



May 12, 2022

BY EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

Assurance IQ, LLC ("Assurance") and USA Family Protection Insurance Services, LLC ("USA Family") (together with Assurance, "we" or "us") are notifying you, pursuant to Md. Code Ann. Comm. Law 14-3504, of a cybersecurity event involving an online digital insurance application platform operated by Assurance for a life insurance product offered through USA Family on [REDACTED]

Assurance is a licensed insurance agency headquartered in Seattle, WA and operates websites that allow consumers to obtain quotes and purchase insurance products issued by various insurance carriers. [REDACTED]
[REDACTED]

[REDACTED]

Based on our investigation to date, we have determined that one or more unauthorized third parties entered an individual's name, along with a mailing address, date of birth, and other information purported to be associated with the individual into an online life insurance application. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Our investigation to date has identified unauthorized activity beginning on November 13, 2020 and continuing intermittently until April 1, 2022, when we implemented measures designed to prevent further data exposure.

We are not able to confirm the accuracy of the personal information provided by the unauthorized third party or whether the driver's license number displayed in fact belongs to the individual whose information was entered. At this time, for purposes of assessing our

obligations under applicable law, we are proceeding on the assumption that the displayed driver's license number was that of the individual whose information was entered.

[REDACTED]

To date, we have determined that the driver's license numbers of 131 Maryland residents may have been displayed to an unauthorized third party. Our investigation remains ongoing.

Attached is a sample notification letter we expect to begin sending to Maryland residents on May 13, 2022.

[REDACTED]

[REDACTED]

We take this matter very seriously and are committed to answering any questions you may have. If you have any questions regarding this submission, please do not hesitate to contact us.

* * *

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Sincerely,

Douglas Morrin
Chief Legal Officer
Assurance IQ, LLC
dmorrin@assurance.com

Gary Jenkins
Head Legal Counsel
USA Family Protection Insurance Services, LLC
gary_jenkins@swissre.com



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

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

NOTICE OF SECURITY INCIDENT

Dear <<first_name>>,

We are writing to let you know about an incident that affected an online digital insurance application platform operated by Assurance IQ, LLC (“Assurance”) for consumers to apply for certain life insurance products offered through USA Family Protection Insurance Services, LLC on behalf of its affiliated insurance company, Lumico Life Insurance Company (together, “USA Family”).

We want to make clear at the outset that keeping personal data safe and secure is very important to both Assurance and USA Family, and will continue to be a priority moving forward.

WHAT HAPPENED?

We have learned that an unauthorized third party or parties may have obtained the driver’s license numbers of certain individuals through an online life insurance application process hosted on Assurance’s websites. We are conducting a thorough investigation. Based on our investigation to date, we believe that this unauthorized activity, which was limited to the use of Assurance’s public-facing websites, began in November 2020 and continued intermittently through April 1, 2022, when we implemented measures designed to prevent further data exposure.

Our investigation has determined that an unauthorized third party entered your name, along with a mailing address, date of birth, or other information purported to be associated with you, into the online life insurance application. We believe your name, address, and other information were obtained by the unauthorized third party from external sources and not from Assurance or USA Family, companies that may be unfamiliar to you if you have never applied for life insurance on Assurance websites. Based on that information, USA Family retrieved a driver’s license number that was then displayed to the unauthorized third party in the online application hosted by Assurance.

We have notified law enforcement of this incident, but have not delayed this notification as a result of any law enforcement investigation.

WHAT INFORMATION WAS INVOLVED?

The personal information that may have been exposed was limited to your driver’s license number and state of issuance. However, we are not able to confirm the accuracy of the personal information provided by the unauthorized third party or whether the driver’s license number displayed in fact belongs to you. We are offering the identity monitoring services below out of an abundance of caution.

Please note that no insurance policy or other product was issued in your name in connection with this incident, and we have no information suggesting that your driver’s license number has been misused.

WHAT WE ARE DOING

Upon learning about this unauthorized activity, we promptly began an investigation and took action to address this incident, including by taking steps to prevent unauthorized actors from obtaining further personal information.

We have also secured the services of Kroll to provide identity monitoring services at no cost to you for two years. 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.

<<Date>> (Format: Month Day, Year)
Membership Number: <<Membership Number s_n>>
Activation Deadline: <<b2b_text_6(activation deadline)>>

Below please find information on signing up for a complimentary membership to Kroll's identity monitoring services.

The identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, 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.

Additional information describing your services is included at the end of this letter.

WHAT YOU CAN DO

We encourage you to contact Kroll and take advantage of the identity monitoring services we are providing to you free of charge. In addition, you should remain vigilant and carefully review your accounts for any suspicious activity. This is a best practice for all consumers.

As noted above, we have no evidence that your information has been misused. However, as always, if you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or other company with which the account is maintained and any relevant government agency, such as your State Department of Motor Vehicles.

If you would like to take additional steps to help protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

We take our responsibility to protect your information extremely seriously, and we sincerely regret any inconvenience that this matter has caused you.

If you have any questions, please contact us at **(855) 788-2608**, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

Nicholas Howard
Chief Information Officer
Assurance IQ, LLC
920 5th Ave, Ste 3600
Seattle, WA 98104

Michael Nawrath
Chief Information Security Officer
USA Family Protection Insurance Services, Inc.
175 King Street
Armonk, NY 10504

<<Date>> (Format: Month Day, Year)
Membership Number: <<Membership Number s_n>>
Activation Deadline: <<b2b_text_6(activation deadline)>>

Additional Resources

Below are additional helpful tips you may want to consider to help protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at <https://www.annualcreditreport.com/manualRequestForm.action>. Credit reporting agency contact details are provided below.

Equifax:

equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
866-349-5191

Experian:

experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:

transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 1 year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

<<Date>> (Format: Month Day, Year)
Membership Number: <<Membership Number s_n>>
Activation Deadline: <<b2b_text_6(activation deadline)>>

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies 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 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. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado, Delaware, and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov>, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov>, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Georgia, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

<<Date>> (Format: Month Day, Year)
Membership Number: <<Membership Number s_n>>
Activation Deadline: <<b2b_text_6(activation deadline)>>



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will 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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.



November 29, 2022

BY EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

Assurance IQ, LLC ("Assurance") and USA Family Protection Insurance Services, LLC ("USA Family") (together with Assurance, "we" or "us") are providing an update regarding the cybersecurity event we first notified you about on May 12, 2022 [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

We are providing this update because our investigation into the root cause, timeline, and scope of the incident is now substantially complete.

We determined that the driver's license numbers of 166 Maryland residents might have been displayed to an unauthorized third party. We notified the potentially affected Maryland residents on May 13, 2022 and May 31, 2022, using the sample notification letter we previously shared with you.

We take this matter very seriously and are committed to answering any questions you may have. If you have any questions regarding this supplemental submission, please do not hesitate to contact us.

* * *

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Sincerely,

[REDACTED]