CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

JORDAN MORGAN
jmorgan@c-wlaw.com

LEI WANG
lwang@c-wlaw.com

December 1, 2022

Via E-Mail (IDTheft@oag.state.md.us)
Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

I serve as counsel for Ingalls & Snyder, LLC ("I&S"), located at 1325 6th Ave, New York, NY 10019, and provide this notification to you of a recent data security incident. By providing this notice, I&S does not waive any rights or defenses under Maryland state law, including the data breach notification statute.

On October 31, 2022, I&S became aware of a ransomware attack that had infiltrated its network. Upon discovery, I&S immediately further secured its network and engaged a third-party forensic firm to investigate the incident. As part of this forensic investigation, I&S sought to determine whether any information may have been compromised by the threat actor who initiated the ransomware attack. During the investigation, on November 3, 2022, I&S discovered that a limited amount of personal information may have been accessed in connection with this incident.

On November 17, 2022, I&S discovered that 386 residents of Maryland may have been affected by this incident. As our investigation is ongoing, we will provide supplemental notification should we determine additional residents of Maryland are potentially affected.

I&S will provide written notice of this incident to the potentially impacted Maryland residents on December 2, 2022 pursuant to Maryland state law. A copy of the notice letter is attached hereto as **Exhibit A**, which provides details of the incident and an offers complimentary credit monitoring and identity protection services for 12 months and access to a dedicated call center.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: ______________________
Jordan Morgan, Esq.

EXHIBIT A

INGALLS & SNYDER
INVESTMENT MANAGEMENT SINCE 1924

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: <<Variable Header>>

<<Salutation>>

Ingalls & Snyder, LLC ("I&S") writes to notify you of a recent incident that may have involved your personal information described below.

I&S takes the privacy of information in its care seriously and has consistently maintained information security programs at a high commercial standard for our industry. While there is no evidence to suggest that any information was misused, I&S is providing you information about the incident, its response, and steps you can take to protect your information if you feel it is necessary to do so.

What Happened:

On or around October 31, 2022, I&S became aware of a network intrusion that affected a limited number of systems. Upon discovery, I&S immediately took measures to further secure its network and engaged a third-party forensic firm to investigate the nature and scope of the incident. On November 3, 2022, following a thorough investigation, I&S discovered that personal information may have been accessed by an unauthorized party in connection with this incident.

At this time, there is no indication that any information has been misused. However, I&S is providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel you would like to do so.

What Information Was Involved:

The potentially accessed information may have included your first and last name, in combination with additional data elements, including but not limited to, your I&S account number, social security or tax ID number, driver's license photo, date of birth, address, and bank account information. Importantly, the information potentially impacted as it relates to you may include all, or just one of the above-listed types of information.

What We Are Doing:

I&S has taken steps to address the incident and is committed to protecting personal information in its care. In response to this incident, I&S has taken additional steps to further secure its systems, and to enhance the security of its network to prevent similar incidents from occurring in the future.

Credit Monitoring:

As a safeguard, I&S has arranged for you to enroll, at no cost to you, in an online credit monitoring and identity protection service for <<CM length 12/24>> months. Due to privacy laws, I&S cannot register you directly. Additional information regarding how to enroll in the complimentary credit monitoring and identity protection service from Equifax is enclosed.

What You Can Do:

In addition to enrolling in the complimentary credit monitoring service detailed within, I&S recommends that you contact your other financial institutions to report the incident and take any recommended actions to protect your accounts from fraud and identity theft. We strongly encourage you to change your passwords and activate multifactor authentication if you have not already done so. In addition, you should remain vigilant in regularly reviewing and monitoring all of your account statements provided by financial institutions with which you maintain accounts and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password(s) and take additional steps to protect your account, and notify your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your State Attorney General. Please review the additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have questions about the details of this incident or the free credit monitoring service, please do not hesitate to contact us at 855-608-2952, Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time, except holidays. You may contact your I&S Account Representative with all other inquiries.

Sincerely,

Ingalls & Snyder, LLC

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

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

As an alternative to a fraud alert, and for enhanced protection, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide some or all of the following information:

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

Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below. If you wish to request a credit freeze, you should contact each of the three credit reporting bureaus listed below separately. Most bureaus now allow you to implement these requests online.

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Ingalls & Snyder, LLC may be contacted at 1325 6th Ave, New York, NY 10019.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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

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

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection. Ingalls & Snyder, LLC may be contacted at 1325 6th Ave, New York, NY 10019.

Enter your Activation Code: *<<ACTIVATION CODE>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of *<<ACTIVATION CODE>>* then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

---

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

JORDAN MORGAN
jmorgan@c-wlaw.com

LEI WANG
lwang@c-wlaw.com

December 28, 2022

Via E-Mail (IDTheft@oag.state.md.us)
Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

I continue to serve as counsel for Ingalls & Snyder, LLC ("I&S"), located at 1325 6th Ave, New York, NY 10019. Please accept this this supplemental notification relating to the recent data security incident suffered by I&S on or about October 31, 2022.

On December 1, 2022, I&S notified your office of this incident and that 386 Maryland residents may have been affected by this incident. A copy of that letter is attached hereto as ***Exhibit A***. Subsequent to that notification, I&S continued to investigate this incident to determine if any additional residents of Maryland were potentially affected. On December 16, 2022, after a thorough investigation, I&S discovered that an additional 45 residents of Maryland were potentially affected by this incident. Following this discovery, I&S promptly notified the additional residents of Maryland via First Class mail on December 23, 2022. A copy of the notice letter is attached hereto as **Exhibit B**, which provides details of the incident and offers complimentary credit monitoring and identity protection services for 12 months and access to a dedicated call center.

I&S continues to take proactive steps to ensure that all state and federal notification obligations are complied with due to this incident. Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

Jordan Morgan, Esq.

EXHIBIT A

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

JORDAN MORGAN
jmorgan@c-wlaw.com

LEI WANG
lwang@c-wlaw.com

December 1, 2022

Via E-Mail (IDTheft@oag.state.md.us)
Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

I serve as counsel for Ingalls & Snyder, LLC ("I&S"), located at 1325 6th Ave, New York, NY 10019, and provide this notification to you of a recent data security incident. By providing this notice, I&S does not waive any rights or defenses under Maryland state law, including the data breach notification statute.

On October 31, 2022, I&S became aware of a ransomware attack that had infiltrated its network. Upon discovery, I&S immediately further secured its network and engaged a third-party forensic firm to investigate the incident. As part of this forensic investigation, I&S sought to determine whether any information may have been compromised by the threat actor who initiated the ransomware attack. During the investigation, on November 3, 2022, I&S discovered that a limited amount of personal information may have been accessed in connection with this incident.

On November 17, 2022, I&S discovered that 386 residents of Maryland may have been affected by this incident. As our investigation is ongoing, we will provide supplemental notification should we determine additional residents of Maryland are potentially affected.

I&S will provide written notice of this incident to the potentially impacted Maryland residents on December 2, 2022 pursuant to Maryland state law. A copy of the notice letter is attached hereto as **Exhibit A**, which provides details of the incident and an offers complimentary credit monitoring and identity protection services for 12 months and access to a dedicated call center.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: ______________________________
Jordan Morgan, Esq.

EXHIBIT B

INGALLS & SNYDER
INVESTMENT MANAGEMENT SINCE 1924

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: <<Variable Header>>

<<Salutation>>

Ingalls & Snyder, LLC ("I&S") writes to notify you of a recent incident that may have involved your personal information described below.

I&S takes the privacy of information in its care seriously and has consistently maintained information security programs at a high commercial standard for our industry. While there is no evidence to suggest that any information was misused, I&S is providing you information about the incident, its response, and steps you can take to protect your information if you feel it is necessary to do so.

What Happened:

On or around October 31, 2022, I&S became aware of a network intrusion that affected a limited number of systems. Upon discovery, I&S immediately took measures to further secure its network and engaged a third-party forensic firm to investigate the nature and scope of the incident. On November 3, 2022, following a thorough investigation, I&S discovered that personal information may have been accessed by an unauthorized party in connection with this incident.

At this time, there is no indication that any information has been misused. However, I&S is providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel you would like to do so.

What Information Was Involved:

The potentially accessed information may have included your first and last name, in combination with additional data elements, including but not limited to, your I&S account number, social security or tax ID number, driver's license photo, date of birth, address, and bank account information. Importantly, the information potentially impacted as it relates to you may include all, or just one of the above-listed types of information.

What We Are Doing:

I&S has taken steps to address the incident and is committed to protecting personal information in its care. In response to this incident, I&S has taken additional steps to further secure its systems, and to enhance the security of its network to prevent similar incidents from occurring in the future.

Credit Monitoring:

As a safeguard, I&S has arranged for you to enroll, at no cost to you, in an online credit monitoring and identity protection service for <<CM length 12/24>> months. Due to privacy laws, I&S cannot register you directly. Additional information regarding how to enroll in the complimentary credit monitoring and identity protection service from Equifax is enclosed.

AH7661 v.04

What You Can Do:

In addition to enrolling in the complimentary credit monitoring service detailed within, I&S recommends that you contact your other financial institutions to report the incident and take any recommended actions to protect your accounts from fraud and identity theft. We strongly encourage you to change your passwords and activate multifactor authentication if you have not already done so. In addition, you should remain vigilant in regularly reviewing and monitoring all of your account statements provided by financial institutions with which you maintain accounts and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password(s) and take additional steps to protect your account, and notify your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your State Attorney General. Please review the additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have questions about the details of this incident or the free credit monitoring service, please do not hesitate to contact us at 855-608-2952, Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time, except holidays. You may contact your I&S Account Representative with all other inquiries.

Sincerely,

Ingalls & Snyder, LLC

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

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

As an alternative to a fraud alert, and for enhanced protection, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide some or all of the following information:

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

Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below. If you wish to request a credit freeze, you should contact each of the three credit reporting bureaus listed below separately. Most bureaus now allow you to implement these requests online.

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Ingalls & Snyder, LLC may be contacted at 1325 6th Ave, New York, NY 10019.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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

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

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection. Ingalls & Snyder, LLC may be contacted at 1325 6th Ave, New York, NY 10019.

Enter your Activation Code: *<<ACTIVATION CODE>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of *<<ACTIVATION CODE>>* then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

---

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*