FOLEY
FOLEY & LARDNER LLP

ATTORNEYS AT LAW

301 E PINE ST
SUITE 1200
ORLANDO, FL 32801
407.423.7656 TEL
407.648.1743 FAX
FOLEY.COM

CLIENT/MATTER NUMBER
111328-0140

November 22, 2024

VIA E-MAIL: DOJ-CPB@doj.nh.gov

Consumer Protection Bureau
New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification Pursuant to NH Rev. Stat. § 359-C:20

Dear Office of the Attorney General:

We are writing on behalf of our client, Contemporary Information Corp. ("CIC"), to notify you of a breach of security involving the personal information of one (1) New Hampshire resident. For background, CIC is a consumer reporting agency that provided employment screening reports and services to its clients. As part of this process, CIC utilized a third-party vendor, BackChecked, LLC ("BackChecked"), which provided and hosted an online platform for CIC to enable its clients with secure access to employment screening reports in connection with individuals' applications for employment with such entities.

NATURE OF THE INCIDENT

On October 29, 2024, CIC was informed by BackChecked that certain applicant information was impacted by an incident in which an unauthorized third-party accessed BackChecked's systems and viewed and/or acquired a subset of applicant information that was stored in those systems and used in connection with providing employment screening reports to CIC's client, which included an entity to which one (1) New Hampshire applied for employment. BackChecked advised CIC that upon detecting suspicious activity on its systems, BackChecked promptly commenced an investigation through which it was able to identify and immediately stop the unauthorized activity. In addition, BackChecked also advised CIC that it retained outside experts to assist with a forensic investigation and analysis of the incident and put in place additional security measures to protect against further unauthorized access.

According to information provided to CIC by BackChecked to date, BackChecked's investigation confirmed that an unauthorized third-party accessed its systems on September 26, 2024 and viewed and/or acquired certain applicant records stored in those systems during that time. Through their data analysis, BackChecked informed CIC it had determined that some of the applicant records accessed and/or acquired by the unauthorized party contained certain applicant personal information, including the

for one (1) New Hampshire resident.

STEPS TAKEN IN RESPONSE TO THE INCIDENT

CIC mailed a notification letter to the potentially affected New Hampshire resident on November 22, 2024, pursuant to NH Rev. Stat. § 359-C:20. Enclosed is a sample copy of the notice letter that was sent to this individual.

In addition, CIC has provided the potentially affected New Hampshire resident with complimentary access to a comprehensive identity monitoring service through Kroll (which includes credit monitoring, fraud consultation, and identity theft restoration), at no charge, for a period of , and also has set up a dedicated support line that will be staffed to answer any questions individuals may have about this incident or the service available to them.

Further, CIC no longer provides employment screening reports as part of its business and, in response to this incident, has terminated its agreement with BackChecked.

If you have any further inquiries concerning this notification, please do not hesitate to contact me.

Sincerely,

Christi A. Lawson
Foley & Lardner LLP

Encl: Sample Notification Letter

CIC
The Power of Decision™

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<last_name>>:

Contemporary Information Corp. ("CIC") values and respects the privacy of your information, which is why we are writing to inform you of a recent security incident that impacted one of our third-party vendors and affected some of your personal information. We want to provide you with information about the incident, the measures taken in response, and to share some steps that you can take to help protect yourself. Please note that this incident involving our third-party vendor had no impact on CIC's systems.

For background, CIC is a consumer reporting agency that provided employment screening reports and services to its clients. As part of this process, CIC utilized a third-party vendor, BackChecked, LLC, which provided and hosted an online platform for CIC to enable its clients with secure access to employment screening reports. You are receiving this letter because you applied for employment with an entity that was a client of CIC and utilized BackChecked's platform to view your employment screening report in connection with your employment application.

WHAT HAPPENED?

On October 29, 2024, we were notified by BackChecked that certain applicant information was impacted by an incident in which an unauthorized third-party accessed BackChecked's systems and viewed and/or acquired a subset of applicant information that was stored in those systems and used in connection with providing employment screening reports to CIC's client, which included an entity to which you applied for employment. BackChecked advised CIC that upon detecting suspicious activity on its systems, BackChecked promptly commenced an investigation through which it was able to identify and immediately stop the unauthorized activity. In addition, BackChecked advised CIC that it retained outside experts to assist with a forensic investigation and analysis of the incident and put in place additional security measures to protect against further unauthorized access.

We understand that BackChecked's investigation confirmed that an unauthorized third-party accessed its systems on September 26, 2024 and viewed and/or acquired certain applicant records stored in those systems during that time. Through their data analysis, BackChecked determined that some of the applicant records accessed and/or acquired by the unauthorized party contained some of your personal information.

WHAT INFORMATION WAS INVOLVED?

According to BackChecked's review of the contents of the records impacted, one or more of the records contained your .

WHAT WE ARE DOING.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring, at no cost to you, for <<Monitoring Term Length (Months)>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Instructions on how to activate these services are below.

Visit https://enroll.krollmonitoring.com/ to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

WHAT YOU CAN DO.

Please also review the enclosed "Other Important Information" document included with this letter for further steps you can take to help protect your information, including recommendations by the U.S. Federal Trade Commission ("FTC") regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. It is also recommended that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your credit reports for unauthorized activity. If you discover any suspicious or unusual activity on your accounts, you should promptly notify the financial institution or company with which your account is maintained.

FOR MORE INFORMATION.

For further information and assistance, please call , Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Becky Bower
Director of Risk Management
Contemporary Information Corp.

OTHER IMPORTANT INFORMATION

Additional Information Regarding Your Complimentary Identity Monitoring Services.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—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 will be able to help you determine if it is an indicator of identity theft.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months, from each of the nationwide credit reporting agencies listed below. In addition, Equifax, Experian, and TransUnion have also agreed to provide weekly online credit reports. To order your free credit report, please visit www.annualcreditreport.com or call toll free at 877-322-8228. You can also order your free credit report by mailing a completed Annual Credit Report Request Form (available from the FTC's website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the national credit reporting agencies for the purpose of requesting a copy of your credit report and other general inquiries is provided below:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 800-888-4213
- **Innovis**, PO Box 1689, Pittsburgh, PA 15230-1689, www.innovis.com, 800-540-2505

Fraud Alert. You have the right to place an initial or extended "fraud alert" on your file at no cost by contacting any of the nationwide credit reporting agencies listed below. Contact information for the national credit reporting agencies for the purposes of placing a fraud alert on your file is provided below. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For this reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

- **Equifax**, PO Box 105069, Atlanta, GA 30348-5069, www.equifax.com/personal/credit-report-services/credit-fraud-alerts, 800-525-6285
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html, 888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts, 800-680-7289
- **Innovis Consumer Assistance**, PO Box 26, Pittsburgh, PA 15230-0026, https://www.innovis.com/personal/fraudActiveDutyAlerts, 800-540-2505

Security Freeze. You have the right to place, lift, or remove a "security freeze" on your credit report, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze separately with each of the consumer reporting agencies. To place a security freeze on your credit report, you may do so by contacting each of the consumer reporting agencies through the contact information below:

- **Equifax**, PO Box 105788, Atlanta, GA 30348-5788, www.equifax.com/personal/credit-report-services/credit-freeze, 800-298-0045
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html, 888-397-3742
- **TransUnion**, PO Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze, 888-909-8872
- **Innovis**, PO Box 26, Pittsburgh, PA 15230-0026, www.innovis.com/personal/securityFreeze, 800-540-2505

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. 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.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and may provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security

freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the FTC, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 877-ID-THEFT (438-4338). This notice has not been delayed by law enforcement.

- ***California residents***: You may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.
- ***Maryland residents***: You may obtain information about avoiding identity theft from the Maryland Office of the Attorney General at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.
- ***New Mexico residents***: Consumers have rights pursuant to the Fair Credit Reporting Act ("FCRA"), such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage consumers to review their rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
- ***New York residents***: You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General by calling 1-800-771-7755 or visiting https://ag.ny.gov; the New York State Police by calling 1-518-457-6721 or visiting https://troopers.ny.gov/; and/or the New York Department of State by calling 1-800-697-1220 or visiting https://www.dos.ny.gov.
- ***North Carolina residents***: You may obtain additional information about preventing identity theft provided by the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.
- ***Oregon residents***: You are advised to report any suspected incidents of identity theft to law enforcement, the FTC, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.