PETERSON LAW OFFICES, P.C.

New Rockford Office
523 Central Avenue
New Rockford, ND 58356
Telephone: (701) 947-2442

Cooperstown Office
912 Burrel Avenue
Cooperstown, ND 58425
Telephone: (701) 947-2828

March 31, 2025

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Dear Sir/Madam:

On behalf of Peterson Law Offices, a law firm in North Dakota, I am writing to inform your office about a security event that affected three Maryland residents. The event involved unauthorized activity on our network. We promptly began working with cybersecurity experts to investigate. While that investigation was underway, we provided notice to our clients that an unauthorized party may have accessed files related to our representation of them. We also informed those clients that we would provide additional notice, as appropriate, based on the results of a data review.

In late October 2024, we detected suspicious activity on our network. We promptly started remedial action designed to prevent further disruption and retained outside counsel to assist with assessing our legal obligations. Our outside counsel then engaged a leading cybersecurity firm to investigate and assist with remediation. The investigation identified the impacted files and determined that the unauthorized activity started on October 25, 2024, and ended on October 31, 2024. Based on that investigation, we have worked with experts to further bolster our security by, among other measures: upgrading firewalls, expanding the use of multifactor authentication, and adding endpoint detection and response protection.

Drawing from the investigation findings, we engaged a data-review firm to assess the impacted files on December 10, 2024. The data-review firm provided their report on February 3, 2025. Based on our counsel's review of the data-mining results, we have reason to believe this incident impacted the following types of personal information: name, contact information, government identification numbers (such as a driver's license or Social Security number), financial account numbers, and limited medical information. We worked with our counsel to assess notification obligations and to locate current addresses for impacted individuals. We completed that process on March 13, 2025, and began coordinating the notification process with a mailing vendor.

We will mail notices to affected individuals on April 2, 2025. We are providing complimentary credit monitoring to any individual who had a Social Security number or driver's license number impacted by the event. We have included templates of the notices we are providing to the impacted individuals.

If you have any questions, please contact Josh Hansen, our outside counsel for this event, at (303) 285-5306 or jahansen@shb.com.

Sincerely,
Travis Peterson

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

PETERSON LAW OFFICES, P.C.

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>,

At Peterson Law Offices, we take our relationships with our clients seriously. That's why we are contacting you about a security incident that impacted some of your data. We detected suspicious activity on our network late last year and promptly began working with outside cybersecurity experts to investigate that activity. Based on our investigation, we determined that an unauthorized third party acquired some of your personal information. We are reaching out to provide you information on what happened and what we are doing in response.

WHAT HAPPENED

On October 31, 2024, we detected suspicious activity on our network. We promptly began working with third-party experts to investigate and assist with remediation efforts, including identifying the potentially affected files. Once we identified the impacted files, we engaged a data-review firm to review the content of those files. We received the results of that data review on February 3, 2025, and have since been working to get current addresses for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the third party acquired a limited amount of your personal information. The affected data includes some combination of your: name, contact information, medical information, financial details, and government identification number (such as a driver's license number or Social Security number).

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect yourself against fraud. In addition, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of personal information. Additional details about this product can be found on the next page. To register, please:

- Ensure that you **enroll by:** **<<Enrollment Deadline>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** **<<Activation Code>>**

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 877-288-8057 by **<<Enrollment Deadline>>** and provide them engagement number **<<Engagement Number>>**.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at (701) 947-2442, and we will be happy to assist you.

Sincerely,

Travis Peterson

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your credit report, free of charge, once per week. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. A fraud alert is free and will stay on your credit report for 1 year, but you can renew it. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.identitytheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	Equifax	Experian	TransUnion
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

PETERSON LAW OFFICES, P.C.

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>,

At Peterson Law Offices, we take our relationships with our clients seriously. That's why we are contacting you about a security incident that impacted some of your data. We detected suspicious activity on our network late last year and promptly began working with outside cybersecurity experts to investigate that activity. Based on our investigation, we determined that an unauthorized third party acquired some of your personal information. We are reaching out to provide you information on what happened and what we are doing in response.

WHAT HAPPENED

On October 31, 2024, we detected suspicious activity on our network. We promptly began working with third-party experts to investigate and assist with remediation efforts, including identifying the potential affected files. Once we identified the impacted files, we engaged a data-review firm to review the content of those files. We received the results of that data review on February 3, 2025, and have since been working to get current addresses for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the third party acquired a limited amount of your personal information. The affected data includes your: name, contact information, and date of birth

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect yourself against fraud.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at (701) 947-2442, and we will be happy to assist you.

Sincerely,

Travis Peterson

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your credit report, free of charge, once per week. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. A fraud alert is free and will stay on your credit report for 1 year, but you can renew it. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.identitytheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

PETERSON LAW OFFICES, P.C.

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>,

At Peterson Law Offices, we take our relationships with our clients seriously. That's why we are contacting you about a security incident that impacted some of your data. We detected suspicious activity on our network late last year and promptly began working with outside cybersecurity experts to investigate that activity. Based on our investigation, we determined that an unauthorized third party acquired some of your personal information. We are reaching out to provide you information on what happened and what we are doing in response.

WHAT HAPPENED

On October 31, 2024, we detected suspicious activity on our network. We promptly began working with third-party experts to investigate and assist with remediation efforts, including identifying the potentially affected files. Once we identified the impacted files, we engaged a data-review firm to review the content of those files. We received the results of that data review on February 3, 2025 and have since been working to get current addresses for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the third party acquired a limited amount of your personal information. The affected data includes your: name, contact information, medical information, and financial details.

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect yourself against fraud.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at (701) 947-2442, and we will be happy to assist you.

Sincerely,

Travis Peterson

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your credit report, free of charge, once per week. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. A fraud alert is free and will stay on your credit report for 1 year, but you can renew it. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.identitytheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

PETERSON LAW OFFICES, P.C.

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>,

At Peterson Law Offices, we take our relationships with our clients seriously. That's why we are contacting you about a security incident that impacted some of your data. We detected suspicious activity on our network late last year and promptly began working with outside cybersecurity experts to investigate that activity. Based on our investigation, we determined that an unauthorized third party acquired some of your personal information. We are reaching out to provide you information on what happened and what we are doing in response.

WHAT HAPPENED

On October 31, 2024, we detected suspicious activity on our network. We promptly began working with third-party experts to investigate and assist with remediation efforts, including identifying the potentially affected files. Once we identified the impacted files, we engaged a data-review firm to review the content of those files. We received the results of that data review on February 3, 2025 and have since been working to get current addresses for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the third party acquired a limited amount of your personal information. The affected data includes your: name, contact information, and government identification number (such as a driver's license number or Social Security number).

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect yourself against fraud. In addition, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of personal information. Additional details about this product can be found on the next page. To register, please:

- Ensure that you **enroll by:** **<<Enrollment Deadline>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** **<<Activation Code>>**

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 877-288-8057 by **<<Enrollment Deadline>>** and provide them engagement number <<Engagement Number>>.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at (701) 947-2442, and we will be happy to assist you.

Sincerely,

Travis Peterson

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your credit report, free of charge, once per week. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. A fraud alert is free and will stay on your credit report for 1 year, but you can renew it. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.identitytheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	Equifax	Experian	TransUnion
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

PETERSON LAW OFFICES, P.C.

New Rockford Office
523 Central Avenue
New Rockford, ND 58356
Telephone: [redacted]

Cooperstown Office
912 Burrel Avenue
Cooperstown, ND 58425
Telephone: [redacted]

<Date>

<Name>
<Address>
<City>, <State> <ZIP>

NOTICE OF DATA BREACH

Dear <Name>,

At Peterson Law Offices, we take our relationships with our clients seriously. That's why we are contacting you about a security incident that impacted some of your data. We detected suspicious activity on our network late last year and promptly began working with outside cybersecurity experts to investigate that activity. Based on our investigation, we determined that an unauthorized third party acquired some of your personal information. We are reaching out to provide you information on what happened and what we are doing in response.

WHAT HAPPENED

On October 31, 2024, we detected suspicious activity on our network. We promptly began working with third-party experts to investigate and assist with remediation efforts, including identifying the potentially affected files. Once we identified the impacted files, we engaged a data-review firm to review the content of those files. We received the results of that data review on February 3, 2025, and have since been working to get current addresses for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the third party acquired a limited amount of your personal information. The affected data includes your: name, contact information, and government identification number (such as a driver's license number or Social Security number).

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect yourself against fraud. In addition, we are offering a complimentary two-year membership to Experian IdentityWorks. This product helps detect possible misuse of personal information. Additional details about this product can be found on the next page. To register, please:

- Ensure that you **enroll by: 06/30/2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** <Code>

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **06/30/2025** and provide them engagement number [redacted].

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at [redacted], and we will be happy to assist you.

Sincerely,

Travis Peterson

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your credit report, free of charge, once per week. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. A fraud alert is free and will stay on your credit report for 1 year, but you can renew it. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.identitytheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

PETERSON LAW OFFICES, P.C.

New Rockford Office
523 Central Avenue
New Rockford, ND 58356
Telephone: [redacted]

Cooperstown Office
912 Burrel Avenue
Cooperstown, ND 58425
Telephone: [redacted]

<Date>

To the Parent or Legal Guardian of:
<Name>
<Address>
<City>, <State> <ZIP>

NOTICE OF DATA BREACH

Dear Parent or Legal Guardian of <Name>,

At Peterson Law Offices, we take our relationships with our clients seriously. That's why we are contacting you about a security incident that impacted some of your child's data. We detected suspicious activity on our network late last year and promptly began working with outside cybersecurity experts to investigate that activity. Based on our investigation, we determined that an unauthorized third party acquired some of your child's personal information. We are reaching out to provide you information on what happened and what we are doing in response.

WHAT HAPPENED

On October 31, 2024, we detected suspicious activity on our network. We promptly began working with third-party experts to investigate and assist with remediation efforts, including identifying the potentially affected files. Once we identified the impacted files, we engaged a data-review firm to review the content of those files. We received the results of that data review on February 3, 2025, and have since been working to get current addresses for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the third party acquired a limited amount of your child's personal information. The affected data includes some combination of your child's: name, contact information, medical information, and government identification number (such as a driver's license number or Social Security number).

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your child's information. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect your child against fraud. In addition, we are offering a complimentary one-year membership to Experian IdentityWorks. This product helps detect possible misuse of personal information. Additional details about this product can be found on the next page. To register, please:

- Ensure that you **enroll by: 06/30/2025** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/minorplus
- Provide your **activation code:** <Code>

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **06/30/2025** and provide them engagement number [redacted].

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at [redacted], and we will be happy to assist you.

Sincerely,

Travis Peterson

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your child's account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov.

- You should confirm that your child's credit card company has the correct address on file for your child and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your child's credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your child's credit report, free of charge, once per week. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your child's credit file – Consumer reporting agencies have tools you can use to protect your child's credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending your child's credit that they should take special precautions to verify your child's identity. A fraud alert is free and will stay on your child's credit report for 1 year, but you can renew it. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your child's credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe your child is the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.identitytheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting your child from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – Your child also has certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your child's rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/sites/default/ files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

PETERSON LAW OFFICES, P.C.

New Rockford Office
523 Central Avenue
New Rockford, ND 58356
Telephone: [redacted]

Cooperstown Office
912 Burrel Avenue
Cooperstown, ND 58425
Telephone: [redacted]

<Date>

To the Parent or Legal Guardian of:
<Name>
<Address>
<City>, <State> <ZIP>

NOTICE OF DATA BREACH

Dear Parent or Legal Guardian of <Name>,

At Peterson Law Offices, we take our relationships with our clients seriously. That's why we are contacting you about a security incident that impacted some of your child's data. We detected suspicious activity on our network late last year and promptly began working with outside cybersecurity experts to investigate that activity. Based on our investigation, we determined that an unauthorized third party acquired some of your child's personal information. We are reaching out to provide you information on what happened and what we are doing in response.

WHAT HAPPENED

On October 31, 2024, we detected suspicious activity on our network. We promptly began working with third-party experts to investigate and assist with remediation efforts, including identifying the potential affected files. Once we identified the impacted files, we engaged a data-review firm to review the content of those files. We received the results of that data review on February 3, 2025, and have since been working to get current addresses for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the third party acquired a limited amount of your child's personal information. The affected data includes your child's: name, contact information, and date of birth

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your child's information. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect your child against fraud.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at [redacted]. We will be happy to assist you.

Sincerely,

Travis Peterson

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your child's account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov.

- You should confirm that your child's credit card company has the correct address on file for your child and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your child's credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your child's credit report, free of charge, once per week. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your child's credit file – Consumer reporting agencies have tools you can use to protect your child's credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending you credit that they should take special precautions to verify your child's identity. A fraud alert is free and will stay on your child's credit report for 1 year, but you can renew it. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your child's credit report, which will prevent them from extending your child credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe your child is the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.identitytheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting your child from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – Your child also has certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your child's rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/sites/default/ files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

PETERSON LAW OFFICES, P.C.

New Rockford Office
523 Central Avenue
New Rockford, ND 58356
Telephone: [redacted]

Cooperstown Office
912 Burrel Avenue
Cooperstown, ND 58425
Telephone: [redacted]

<Date>

To the Parent or Legal Guardian of:
<Name>
<Address>
<City>, <State> <ZIP>

NOTICE OF DATA BREACH

Dear Parent or Legal Guardian of <Name>,

At Peterson Law Offices, we take our relationships with our clients seriously. That's why we are contacting you about a security incident that impacted some of your child's data. We detected suspicious activity on our network late last year and promptly began working with outside cybersecurity experts to investigate that activity. Based on our investigation, we determined that an unauthorized third party acquired some of your child's personal information. We are reaching out to provide you information on what happened and what we are doing in response.

WHAT HAPPENED

On October 31, 2024, we detected suspicious activity on our network. We promptly began working with third-party experts to investigate and assist with remediation efforts, including identifying the potential affected files. Once we identified the impacted files, we engaged a data-review firm to review the content of those files. We received the results of that data review on February 3, 2025, and have since been working to get current addresses for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the third party acquired a limited amount of your child's personal information. The affected data includes your child's: name, contact information, medical information, and date of birth.

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your child's information. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect your child against fraud.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at [redacted]. We will be happy to assist you.

Sincerely,

Travis Peterson

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your child's account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov.

- You should confirm that your child's credit card company has the correct address on file for your child and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your child's credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your child's credit report, free of charge, once per week. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your child's credit file – Consumer reporting agencies have tools you can use to protect your child's credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending you credit that they should take special precautions to verify your child's identity. A fraud alert is free and will stay on your child's credit report for 1 year, but you can renew it. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your child's credit report, which will prevent them from extending your child credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe your child is the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.identitytheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting your child from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – Your child also has certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your child's rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/sites/default/ files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

PETERSON LAW OFFICES, P.C.

New Rockford Office
523 Central Avenue
New Rockford, ND 58356
Telephone: [redacted]

Cooperstown Office
912 Burrel Avenue
Cooperstown, ND 58425
Telephone: [redacted]

<Date>

To the Parent or Legal Guardian of:
<Name>
<Address>
<City>, <State> <ZIP>

NOTICE OF DATA BREACH

Dear Parent or Legal Guardian of <Name>,

At Peterson Law Offices, we take our relationships with our clients seriously. That's why we are contacting you about a security incident that impacted some of your child's data. We detected suspicious activity on our network late last year and promptly began working with outside cybersecurity experts to investigate that activity. Based on our investigation, we determined that an unauthorized third party acquired some of your child's personal information. We are reaching out to provide you information on what happened and what we are doing in response.

WHAT HAPPENED

On October 31, 2024, we detected suspicious activity on our network. We promptly began working with third-party experts to investigate and assist with remediation efforts, including identifying the potential affected files. Once we identified the impacted files, we engaged a data-review firm to review the content of those files. We received the results of that data review on February 3, 2025, and have since been working to get current addresses for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the third party acquired a limited amount of your child's personal information. The affected data includes your child's: name, contact information, and medical information.

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your child's information. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect your child against fraud.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at [redacted]. We will be happy to assist you.

Sincerely,

Travis Peterson

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your child's account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov.

- You should confirm that your child's credit card company has the correct address on file for your child and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your child's credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your child's credit report, free of charge, once per week. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your child's credit file – Consumer reporting agencies have tools you can use to protect your child's credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending you credit that they should take special precautions to verify your child's identity. A fraud alert is free and will stay on your child's credit report for 1 year, but you can renew it. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your child's credit report, which will prevent them from extending your child credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe your child is the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.identitytheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting your child from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – Your child also has certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your child's rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/sites/default/ files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

PETERSON LAW OFFICES, P.C.

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
To the Parent or Legal Guardian of:
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

PETERSON LAW OFFICES, P.C.

<<Date>>

NOTICE OF DATA BREACH

Dear Parent or Legal Guardian of <<Full Name>>,

At Peterson Law Offices, we take our relationships with our clients seriously. That's why we are contacting you about a security incident that impacted some of your child's data. We detected suspicious activity on our network late last year and promptly began working with outside cybersecurity experts to investigate that activity. Based on our investigation, we determined that an unauthorized third party acquired some of your child's personal information. We are reaching out to provide you information on what happened and what we are doing in response.

WHAT HAPPENED

On October 31, 2024, we detected suspicious activity on our network. We promptly began working with third-party experts to investigate and assist with remediation efforts, including identifying the potentially affected files. Once we identified the impacted files, we engaged a data-review firm to review the content of those files. We received the results of that data review on February 3, 2025 and have since been working to get current addresses for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the third party acquired a limited amount of your child's personal information. The affected data includes your child's: name, contact information, and government identification number (such as a driver's license number or Social Security number).

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your child's information. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect your child against fraud. In addition, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of personal information. Additional details about this product can be found on the next page. To register, please:

- Ensure that you **enroll by:** **<<Enrollment Deadline>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/minorplus
- Provide your **activation code:** **<<Activation Code>>**

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 877-288-8057 by **<<Enrollment Deadline>>** and provide them engagement number **<<Engagement Number>>**.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at (701) 947-2442, and we will be happy to assist you.

Sincerely,

Travis Peterson

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your child's account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov.

- You should confirm that your child's credit card company has the correct address on file for your child and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your child's credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your child's credit report, free of charge, once per week. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your child's credit file – Consumer reporting agencies have tools you can use to protect your child's credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending your child credit that they should take special precautions to verify your child's identity. A fraud alert is free and will stay on your child's credit report for 1 year, but you can renew it. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your child's credit report, which will prevent them from extending your child credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and previous addresses. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe your child is the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.identitytheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting your child from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.
For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; (800) 771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – Your child also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in their file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your child's rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.