Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

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

April 4, 2022

VIA E-MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Cherry Bekaert, LLP ("Cherry Bekaert") located at 6806 Paragon Place, Suite 310, Richmond, VA, 23230, and are writing to notify your office of an incident that may affect the security of some personal information relating to approximately 10 Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Cherry Bekaert does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around September 8, 2021, Cherry Bekaert discovered that an employee's email account was accessed by an unauthorized user. Cherry Bekaert immediately launched an investigation to determine the nature and scope of the event, working with the assistance of third-party forensic specialists. On February 17, 2022, Cherry Bekaert determined that certain personal information was included in the accessed employee email account. To date, Cherry Bekaert has no evidence that any personal information has been misused.

The information that could have been subject to unauthorized access includes name, address, Social Security number, date of birth, driver's license number, passport number, financial account information, and medical treatment information.

Notice to Maryland Residents

On or about April 4, 2022, Cherry Bekaert began providing written notice of this incident to affected individuals, which includes approximately 10 Maryland residents. 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, Cherry Bekaert moved quickly to investigate and respond to the incident, assess the security of Cherry Bekaert systems, and notify potentially affected individuals. Cherry Bekaert is also working to implement additional safeguards and training to its employees. Cherry Bekaert is providing access to credit monitoring services for 1 year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Cherry Bekaert 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. Cherry Bekaert 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/lhw
Enclosure

EXHIBIT A

Cherry Bekaert LLP
CPAs & Advisors

200 South 10th Street, Suite 900
Richmond, VA 23219

[redacted]

4/4/2022

NOTICE OF SECURITY INCIDENT

Dear [redacted]:

Cherry Bekaert, LLP writes to notify you of a recent event that may affect the security of some of your personal information. Although we have no indication that your information has been misused, we are providing you with information about the event, our response to it, and steps you can take to protect your personal information, should you feel it appropriate to do so.

What Happened? On or around September 10, 2021, we discovered that an employee's email account was accessed by an unauthorized user. We immediately launched an investigation to determine the nature and scope of this event. Through this investigation we determined that the account may have been accessed between September 8, 2021 and September 10, 2021. We then reviewed the contents of the account to determine what information may have been accessible within the email account. On February 17, 2022, we determined that your personal information was contained within employee email account. To date, we have no evidence that your personal information has been misused.

What Information Was Involved? Our investigation determined that the potentially accessed information within the email account includes your name, Driver's License, Passport number, Social Security number, and financial account information.

What We Are Doing. Safeguarding the privacy of information in our care and the security of our network is among our highest priorities. Upon learning of this event, we took appropriate measures to evaluate the security of our systems and confirm the exact personal information potentially impacted.

As an added precaution, we are offering you access to 12 months of credit monitoring through Kroll at no cost to you. More information about these services and instructions on how to enroll may be found in the enclosed "Steps You Can Take to Protect Personal Information." We are unable to act on your behalf so if you would like to enroll in these services, please follow the instructions in the enclosure.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. Please review the enclosed "Steps You Can Take to Protect Personal Information" for instructions on how to enroll in the free credit monitoring services we are providing to you and to learn about additional ways to protect your personal information, should you feel it appropriate to do so.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call [Phone number] at [Time].

Sincerely,

Cherry Bekaert, LLP

Cherry Bekaert, LLP

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

<u>Enroll in Credit Monitoring</u>

<u>How to Activate Your Identity Monitoring Services</u>

1. You must activate your identity monitoring services by **October 31, 2022.** Your Activation Code will not work after this date.
2. Visit **https://enroll.idheadquarters.com/redeem** to activate your identity monitoring services.
3. Provide Your Activation Code: [redacted] and Your Verification ID: [redacted].
4. To sign into your account <u>after you have activated</u> your identity monitoring services, please visit **https://enroll.idheadquarters.com/redeem**

<u>Take Advantage of Your Identity Monitoring Services</u>

You've been provided with access to the following services[1] 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'll have the option to call a Kroll fraud specialist, who can help you determine if it's 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'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

1 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.

507-0220

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 Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us. You may write to Cherry Bekaert at: 200 South 10th Street, Suite 900, Richmond, VA 23219.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.