

Morgan Lewis

Ezra D. Church

Partner
215.963.5710
ezra.church@morganlewis.com

September 22, 2022

VIA EMAIL TO IDTHEFT@OAG.STATE.MD.US

State of Maryland
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
Attn: Security Breach Notification

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents Validity Finance, LLC ("Validity") and we are writing to notify your office and provide details regarding the nature and circumstances of a recent data security incident.

On or about July 18, 2022, it came to Validity's attention that on July 17, 2022, an email account for one of its employees was compromised. Validity immediately consulted with cybersecurity experts to investigate what happened and make sure its system was secure. With the assistance of counsel, Validity also reviewed the affected email account to determine whether the hacker may have accessed any personal information. On or about September 9, 2022, Validity determined that certain personal information may have been exposed to the hacker, including information such as names, addresses, social security numbers, dates of birth, passport numbers, and/or driver's license numbers. Validity has no reason to believe that any personal information accessed has been used inappropriately, but out of an abundance of caution, we are sending this notice to you.

Although Validity is not aware of any instance of fraud or misuse of personal information, Validity will send notifications by mail or electronic mail to the affected individuals to explain what happened, what information was involved, what Validity has done, and how affected individuals can contact Validity with questions. Validity is also making an offer of two years of credit monitoring to the affected individuals.

Since learning of this incident, Validity has consulted with third-party cyber experts to better understand what happened and to prevent a similar incident in the future. Validity has also taken steps to strengthen the security of its systems, including by implementing password resets for all system users, adding password security programs, and implementing additional safeguards. Validity will continue with these efforts.

Morgan, Lewis & Bockius LLP

1701 Market Street
Philadelphia, PA 19103-2921
United States

T +1.215.963.5000
F +1.215.963.5001

State of Maryland
Office of the Attorney General
September 22, 2022
Page 2

Further information about what Validity has done and is recommending to the individuals in question can be found in the enclosed notification that Validity will send to four (4) Maryland residents via email and/or mail on September 22, 2022.

If you have any questions, please do not hesitate to contact me.

Regards,

A handwritten signature in dark ink, appearing to read "E.D. Church", is written over a light gray rectangular background.

Ezra D. Church

Enclosure

Validity Finance, LLC
1270 Avenue of the Americas
New York, NY 10020
(646) 798-7168



September 22, 2022

Notice of Data Breach

Dear [REDACTED]:

We write to notify you of an incident that occurred that could affect some of your personal information. Please review this letter carefully. We truly regret any inconvenience to you, and have undertaken numerous steps to secure our system.

What Happened?

On or about July 18, 2022, Validity learned that an email account for one of its employees had been compromised. We immediately consulted with cybersecurity experts to investigate what happened and make sure our system was secure.

What Information Was Involved?

After review of the affected email account, our counsel, Morgan Lewis, reviewed the relevant emails in the affected account. Morgan Lewis determined that certain personal information may have been exposed to the hacker, including information such as names, addresses, social security numbers, dates of birth, passport numbers, and/or driver's license numbers. *However, we are not aware of any instance of fraud or misuse of personal information at this time.*

What We Are Doing

Upon becoming aware of the breach, we consulted with cybersecurity experts, in addition to counsel, to investigate the scope of what happened. Working with our experts, we confirmed that only one user's email account was compromised. Nor did the breach extend to any other Validity system, fortunately. We implemented password resets for all system users, added password security programs and our cybersecurity experts implemented additional safeguards.

Although, as mentioned, we are not aware of any instances of fraud or misuse to date, we are offering complimentary access to credit monitoring and identity theft protection through Experian's® IdentityWorksSM for 24 months, at no cost to you.

To activate your IdentityWorksSM membership and start monitoring your credit and personal information, please follow the steps below:

- Ensure that you **enroll by 5:59 p.m. CT on December 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** [REDACTED]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332** by **December 31, 2022**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

Additional details on the IdentityWorksSM service and other security suggestions are provided in the attached "Additional Resources."

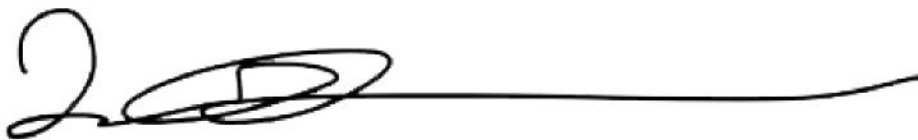
What You Can Do

We strongly recommend that you remain alert for incidents of fraud and identity theft, including regular monitoring of your account statements and free credit reports. For more information on how you can help protect yourself, please review the enclosed "Steps You Can Take to Protect Your Information."

For More Information

Again, we are sorry for any inconvenience caused by this incident. If you have further questions or concerns, need assistance with identity restoration, or would like an alternative to enrolling in credit monitoring online, please contact Jason Listhaus, our general counsel, Monday through Friday from 8 am–6 PM Eastern.

Sincerely,

A handwritten signature in black ink, appearing to read 'R. Sutton', followed by a long horizontal line extending to the right.

Ralph J. Sutton
Chief Executive Officer

ADDITIONAL RESOURCES

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, Equifax and Transunion files 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.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 at 877-890-9332. 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. You will also find self-help tips and information about identity protection at this site.

* 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.

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, 1-877-3228228. 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, military identification, 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 fraud alert or 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

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; 1877-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, you can obtain information from the Federal Trade Commission and the Office of the District of Columbia Attorney General about steps to take to avoid identity theft. You can contact the D.C. Attorney General: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Iowa Residents, state law advises to you to report any suspected identity theft to law enforcement or the Attorney General.

For Maryland residents, you can obtain information from the Maryland Attorney General about steps that you can take to help prevent identity theft: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For Massachusetts residents, you have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

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 a 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, you may contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office Bureau of Internet and Technology (212) 416-8433 https://ag.ny.gov/internet/resource-center	NYS Department of State's Division of Consumer Protection (800) 697-1220 https://www.dos.ny.gov/consumerprotection
--	--

For North Carolina residents, you can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

For Oregon residents, state laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

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 information about steps you can take to help prevent identity theft and a copy of any police report filed in regard to this incident. There are approximately [#] Rhode Island residents impacted by this incident.