



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

July 25, 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 Hanbury Evans Wright Vlattas + Company (“Hanbury”) located at 120 Atlantic Street, Suite 100, Norfolk, VA 23510, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately two (2) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Hanbury 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 March 22, 2022, Hanbury discovered unauthorized access to certain computer systems on their network. Hanbury immediately took steps to secure their systems and launched an investigation with the assistance of third-party computer forensic specialists to determine what may have happened. The investigation determined that an unknown actor gained access to certain computer systems on the Hanbury network, and on or about March 20, 2022, accessed and/or acquired certain files from these systems. Hanbury then undertook an extensive review of the acquired files and folders, with the assistance of an outside vendor, to identify any sensitive information stored therein and to whom it relates. On June 10, 2022, Hanbury determined information related to two (2) Maryland residents was potentially accessed.

The information that could have been subject to unauthorized access includes name, Social Security number, passport number, and financial account information.

Notice to Maryland Residents

On July 25, 2022, Hanbury began providing written notice of this incident to approximately two (2) 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, Hanbury moved quickly to investigate and respond to the incident, assess the security of Hanbury's systems, and identify potentially affected individuals. Further, Hanbury notified federal law enforcement regarding the event. Hanbury is also working to implement additional security measures to help protect the information in its care. Hanbury is providing access to credit monitoring services for 24 months, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Hanbury is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Hanbury 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) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/jpc
Enclosure

EXHIBIT A



HANBURY

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF SECURITY INCIDENT

Dear <<Name 1>>:

Hanbury Evans Wright Vlattas + Company (“Hanbury”) is writing to notify you of a recent incident that may have impacted the security of some of your information. This letter provides details of the incident, our response to date, and resources available to help protect your information, should you feel it is appropriate to do so.

What Happened? On March 22, 2022, Hanbury discovered unauthorized access to certain computer systems on our network. We immediately took steps to secure our systems and launched an investigation with the assistance of third-party computer forensic specialists to determine what may have happened. The investigation determined that an unknown actor gained access to certain computer systems on our network, and on or about March 20, 2022, accessed and/or acquired certain files from these systems. We have identified the affected files and conducted a thorough review of each file to identify whether any personal information is contained therein and to whom that information relates. As a result of this review, which was completed by June 10, 2022, we determined that some of your information was contained in the affected files.

What Information Was Involved? Our review determined that the following types of your information were present in the files that were accessed or acquired by the unauthorized actor: your name, <<Breached elements>>. The investigation was unable to determine whether your specific information was actually viewed, and we have no evidence of actual or attempted fraud resulting from this incident.

What We Are Doing. The security of information on our systems is one of our highest priorities, and Hanbury has strict security measures in place to protect the information in our care. Following discovery of this incident, we took immediate steps to secure our environment and are in the process of implementing additional security measures.

We are also offering credit and identity monitoring services for 24 months through Epiq at no cost to you. Information and instructions on how to activate these complimentary services can be found in the “Steps You Can Take to Help Protect Your Information” attached to this letter.

What You Can Do. While Hanbury has no evidence of any actual or attempted misuse of your information related to this incident, 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 and to detect errors. You may also activate to receive the complimentary credit and identity monitoring services we are making available to you. Further information is enclosed in the “Steps You Can Take To Protect Personal Information” insert.

For More Information. If you have questions regarding this letter, please contact our dedicated call center at 877-559-7158 Monday through Friday, between the hours of 9:00 a.m. and 9:00 p.m.

We sincerely regret any inconvenience this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

A handwritten signature in cursive script, appearing to read "Chrissy Gahm".

Chrissy Gahm
Finance Director
Hanbury Evans Wright Vlattas + Company

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Identity Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online 3-bureau credit monitoring service (*myTrueIdentity*) for 24 months provided by TransUnionInteractive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, 3-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Insert static 6-digit Telephone Pass Code >> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain 24 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily 3-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online 3-Bureau Credit Monitoring service anytime between now and <<Insert Date>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit files at TransUnion®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

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 credit freeze, you may need to provide the following information, depending on whether you make the request online, by phone, or by mail:

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.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning 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
1-888-298-0045	1-888-397-3742	1-833-395-6938
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. Hanbury is located at 120 Atlantic Street, Suite 100, Norfolk, VA 23510.

Under Massachusetts law, you have the right to obtain any police report filed in regard to 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.

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.