cierant

July 3, 2025

[redacted]

Re: NOTICE OF DATA SECURITY EVENT

Dear [redacted]:

Cierant Corporation ("Cierant") is writing to make you aware of a data security event, which may have impacted some of your personal information that you provided to your health plan. This notice provides you with information about the event, our response, and steps you may take to protect your personal information, should you feel it is necessary.

Who is Cierant / Why Did We Have Your Data? Cierant is a distributed marketing software and services company. Your health plan uses Cierant to mail letters to you such as those relating to your Explanations of Benefits and health insurance appeals. In connection with these, Cierant processed some of your member data, and is sending this letter to you on behalf of your health plan.

What Happened? On December 10, 2024, Cierant became aware of suspicious activity on one of our systems and learned of a vulnerability with the Cleo VLTrader tool, which is a third-party secure file transfer tool. In response, we began an investigation with assistance from an industry-leading cybersecurity team. The investigation determined that an unauthorized actor exploited the third-party Cleo VLTrader vulnerability to gain limited access to Cierant systems that may have compromised certain files. A recently concluded review of potentially impacted files identified information related to you.

What Information Was Involved? A review of potentially impacted files determined the following types of your personal information may have been involved your: name, address, date of birth, treatment-related dates, a generic description of services received, provider name, medical record number, health plan beneficiary number, claims number, and/or plan member account number. The impacted files did not include your Social Security number or financial information.

What We Are Doing. Cierant takes the privacy and security of information in our care seriously. Upon becoming aware of suspicious activity, we immediately ceased the use of Cleo VLTrader, rotated passwords, and took a number of steps to enhance our existing network security controls. We also reported the event to federal law enforcement and are notifying relevant regulators.

What You Can Do. Cierant encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanations of benefits, and monitoring free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties. You may also review the enclosed *Additional Resources* for best practices and steps you can take to protect your personal information.

For More Information. If you have any questions, you may contact the dedicated assistance line toll-free at 877-841-3066. Please note, telephone service provider charges may be incurred. This toll-free line is available Monday through Friday, 9:00 a.m. – 9:00 p.m. Eastern Time, excluding major U.S holidays.

Sincerely,

Cierant Corporation

ADDITIONAL RESOURCES

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion 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 P.O. Box 160 Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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.

Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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, D.C. 20001; 1-202-442-9828; and https://www.oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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://www.ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; and https://www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; https://www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 373 Rhode Island residents that may be impacted by this event.

cierant

July 3, 2025

[redacted]

Re: NOTICE OF DATA SECURITY EVENT

To the care of [redacted]:

Cierant Corporation ("Cierant") is writing to make you aware of a data security event, which may have impacted some of your personal information that you provided to your health plan. This notice provides you with information about the event, our response, and steps you may take to protect your personal information, should you feel it is necessary.

Who is Cierant / Why Did We Have Your Data? Cierant is a distributed marketing software and services company. Your health plan uses Cierant to mail letters to you such as those relating to your Explanations of Benefits and health insurance appeals. In connection with these, Cierant processed some of your member data, and is sending this letter to you on behalf of your health plan.

What Happened? On December 10, 2024, Cierant became aware of suspicious activity on one of our systems and learned of a vulnerability with the Cleo VLTrader tool, which is a third-party secure file transfer tool. In response, we began an investigation with assistance from an industry-leading cybersecurity team. The investigation determined that an unauthorized actor exploited the third-party Cleo VLTrader vulnerability to gain limited access to Cierant systems that may have compromised certain files. A recently concluded review of potentially impacted files identified information related to you.

What Information Was Involved? A review of potentially impacted files determined the following types of your personal information may have been involved your: name, address, date of birth, treatment-related dates, a generic description of services received, provider name, medical record number, health plan beneficiary number, claims number, and/or plan member account number. The impacted files did not include your Social Security number or financial information.

What We Are Doing. Cierant takes the privacy and security of information in our care seriously. Upon becoming aware of suspicious activity, we immediately ceased the use of Cleo VLTrader, rotated passwords, and took a number of steps to enhance our existing network security controls. We also reported the event to federal law enforcement and are notifying relevant regulators.

What You Can Do. Cierant encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanations of benefits, and monitoring free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties. You may also review the enclosed *Additional Resources* for best practices and steps you can take to protect your personal information.

For More Information. If you have any questions, you may contact the dedicated assistance line toll-free at 877-841-3066. Please note, telephone service provider charges may be incurred. This toll-free line is available Monday through Friday, 9:00 a.m. – 9:00 p.m. Eastern Time, excluding major U.S holidays.

Sincerely,

Cierant Corporation

ADDITIONAL RESOURCES

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion 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 P.O. Box 160 Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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.

Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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, D.C. 20001; 1-202-442-9828; and https://www.oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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://www.ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; and https://www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; https://www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 373 Rhode Island residents that may be impacted by this event.

cierant

DEV

July 3, 2025

[redacted]
TO THE PARENT OR GUARDIAN OF: [redacted]
[redacted]
[redacted]

Re: NOTICE OF DATA SECURITY EVENT

Dear Parent or Guardian of [redacted]:

Cierant Corporation ("Cierant") is writing to make you aware of a data security event, which may have impacted some of your minor's personal information that was provided to your health plan. This notice provides you with information about the event, our response, and steps you may take to protect your minor's personal information, should you feel it is necessary.

Who is Cierant / Why Did We Have Your Data? Cierant is a distributed marketing software and services company. Your minor's health plan uses Cierant to mail letters such as those relating to your minor's Explanations of Benefits and health insurance appeals. In connection with these, Cierant processed some of your minor's member data, and is sending this letter to you in regard to your minor on behalf of your minor's health plan.

What Happened? On December 10, 2024, Cierant became aware of suspicious activity on one of our systems and learned of a vulnerability with the Cleo VLTrader tool, which is a third-party secure file transfer tool. In response, we began an investigation with assistance from an industry-leading cybersecurity team. The investigation determined that an unauthorized actor exploited the third-party Cleo VLTrader vulnerability to gain limited access to Cierant systems that may have compromised certain files. A recently concluded review of potentially impacted files identified information related to your minor.

What Information Was Involved? A review of potentially impacted files determined the following types of your minor's personal information may have been involved your: name, address, date of birth, treatment-related dates, a generic description of services received, provider name, medical record number, health plan beneficiary number, claims number, and/or plan member account number. The impacted files did not include your Social Security number or financial information.

What We Are Doing. Cierant takes the privacy and security of information in our care seriously. Upon becoming aware of suspicious activity, we immediately ceased the use of Cleo VLTrader, rotated passwords, and took a number of steps to enhance our existing network security controls. We also reported the event to federal law enforcement and are notifying relevant regulators.

What You Can Do. Cierant encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your minor's account statements and explanations of benefits, and if applicable, monitoring your minor's free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties. You may also review the enclosed *Additional Resources* for best practices and steps you can take to protect your minor's personal information.

For More Information. If you have any questions, you may contact the dedicated assistance line toll-free at 877-841-3066. Please note, telephone service provider charges may be incurred. This toll-free line is available Monday through Friday, 9:00 a.m. – 9:00 p.m. Eastern Time, excluding major U.S holidays.

Sincerely,

Cierant Corporation

ADDITIONAL RESOURCES

Monitor Your Minor's Accounts

Typically, credit reporting agencies do not have a credit report in a minor's name. To find out if your minor has a credit report or to request a manual search for your minor's Social Security number each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone, writing, or online:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/education/identity-theft/child-identity-theft/	https://www.experian.com/help/minor-request.html	https://www.transunion.com/fraud-victim-resources/child-identity-theft
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 105788 Atlanta, GA 30348-5788	P.O. Box 9554 Allen, TX 75013	P.O. Box 2000 Chester, PA 19016

To request information about the existence of a credit file in your minor's name, search for your minor's Social Security number, place a security freeze or fraud alert on your minor's credit report (if one exists), or request a copy of your minor's credit report you may be required to provide the following information:

- A copy of your driver's license or another government issued identification card, such as a state identification card, etc.;
- Proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- A copy of your minor's birth certificate;
- A copy of your minor's Social Security card;
- Your minor's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- Your minor's date of birth; and
- Your minor's previous addresses for the past two years.

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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, D.C. 20001; 1-202-442-9828; and https://www.oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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://www.ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; and https://www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; https://www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 373 Rhode Island residents that may be impacted by this event.

cierant

July 3, 2025

[redacted]

Re: NOTICE OF DATA SECURITY EVENT

Dear Parent or Guardian of [redacted]:

Cierant Corporation ("Cierant") is writing to make you aware of a data security event, which may have impacted some of your minor's personal information that was provided to your health plan. This notice provides you with information about the event, our response, and steps you may take to protect your minor's personal information, should you feel it is necessary.

Who is Cierant / Why Did We Have Your Data? Cierant is a distributed marketing software and services company. Your minor's health plan uses Cierant to mail letters such as those relating to your minor's Explanations of Benefits and health insurance appeals. In connection with these, Cierant processed some of your minor's member data, and is sending this letter to you in regard to your minor on behalf of your minor's health plan.

What Happened? On December 10, 2024, Cierant became aware of suspicious activity on one of our systems and learned of a vulnerability with the Cleo VLTrader tool, which is a third-party secure file transfer tool. In response, we began an investigation with assistance from an industry-leading cybersecurity team. The investigation determined that an unauthorized actor exploited the third-party Cleo VLTrader vulnerability to gain limited access to Cierant systems that may have compromised certain files. A recently concluded review of potentially impacted files identified information related to your minor.

What Information Was Involved? A review of potentially impacted files determined the following types of your minor's personal information may have been involved your: name, address, date of birth, treatment-related dates, a generic description of services received, provider name, medical record number, health plan beneficiary number, claims number, and/or plan member account number. The impacted files did not include your Social Security number or financial information.

What We Are Doing. Cierant takes the privacy and security of information in our care seriously. Upon becoming aware of suspicious activity, we immediately ceased the use of Cleo VLTrader, rotated passwords, and took a number of steps to enhance our existing network security controls. We also reported the event to federal law enforcement and are notifying relevant regulators.

What You Can Do. Cierant encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your minor's account statements and explanations of benefits, and if applicable, monitoring your minor's free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties. You may also review the enclosed *Additional Resources* for best practices and steps you can take to protect your minor's personal information.

For More Information. If you have any questions, you may contact the dedicated assistance line toll-free at 877-841-3066. Please note, telephone service provider charges may be incurred. This toll-free line is available Monday through Friday, 9:00 a.m. – 9:00 p.m. Eastern Time, excluding major U.S holidays.

Sincerely,

DEV

Cierant Corporation

ADDITIONAL RESOURCES

Monitor Your Minor's Accounts

Typically, credit reporting agencies do not have a credit report in a minor's name. To find out if your minor has a credit report or to request a manual search for your minor's Social Security number each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone, writing, or online.

Equifax	Experian	TransUnion
https://www.equifax.com/personal/education/identity-theft/child-identity-theft/	https://www.experian.com/help/minor-request.html	https://www.transunion.com/fraud-victim-resources/child-identity-theft
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 105788 Atlanta, GA 30348-5788	P.O. Box 9554 Allen, TX 75013	P.O. Box 2000 Chester, PA 19016

To request information about the existence of a credit file in your minor's name, search for your minor's Social Security number, place a security freeze or fraud alert on your minor's credit report (if one exists), or request a copy of your minor's credit report you may be required to provide the following information:

- A copy of your driver's license or another government issued identification card, such as a state identification card, etc.;
- Proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- A copy of your minor's birth certificate;
- A copy of your minor's Social Security card;
- Your minor's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- Your minor's date of birth; and
- Your minor's previous addresses for the past two years.

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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, D.C. 20001; 1-202-442-9828; and https://www.oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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://www.ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; and https://www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; https://www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 373 Rhode Island residents that may be impacted by this event.

Enclosure B

Notice of Data Incident – Confidential Enclosure

Horizon Blue Cross Blue Shield of New Jersey
3 Penn Plaza East
Newark, New Jersey 07105