct a diligent investigation into the full nature and scope of the incident. We are also implementing additional training and education to our employees regarding cyber threats.

As an added precaution, we are also offering you complimentary access to <<Variable Text 3>> months of credit monitoring through IDX. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. 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 and to detect errors. We also encourage you to enroll in the complimentary credit and identity monitoring services we are offering. Please also review the enclosed *Steps You Can Take To Help Protect Your Information* for instruction on how to enroll, as well as additional steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

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 call (833) 909-3905 between the hours of 6:00 a.m. and 6:00 p.m., Pacific Time, Monday through Friday.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Paxton Media Group

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To enroll, please call (833) 909-3905 or visit <https://app.idx.us/account-creation/protect> and follow the instruction provided. You will need your unique enrollment code to enroll and found above.

- **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. Please note the deadline to enroll is September 24, 2021.
- **Contact IDX at (833) 909-3905 to gain additional information** about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX Care team who will help you determine the cause of the suspicious items. If you fall victim to identity theft, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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 fraud alert or 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
888-298-0045	1-888-397-3742	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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

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. Paxton Media Group LLC may be reached by mail at PO Box 747 Eddyville, KY 42038, United States.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. 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, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
(833) 909-3905
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

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

July 28, 2021

RE: Notice of Data <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>:

Paxton Media Group (“Paxton”) writes to inform you of an incident that may affect some of your information. We take this incident and the security of information in our care seriously and are providing you with an overview of the incident, our response, and steps you may take to better protect yourself, should you feel it appropriate to do so.

What Happened? On March 20, 2021, Paxton identified suspicious activity on certain computer systems in our environment. We immediately commenced an investigation to determine the full nature and scope of the incident and to secure our network. Through this investigation, we determined that Paxton was the target of a cyber-attack and that, in connection with the cyber event, an unauthorized actor was able to copy certain information from our system. This activity occurred sometime between February 26 and March 20, 2021.

What Information Was Involved? Based on the investigation, we conducted a thorough review of the affected data to identify the types of information stored there and to whom it related. On June 28, 2021, our review determined that your information was present in the affected data. This information included your <<Variable Text 2>>, and name.

What We Are Doing. We have security measures in place to protect our systems and the information in our possession and we have worked to add further technical safeguards to our environment. Following this incident, we took immediate steps to secure our systems against the attack and to conduct a diligent investigation into the full nature and scope of the incident. We are also implementing additional training and education to our employees regarding cyber threats.

As an added precaution, we are also offering you complimentary access to <<Variable Text 3>> months of credit monitoring through IDX. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. 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 and to detect errors. We also encourage you to enroll in the complimentary credit and identity monitoring services we are offering. Please also review the enclosed *Steps You Can Take To Help Protect Your Information* for instruction on how to enroll, as well as additional steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

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 call (833) 909-3905 between the hours of 6:00 a.m. and 6:00 p.m., Pacific Time, Monday through Friday.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Paxton Media Group

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To enroll, please call (833) 909-3905 or visit <https://app.idx.us/account-creation/protect> and follow the instruction provided. You will need your unique enrollment code to enroll and found above.

- **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. Please note the deadline to enroll is September 23, 2021.
- **Contact IDX at (833) 909-3905 to gain additional information** about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX Care team who will help you determine the cause of the suspicious items. If you fall victim to identity theft, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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 fraud alert or 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
888-298-0045	1-888-397-3742	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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

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. Paxton Media Group LLC may be reached by mail at PO Box 747 Eddyville, KY 42038, United States.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. 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, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<#>> Rhode Island residents impacted by this incident.