MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

RECEIVED
JUL 05 2022
CONSUMER PROTECTION

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

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

July 1, 2022

VIA U.S. MAIL

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

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We continue to represent WellDyneRx, LLC ("WellDyne") located at 500 Eagles Landing Drive Lakeland, FL 33810, and write to supplement our June 22, 2022, notice to your office. This notice, which includes a full description of the incident, is attached hereto as ***Exhibit A***. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, WellDyne does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On December 2, 2021, WellDyne became aware of suspicious activity related to a WellDyne email account. In response, WellDyne began an investigation of the activity with the assistance of third-party forensic investigators to determine the nature and scope of the incident. WellDyne determined that there was unauthorized access to the account between October 30, 2021, and November 17, 2021. Although there is no evidence that individually-identifiable information contained within the email account was accessed or taken by an unauthorized party, WellDyne could not rule out this possibility. In response, WellDyne undertook a comprehensive and time-consuming programmatic and manual review of the contents of the email account to determine the type of information stored therein, and to whom the information pertained. On March 11, 2022, WellDyne completed this extensive review process, and identified the scope of the information at risk and the population potentially impacted. WellDyne worked diligently since this time to confirm the contact information for the individuals who may be impacted and the types of information at issue for each individual, as well as to identify and notify applicable data-owner

entities. WellDyne began providing notice of this incident on May 6, 2022, to the potentially impacted individuals for whom WellDyne was determined to be the data owner with respect to the impacted information. Since this time, WellDyne continued working to match the potentially impacted individuals back to its covered entity clients in order to make the appropriate notifications.

The information that may have been affected by this event includes the following: name, date of birth, Social Security number, driver's license number, treatment information, health insurance information, contact information, prescription information, and other medical/health information.

Notice to New Hampshire Residents

On June 22, 2022, WellDyne began providing written notice of this incident to affected individuals, which included thirteen (13) New Hampshire residents. On June 29, 2022, WellDyne provided written notice to an additional twenty-eight (28) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, WellDyne moved quickly to investigate and respond to the incident, assess the security of its email tenant, and notify potentially affected individuals. WellDyne is also working to implement additional security to its network. WellDyne is providing access to credit monitoring services for one (1) year through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, WellDyne is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. WellDyne is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

On May 6, 2022, WellDyne provided written notice to the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA). WellDyne also provided written notice of this incident to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/smm
Enclosure

EXHIBIT A

MULLEN
COUGHLIN

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

FIRST-CLASS

US POSTAGE™ PITNEY BOWES

ZIP 19333
02 7H
0001297298

$ 000.53⁰
JUN 22 2022

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

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

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

June 22, 2022

VIA E-MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent WellDyneRx, LLC ("WellDyne") located at 500 Eagles Landing Drive Lakeland, FL 33810, and are writing to notify your office of an incident that may affect the security of information relating to one (1) New Hampshire resident. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, WellDyne does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On December 2, 2021, WellDyne became aware of suspicious activity related to a WellDyne email account. In response, WellDyne began an investigation of the activity with the assistance of third-party forensic investigators to determine the nature and scope of the incident. WellDyne determined that there was unauthorized access to the account between October 30, 2021, and November 17, 2021. Although there is no evidence that individually-identifiable information contained within the email account was accessed or taken by an unauthorized party, WellDyne could not rule out this possibility. In response, WellDyne undertook a comprehensive and time-consuming programmatic and manual review of the contents of the email account to determine the type of information stored therein, and to whom the information pertained. On March 11, 2022, WellDyne completed this extensive review process, and identified the scope of the information at risk and the population potentially impacted. WellDyne worked diligently since this time to confirm the contact information for the individuals who may be impacted and the types of

information at issue for each individual, as well as to identify and notify applicable data-owner entities. WellDyne began providing notice of this incident on May 6, 2022, to the potentially impacted individuals for whom WellDyne was determined to be the data owner with respect to the impacted information. Since this time, WellDyne continued working to match the potentially impacted individuals back to its covered entity clients in order to make the appropriate notifications. WellDyne is now providing notice directly to those for whom it has been unable to match to an appropriate covered entity data owner.

The information that may have been affected by this event includes the following: name, date of birth, Social Security number, driver's license number, treatment information, health insurance information, contact information, prescription information, and other medical/health information.

Notice to New Hampshire Resident

On June 22, 2022, WellDyne provided written notice of this incident to the additional potentially affected individuals that were unable to be matched back to any of its covered entity clients, which includes approximately one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, WellDyne moved quickly to investigate and respond to the incident, assess the security of its email tenant, and notify potentially affected individuals. WellDyne is also working to implement additional security to its network. WellDyne is providing access to credit monitoring services for one (1) year through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, WellDyne is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. WellDyne is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

On May 6, 2022, WellDyne provided written notice to the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA). WellDyne also provided written notice of this incident to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/RZH
Enclosure

EXHIBIT A

Return Mail Processing Center
P.O. 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>>

Dear <<Name 1>>:

[IF AG700 - W4 Adult 1]
<<WellDyneRx, LLC ("WellDyne") is writing to notify you of a recent incident that may have impacted the privacy of your information. WellDyne is a mail-order pharmacy and we have your information in connection with the pharmacy services we provided to you. We want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.>>

[IF AG701 - W4 Adult 2]
<<WellDyneRx, LLC ("WellDyne") is writing to notify you of a recent incident that may have impacted the privacy of your information. WellDyne is a pharmacy benefit management company, and we received your information in connection with the services we provide to you, or to one of your benefit providers. We want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.>>

What Happened? On December 2, 2021, we became aware of suspicious activity related to a WellDyne email account. In response, we began an investigation of the activity with the assistance of third-party forensic investigators to determine the nature and scope of the incident. We determined that there was unauthorized access to the account between October 30, 2021, and November 17, 2021. Although there is no evidence that individually-identifiable information contained within the email account was accessed or taken by an unauthorized party, we cannot rule out this possibility. In response, WellDyne undertook a comprehensive and time-consuming programmatic and manual review of the contents of the email account to determine the type of information stored therein, and to whom the information pertained. On March 11, 2022, we completed this extensive review process, and identified that information pertaining to you was present in the accessed email account at the time of unauthorized access. While we are unaware of any actual or attempted misuse of your information as a result of this incident, we take the security of data we hold very seriously and are notifying you out of an abundance of caution.

What Information Was Involved? The investigation determined that your name, <<Breached Elements>> may have been affected by this event.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care is among our highest priorities. Upon learning of the event, we secured the compromised account and investigated to identify any individuals that were affected. We have taken additional steps to improve security and better protect against similar incidents in the future. We are also notifying applicable regulators, including the Department of Health and Human Services.

Although we are unaware of any actual or attempted misuse of your personal information as a result of this event, out of an abundance of caution, we are offering you access to complimentary credit monitoring and identity theft protection services for <<CM Length>> months through Equifax. Please note that you will not be automatically enrolled in these services. Should you find it appropriate to do so, we encourage you to enroll yourself in these services, as we are not able to do so on your behalf. You may find instructions on how to enroll in these services in the attached *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the credit monitoring and identity theft protection services we are making available to you, free of cost.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 877-389-2455, Monday-Friday: 9am to 9pm Eastern time. You may also write to us at 500 Eagles Landing Drive Lakeland, FL 33810, Attn: Privacy Officer.

We regret any inconvenience this incident may cause you. WellDyne remains committed to safeguarding information in our care, and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,

Phil Bisesi
Chief Compliance and Privacy Officer

Steps You Can Take to Help Protect Personal Information

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.*

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

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

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in

your credit report; and you may seek damages from 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 www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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

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

EXHIBIT B

[WellDyneRx LOGO]

<<Return Mail Address>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>> <<Name 2>>:

WellDyneRx, LLC ("WellDyne") is writing to notify you of a recent incident that may have impacted the privacy of your information. WellDyne is a pharmacy benefit management company, and we received your information in connection with the services we provide to you, or to one of your benefit providers. We want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened? On December 2, 2021, we became aware of suspicious activity related to a WellDyne email account. In response, we began an investigation of the activity with the assistance of third-party forensic investigators to determine the nature and scope of the incident. We determined that there was unauthorized access to the account between October 30, 2021, and November 17, 2021. Although there is no evidence that individually-identifiable information contained within the email account was accessed or taken by an unauthorized party, we cannot rule out this possibility. In response, WellDyne undertook a comprehensive and time-consuming programmatic and manual review of the contents of the email account to determine the type of information stored therein, and to whom the information pertained. On March 11, 2022, we completed this extensive review process, and identified that information pertaining to you was present in the accessed email account at the time of unauthorized access. While we are unaware of any actual or attempted misuse of your information as a result of this incident, we take the security of data we hold very seriously and are notifying you out of an abundance of caution.

What Information Was Involved? The investigation determined that your name, [Variable Text 1] may have been affected by this event.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care is among our highest priorities. Upon learning of the event, we secured the compromised account and investigated to identify any individuals that were affected. We have taken additional steps to improve security and better protect against similar incidents in the future. We are also notifying applicable regulators, including the Department of Health and Human Services.

Although we are unaware of any actual or attempted misuse of your personal information as a result of this event, out of an abundance of caution, we are offering you access to complimentary credit monitoring and identity theft protection services for [Variable Text 2] months through Equifax. Please note that you will not be automatically enrolled in these services. Should you find it appropriate to do so, we encourage you to enroll yourself in these services, as we are not able to do so on your behalf. You may find instructions on how to enroll in these services in the attached *Steps You Can Take to Help Protect Personal Information.*

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information.* There you will also find more information on the credit monitoring and identity theft protection services we are making available to you, free of cost.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 877-389-2455, Monday-Friday: 9am to 9pm Eastern time. You may also write to us at 500 Eagles Landing Drive Lakeland, FL 33810, Attn: Privacy Officer.

We regret any inconvenience this incident may cause you. WellDyne remains committed to safeguarding information in our care, and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,

Phil Bisesi
Chief Compliance and Privacy Officer

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enter your Activation Code: *<ACTIVATION CODE>*
Enrollment Deadline: *<DEADLINE MMMM DD, YYYY>*

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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

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

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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

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

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

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this incident.

NH DEPT OF JUSTICE
JUL 5 2022 PM3:14