<<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>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you that Scoular recently experienced a security event where confidential information was accessed by an external unauthorized party. Although we are unaware of any actual misuse of this information, we are providing notice to you about the incident. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on how you can obtain, at no cost to you, identity monitoring and restoration services.

What happened?

On January 20, 2022, Scoular was alerted to activity indicating unauthorized access by a third party to information on our internal network. Upon detection, we took immediate steps to shut down further access to the impacted systems. We were able to contain the unauthorized access after following our internal processes. We reported the event to law enforcement and worked with external cybersecurity experts to investigate the event and determine what happened, what data was impacted, and to whom the data belonged. Through the investigation, we learned that the unauthorized third party was able to acquire a set of files with confidential data from our internal network.

What information was involved?

Scoular began a thorough process to determine if the files contained personal information, and if so, who was affected and the types of information that were affected. This analysis was time consuming. We completed this process on August 1, 2022 and determined that your personal information was accessed and/or acquired. The potential types of information accessed could include name, date of birth, Social Security number, driver's license number, passport number, other government ID number, credit card number, financial account number, medical information, and health insurance information.

What we are doing:

1. **We are supporting those potentially impacted.** This type of security event is, unfortunately, more common than not. Rest assured, Scoular is committed to safeguarding confidential and sensitive information, and is offering two years of identity monitoring and restoration services at no cost to you, through our preferred third-party vendor Kroll, where those services are available.

   Please see Attachment A for details regarding these complimentary identity monitoring and identity theft restoration services, as well as how to activate with your unique activation code.

   You must enroll by <<b2b_text_6 (date)>> to receive these services.

2. **We are taking additional proactive measures in our systems and processes.** In addition to the above actions, Scoular has taken steps to deploy additional safeguards onto our systems, including reinforcing our security practices. We continue to actively review our systems to enhance security monitoring and controls. And, as part of our ongoing security operations, we regularly review our security and privacy policies and procedures and implement changes when needed to enhance our information security and privacy programs and controls.

What you can do:

In addition to enrolling in the identity monitoring and restoration services being offered to you at no charge, we encourage you to take the following precautions:

- It is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to protect your identity is contained in Attachment B.

For more information:

Scoular has established a dedicated call center to answer questions about the cybersecurity event as well as the Kroll services that we are offering to you. If you have any questions, please call the call center at (855) 544-2868 Monday through Friday from 7:00 a.m. to 7:00 p.m. ET.

Sincerely,

David Tomlinson
Chief Information Officer

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

You have until <<b2b_text_6 Date)>> 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.

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

Triple Bureau Identity 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 will 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.

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 will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will 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 securities 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.

Attachment B – Information for U.S. Customers

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. customers are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call tollfree (877) 3228228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might help protect against someone else obtaining credit in your name.

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. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	**Experian**	**TransUnion**
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 190222000
(888) 7660008	(888) 3973742	(800) 6807289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a governmentissued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 3824357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

California Residents: Visit the California Department of Justice's Privacy Unit (https://oag.ca.gov/privacy) for additional information on security against identity theft.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the cybersecurity event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, +1 (800)-771-7755; or www.ag.ny.gov.