



Kaylee Cox Bankston
+1 202 346 4399
KBankston@goodwinlaw.com

Goodwin Procter LLP
1900 N Street, NW
Washington, DC 20036

goodwinlaw.com
+1 202 346 4000

June 6, 2023

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
VIA EMAIL: IDTheft@oag.state.md.us

Re: Notice Pursuant to MD Commercial Code § 14–3501(e)

Dear Attorney General Brown,

Pursuant to *Maryland Commercial Code section 14–3501(e)*, we write on behalf of AnnuityRateWatch.com, Inc. (“AnnuityRateWatch”) to notify you of a data security matter, which we believe impacted approximately seven (7) Maryland residents. AnnuityRateWatch provides financial professionals with research tools for fixed and fixed-indexed annuities is located at 10 Main St, Lakeville, MA 02347.

On or around January 15, 2023, AnnuityRateWatch was the victim of a cybersecurity attack by an unauthorized party. Upon detecting the attack, AnnuityRateWatch initiated an investigation with the assistance of cybersecurity experts, including third-party forensic professionals. On or around March 23, 2023, our investigation identified potential unauthorized access to certain databases on our systems that contained customer information. We then conducted a comprehensive evaluation of the potentially impacted data in order to determine the nature of personal information that may have been impacted and the scope of the impacted population and to confirm address information for impacted individuals. This process was completed on or around May 23, 2023.

The types of personal information that may have been impacted during this incident include: cardholder first and last name, payment card number, billing address, expiration date, and CVV number. The impacted information may have also included customers’ email and phone number.

AnnuityRateWatch determined that the impacted population included seven (7) Maryland residents. Notification of this matter will be mailed to the impacted residents on or around June 6, 2023. A copy of this notification is attached as **Exhibit A**.

AnnuityRateWatch takes the protection of customer information seriously. AnnuityRateWatch is offering two years of identity protection services, at no cost, to affected customers through Experian. In response to this matter, AnnuityRateWatch also has taken steps to further enhance its security protocols. The Company is also in the process of evaluating and investigating this matter further in order to prevent a similar occurrence in the future.

Below is the contact information for Mark Legan, CEO at AnnuityRateWatch:

Mark Legan, CEO
AnnuityRateWatch.com, Inc.
508-947-9388 (Office)
mark.legan@annuityratelaw.com



Office of the Attorney General
Page 2

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,

A handwritten signature in black ink, reading 'Kaylee Cox Bankston', written over a light gray rectangular background.

Kaylee Cox Bankston

Exhibit A

AnnuityRateWatch.com, Inc

Return Mail Processing
PO Box 999
Suwanee, GA 30024

4 1 644 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



June 5, 2023

RE: NOTICE OF DATA BREACH

Dear Sample A. Sample:

AnnuityRateWatch.com, Inc. ("AnnuityRateWatch") is writing to let you know about a data security incident and to recommend steps that you can take to help protect yourself.

What Happened

AnnuityRateWatch discovered that, on or around January 15, 2023, an unauthorized party gained access to certain databases on our systems that contained certain customer information.

You have been identified as one of the individuals whose information may have been impacted by this incident. We are notifying you of the incident in order to provide you with information and steps you can take to help protect your information. Please note that this notification was not delayed as a result of any law enforcement investigation.

What Information Was Involved

At this time, we believe the impacted information may have included data pertaining to the credit or debit card you used to purchase products or services on our website, including: cardholder first and last name, payment card number, billing address, expiration date, and CVV number. The impacted information may have also included your email and phone number.

What We Are Doing

We take the protection of your information seriously, and we regret that this incident occurred. Upon learning of this incident, we initiated an investigation and retained third-party cybersecurity experts to support our investigation. We also have implemented technical and procedural measures in an effort to help prevent a similar occurrence from happening again.

We are also offering you, at our expense, **identity protection services for 2 years**, as described further in this letter.

What You Can Do

There are steps you can take to protect yourself, including enrolling in the free identity protection service we are offering. Details regarding the service and how to enroll are provided below.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** August 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 420 2879** by August 31, 2023. Be prepared to provide engagement number **B092475** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information

We have attached information regarding additional actions you may consider to help reduce the chances of identity theft or fraud on your account as well as resources to obtain additional information about identity theft and ways to protect yourself.

Questions and Concerns

We regret this incident occurred and any inconvenience it may cause you, and encourage you to take advantage of the Experian services. If you have further questions or concerns, or would like an alternative to enrolling online, please call **(833) 420 2879** toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number **B092475**.

Sincerely,

Mark Legan, CEO
AnnuityRateWatch.com, Inc.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

The Federal Trade Commission

600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Credit Reporting Agencies

Equifax

PO Box 740241
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Experian

PO Box 4500
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

PO Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For Maryland Residents. You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023
www.oag.state.md.us

For Massachusetts Residents: You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office:

New York Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
<https://ag.ny.gov/>

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center Raleigh,
NC 27699-9001
1-877-5-NO-SCAM
www.ncdoi.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street Providence, RI 02903
1-401-274-4400
riag.ri.gov