MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Matthew V. Toldero
Office: (267) 930-4554
Fax: (267) 930-4771
Email: mtoldero@mullen.law

19109 West Catawba Avenue, Suite 200
Cornelius, NC 28031

January 9, 2023

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

To Whom It May Concern:

We represent CH Holdings USA, Inc. ("CH Holdings") located at 10733 Sunset Office Drive, #200, St. Louis, MO, 63127 and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, CH Holdings 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 October 12, 2022, CH Holdings noticed suspicious activity related to a single employee's email account (the "Event"). Upon learning of the Event, CH Holdings launched an investigation into the nature and scope of the Event. CH Holdings, with the assistance of data privacy counsel, and a third-party forensic investigator, conducted a thorough forensic investigation of the email tenant to identify any potential unauthorized access to the account.

The investigation determined that two (2) employee email accounts may have been subject to unauthorized access as a result of the Event. Upon confirmation that the two accounts were likely subject to unauthorized access, CH Holdings undertook a thorough and intensive manual review of the email accounts to identify whether any personal information was contained therein. The review, which concluded on December 14, 2022, determined that personal information relating to one (1) Maryland resident was contained within one of the accounts potentially subject to unauthorized access.

The information that could have been subject to unauthorized access includes name and financial account information.

Notice to Maryland Resident

On January 9, 2023, CH Holdings provided written notice of this Event to one (1) Maryland resident. 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, CH Holdings moved quickly to investigate and respond to the Event, assess the security of CH Holdings systems, and identify potentially affected individuals. CH Holdings is also working to implement additional safeguards and training to its employees. CH Holdings is providing access to credit monitoring services for one (1) year, through Experian, to the individual whose personal information was potentially affected by this Event, at no cost to the individual.

Additionally, CH Holdings is providing the impacted individual with guidance on how to better protect against identity theft and fraud. CH Holdings is providing the individual 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.

CH Holdings is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4554.

Very truly yours,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/rmm
Enclosure

EXHIBIT A

ST. LOUIS OFFICE
10733 Sunset Drive, Suite 200
St. Louis, MO 63127

P 651 796 6100 **F** 651 994 6360

[Name]
[Address 1]
[Address 2]

January 6, 2023

Dear [Name]:

CH Holdings USA, Inc. ("CH Holdings") writes to inform you about a recent event that may impact the security of some of your personal information. Although we have received no indication of any actual or attempted misuse of your information as a result of this event, this notice provides information about the event, our response, and resources available to help protect your information from possible misuses.

What Happened? On or about October 11, 2022, CH Holdings' IT Team became aware of unusual activity related to an employee's email account. We immediately launched an investigation into the suspicious activity and learned that an unauthorized actor gained access to an email account belonging to an Accounts Payable employee. We immediately took steps to secure the email account and to ensure that the unauthorized actor was removed from the account. Upon confirming that the email account was subject to unauthorized access, we undertook a detailed and thorough review of the account to determine whether any sensitive information was contained within the account. This review concluded on December 14, 2022. Our review determined that some of your information was contained in the email account. We then worked diligently to provide you this notice.

What Information Was Involved? The investigation determined that your name, address, and financial account information may have been accessible. Although we are unaware of any actual or attempted malicious misuse of your information, we are providing you with this notice out of an abundance of caution.

Our Response. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of the event, we moved quickly to investigate and respond to the event, assess the security of our systems, and notify those potentially affected by the event. To mitigate harm and protect against further incidences, a leading cybersecurity forensics firm worked with internal teams to thoroughly investigate and ensure the security of our email environment. Employee user accounts passwords were reset, and multifactor authentication is being implemented.

We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information. We regret any inconvenience or concern this event may cause.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution. Additional information and resources are included in the enclosed *Steps You Can Take to Protect Personal Information*.

We are also providing you with access to credit monitoring and identity protection services through Experian. Information on how to enroll in these complimentary services are included below under *Steps You Can Take to Protect Personal Information*. Please note, we are unable to enroll you in these services on your behalf, so you will need to follow the enrollment instructions below to engage these services.

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 contact James Springer at 651-796-6149, Monday through Friday from 8:00AM CST – 5:00PM CST. You may also write to CH Holdings at 10733 Sunset Office Drive, #200, St. Louis, Missouri 63127. Again, we take the privacy and security of information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

CH Holdings USA, Inc.

Steps You Can Take to Protect Personal Information

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

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

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 **March 31, 2023.** Be prepared to provide engagement number **XXXXXX** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

Once you enroll in Experian IdentityWorks, you can contact Experian regarding any fraud issues and have access to the following features:

- **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 agents 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 and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **1-888-397-3742**. 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 (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 (3) major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for twelve (12) 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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) 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 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 (7) years. Should you wish to place a fraud alert, please contact any one of the 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 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; 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 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 Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, Maryland 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

Warren Community College

Return to IDX
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 16, 2023

Re: Notice of Data <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>,

Warren County Community College ("WCCC") is writing to inform you of a recent data security incident that involved your personal information. At WCCC, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On November 13, 2022, WCCC discovered unusual network activity impacting certain systems. We immediately took steps to secure our environment and engaged cybersecurity experts to assist us with an investigation. The investigation determined that an unknown actor gained access to and obtained data from the WCCC network without authorization sometime between November 2, 2022 and November 13, 2022. Following a thorough review of the impacted information, on February 8, 2023, we determined that some of your personal information was involved in the incident.

What Information Was Involved? The information affected may have included your name and your <<Variable Text 2>>.

What We Are Doing. As soon as WCCC discovered the incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. Furthermore, we reported the incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrator(s) accountable, if possible. We are also notifying you of this event and advising you about steps you can take to help protect your information.

Additionally, we are offering you complimentary credit monitoring and identity protection services for <<Variable Text 3: 12/24>> months through IDX, a national leader in identity protection services. The IDX services, which are free to you upon enrollment, include a one-year subscription for the following: single bureau credit monitoring, CyberScan dark web monitoring, fully-managed identity recovery services, and $1 million in identity theft insurance coverage. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through IDX at no cost to you. To receive credit monitoring 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.

You can enroll in the IDX identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. Please note the deadline to enroll is May 16, 2023.

For More Information: If you have questions or need assistance, please call 1-800-939-4170, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. Eastern Time. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Dr. William J. Austin, Jr.
President
Warren County Community College

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

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 http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay 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. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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 potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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 insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; http://oag.ca.gov/

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; https://www.maine.gov/ag/

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov. The total number of Rhode Island residents receiving notification of this incident is two (2).

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov