



March 25, 2025

Maryland Attorney General
200 St. Paul Place, Baltimore, MD 21202

RE: National Truck Protection Security Event

Dear Sir/Madam:

On behalf of National Truck Protection Co., Inc. (NTP), a provider of aftermarket-commercial-truck vehicle service contracts (commonly known as extended warranties) based in North Carolina, I am writing to inform your office about a security event that potentially affected one Maryland resident. The event involved unauthorized activity in a portion of our network, but the event did not prevent NTP from continuing to serve our customers.

In late January 2025, 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 in turn engaged a leading cybersecurity firm to investigate.

The investigation determined that the event started on January 20, 2025, and concluded on January 25, 2025. The event involved unauthorized access to a limited portion of NTP's environment and a small number of files. NTP also worked with the cybersecurity experts to further bolster our security by, for example: rebuilding all servers, resetting all passwords, refining the use of multifactor authentication, reconfiguring firewall and endpoint-detection settings, deploying expanded anti-ransomware protection on all servers, and working with a third-party expert to validate the efficacy of those remediation measures. NTP is also working with a third-party expert to validate the efficacy of their remediation measures. On January 31, NTP identified the potentially impacted files and engaged a data-review firm to assess their contents.

The data-review firm provided its report regarding the analyzed files on March 3. In coordination with our counsel, we immediately began reviewing that report to assess notification obligations and to find (and update) addresses. We completed that process on March 14, 2025. Having reviewed the affected information, we have reason to believe that the event involved unauthorized access to the following types of personal information: name, date of birth, contact information, Social Security numbers, financial account details, and two account credentials.

Consistent with our obligations under applicable law, we will mail notices to affected individuals on March 27, 2025. We are providing complimentary credit monitoring to any individual who had a Social Security number potentially 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,
Geoff Stigler

THE STANDARD FOR PROTECTION & PERFORMANCE

📍 7990 North Point Blvd. Suite 108, Winston-Salem, NC 27106
☎ 877-950-3200
🌐 www.ntpwarranty.com





<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<last_name>>,

National Truck Protection is writing to inform you about an incident that may have exposed your personal information to unauthorized persons. In late January 2025, we detected a cybersecurity incident involving unauthorized activity in a limited portion of our environment. We promptly began an investigation. Based on the investigation, we determined that the unauthorized third party may have acquired some of your personal information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On January 25, 2025, we first suspected that an unauthorized third party may have gained access to a limited portion of our environment. We promptly began investigating; we began working with third-party cybersecurity experts to investigate and started remediation efforts, including identifying the potentially affected files and engaging a data-review firm to analyze their contents. We received those results in March 2025 and have been working since that time to find updated contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the unauthorized third party accessed or acquired some of your personal information, which may include your name, contact information, and financial details (such as your bank account and routing number).

WHAT WE ARE DOING

Protecting the integrity of the information we maintain is a responsibility we take very seriously. We hired third-party experts to help us address this situation, perform an investigation into the unauthorized activity, and further secure our systems and the information we maintain as we move forward.

WHAT YOU CAN DO

We currently have no evidence that the unauthorized third party has fraudulently used any information involved in this incident. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity and to review the *Additional Steps You Can Take* guidance included in this letter for steps you can take to help protect yourself against fraud.

THE STANDARD FOR PROTECTION & PERFORMANCE

📍 7990 North Point Blvd. Suite 108, Winston-Salem, NC 27106
📞 877-950-3200
🌐 www.ntpwarranty.com



FOR MORE INFORMATION

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, you can contact us at 336-904-2174 or compliance@ntpc.com. Thank you for your understanding and patience.

Sincerely,

Geoff Sigler

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/Info-Lost-or-Stolen.

- 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. 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. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. 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 charge for requesting a security freeze. 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 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 Washington, DC 20580 (202) 326-2222 www.ftc.gov	P.O. Box 740241 Atlanta, GA 30374 (800) 685-1111 www.equifax.com	P.O. Box 9701 Allen, TX 75013 (888) 397-3742 www.experian.com	P.O. Box 2000 Chester, PA 19016 (888) 909-8872 www.transunion.com
Maryland Attorney General	New York Attorney General	North Carolina Attorney General	Washington, DC Attorney General
200 St. Paul Place, 25th Floor Baltimore, MD 21202 (888) 743-0023 www.marylandattorneygeneral.gov	The Capitol Albany, NY 1224 (800) 771-7755 www.ag.ny.gov	9001 Mail Service Center Raleigh, NC 27699 (919) 716-6400 www.ncdoj.gov	400 6th St. NW Washington, DC 20001 (202) 727-3400 www.oag.dc.gov

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



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<last_name>>,

National Truck Protection is writing to inform you about an incident that may have exposed your personal information to unauthorized persons. In late January, we detected a cybersecurity incident involving unauthorized activity in a limited portion of our environment. We promptly began an investigation. Based on the investigation, we determined that the unauthorized third party may have acquired some of your personal information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On January 25, 2025, we first suspected that an unauthorized third party may have gained access to a limited portion of our environment. We promptly began investigating; we began working with third-party cybersecurity experts to investigate and started remediation efforts, including identifying the potentially affected files and engaging a data-review firm to analyze their contents. We received those results in March 2025 and have been working since that time to find updated contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the unauthorized third party accessed or acquired some of your personal information, which may include your name, contact information, Social Security number, and financial details (such as your bank account and routing number).

WHAT WE ARE DOING

Protecting the integrity of the information we maintain is a responsibility we take very seriously. We hired third-party experts to help us address this situation, perform an investigation into the unauthorized activity, and further secure our systems and the information we maintain as we move forward.

WHAT YOU CAN DO

We currently have no evidence that the unauthorized third party has fraudulently used any information involved in this incident. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity and to review the *Additional Steps You Can Take* guidance included in this letter for steps you can take to help protect yourself against fraud. In addition, we are offering a complimentary 1-year membership to Kroll's identity monitoring services. You can find instructions for activating that service in this packet.

THE STANDARD FOR PROTECTION & PERFORMANCE

📍 7990 North Point Blvd. Suite 108, Winston-Salem, NC 27106
📞 877-950-3200
🌐 www.ntpwarranty.com



FOR MORE INFORMATION

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, you can contact us at 336-904-2174 or compliance@ntpc.com. Thank you for your understanding and patience.

Sincerely,

Geoff Sigler

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

- Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.
- You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
- Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Your complimentary identity monitoring services include:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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/Info-Lost-or-Stolen.

- 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. 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. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. 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 charge for requesting a security freeze. 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 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

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Maryland

Attorney General

200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

New York

Attorney General

The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

North Carolina

Attorney General

9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

Washington, DC

Attorney General

400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

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



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<last_name>>,

National Truck Protection is writing to inform you about an incident that may have exposed your personal information to unauthorized persons. In late January 2025, we detected a cybersecurity incident involving unauthorized activity in a limited portion of our environment. We promptly began an investigation. Based on the investigation, we determined that the unauthorized third party may have acquired some of your personal information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On January 25, 2025, we first suspected that an unauthorized third party may have gained access to a limited portion of our environment. We promptly began investigating; we began working with third-party cybersecurity experts to investigate and started remediation efforts, including identifying the potentially affected files and engaging a data-review firm to analyze their contents. We received those results in March 2025 and have been working since that time to find updated contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the unauthorized third party accessed or acquired some of your personal information, which included your name, contact information, and account credentials from [REDACTED] for [REDACTED].

WHAT WE ARE DOING

Protecting the integrity of the information we maintain is a responsibility we take very seriously. We hired third-party experts to help us address this situation, perform an investigation into the unauthorized activity, and further secure our systems and the information we maintain as we move forward.

WHAT YOU CAN DO

We currently have no evidence that the unauthorized third party has fraudulently used any information involved in this incident. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity and to review the *Additional Steps You Can Take* guidance included in this letter for steps you can take to help protect yourself against fraud. We also encourage you to change the affected password.

THE STANDARD FOR PROTECTION & PERFORMANCE

📍 7990 North Point Blvd. Suite 108, Winston-Salem, NC 27106
📞 877-950-3200
🌐 www.ntpwarranty.com



FOR MORE INFORMATION

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, you can contact us at 336-904-2174 or compliance@ntpc.com. Thank you for your understanding and patience.

Sincerely,

Geoff Sigler

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/Info-Lost-or-Stolen.

- 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. 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. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. 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 charge for requesting a security freeze. 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 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

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Maryland

Attorney General

200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

New York

Attorney General

The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

North Carolina

Attorney General

9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Washington, DC

Attorney General

400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

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



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<last_name>>,

National Truck Protection is writing to inform you about an incident that may have exposed your personal information to unauthorized persons. In late January, we detected a cybersecurity incident involving unauthorized activity in a limited portion of our environment. We promptly began an investigation. Based on the investigation, we determined that the unauthorized third party may have acquired some of your personal information. We are providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

On January 25, 2025, we first suspected that an unauthorized third party may have gained access to a limited portion of our environment. We promptly began investigating; we began working with third-party cybersecurity experts to investigate and started remediation efforts, including identifying the potentially affected files and engaging a data-review firm to analyze their contents. We received those results in March 2025 and have been working since that time to find updated contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

We determined that the unauthorized third party accessed or acquired some of your personal information, which may include your name, contact information, and Social Security Number.

WHAT WE ARE DOING

Protecting the integrity of the information we maintain is a responsibility we take very seriously. We hired third-party experts to help us address this situation, perform an investigation into the unauthorized activity, and further secure our systems and the information we maintain as we move forward.

WHAT YOU CAN DO

We currently have no evidence that the unauthorized third party has fraudulently used any information involved in this incident. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity and to review the *Additional Steps You Can Take* guidance included in this letter for steps you can take to help protect yourself against fraud. In addition, we are offering a complimentary 1-year membership to Kroll's identity monitoring services. You can find instructions for activating that service in this packet.

THE STANDARD FOR PROTECTION & PERFORMANCE

📍 7990 North Point Blvd. Suite 108, Winston-Salem, NC 27106
📞 877-950-3200
🌐 www.ntpwarranty.com



FOR MORE INFORMATION

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, you can contact us at 336-904-2174 or compliance@ntpc.com. Thank you for your understanding and patience.

Sincerely,

Geoff Sigler

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

- Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.
- You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
- Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Your complimentary identity monitoring services include:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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/Info-Lost-or-Stolen.

- 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. 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. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. 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 charge for requesting a security freeze. 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 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

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Maryland

Attorney General

200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

New York

Attorney General

The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

North Carolina

Attorney General

9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

Washington, DC

Attorney General

400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

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