EXHIBIT 1

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Korchmar, The Leather Specialty Co. ("Korchmar") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On April 3, 2023, Korchmar became aware of suspicious activity within its computer environment. Upon becoming aware of the activity, Korchmar launched an investigation, with the assistance of cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that on or about April 2, 2023, an unauthorized actor gained access to certain Korchmar systems through an account belonging to its third-party managed services provider ("MSP") and may have viewed or taken certain information contained therein.

The investigation was not able to determine what, if any, information was actually viewed or taken. Therefore, in an abundance of caution, Korchmar conducted a comprehensive, programmatic and manual review to identify what information was potentially accessible during the event and to whom such information relates. Once complete, Korchmar also worked to validate the results and locate appropriate contact information for potentially affected individuals. Korchmar completed this process on October 3, 2023, and then moved as quickly as possible to provide notice. The personal information potentially impacted by this event includes the following: name, address, and Social Security number.

Notice to Maine Resident

On November 6, 2023, Korchmar provided written notice of this event to potentially impacted individuals, including approximately one (1) Maine 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 becoming aware of the event, Korchmar moved quickly to investigate and respond to the event, assess the security of Korchmar's network and systems, and notify potentially affected individuals. Further, Korchmar notified federal law enforcement. Korchmar is also working to implement additional safeguards and training to its employees.

Korchmar is providing access to credit monitoring services for twelve (12) months, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Additionally, Korchmar is providing 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. Korchmar is providing individuals with information on how to place a fraud alert and credit 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.

Korchmar also is providing written notice of this incident to relevant state regulators, as required.

EXHIBIT A

KORCHMAR

SINCE 1917

<<Return Mail Address>>

<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

<<EXTRA 1 (VARIABLE HEADER FIELD)>>

Dear << Name 1>>:

Korchmar, The Leather Specialty Co. ("Korchmar") is writing to inform you of an event that may impact the security of some of your information. Although we have received no indication of any actual or attempted identity theft or fraud as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On April 3, 2023, Korchmar became aware of suspicious activity within its computer environment. Upon becoming aware of the activity, we launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that on or about April 2, 2023, an unauthorized actor gained access to certain Korchmar systems through an account belonging to our third-party managed services provider ("MSP") and may have viewed or taken certain information contained therein.

The investigation was not able to determine what, if any, information was actually viewed or taken. Therefore, in an abundance of caution, we conducted a comprehensive, programmatic and manual review to identify what information was potentially accessible during the event and to whom such information relates. Once complete, we also worked to validate the results and locate appropriate contact information for potentially affected individuals. We completed this process on October 3, 2023, and then moved as quickly as possible to provide notice.

What Information Was Involved? The investigation determined that your name, address, and Social Security number were potentially accessible during the event.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon becoming aware of the event, we moved quickly to investigate and respond to the event, assess the security of our network and computer systems, and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, we are offering credit monitoring and identity restoration services through Equifax for <<Extra 2 (Credit Monitoring Duration)>> months, at no cost to you.

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*. You may also enroll in the complimentary credit monitoring and identity restoration services available to you. Enrollment instructions are attached to this letter.

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 the dedicated assistance line at 888-562-8347, Monday through Friday from 9:00am – 9:00pm Monday through Friday, excluding major U.S. holidays. Please have this letter ready if you call. Again, we take the confidentiality, privacy, and security of information in our care very seriously and sincerely regret any inconvenience or concern this event may cause.

Sincerely,

Don Michael Korchmar
President
Korchmar, The Leather Specialty Co.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

<< Name 1>>
Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report.
- Daily access to your Equifax credit report.
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card, or bank account numbers, are found on fraudulent Internet trading sites.
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock.[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf.
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft.[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of <<Activation Code>>, then click "Submit" and follow these 4 steps:

1. Register:
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. Create Account:
   Enter your email address, create a password, and accept the terms of use.
3. Verify Identity:
   To enroll in your product, we will ask you to complete our identity verification process.
4. Checkout:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

---

[1] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[2] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3] [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

[4] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

You're done!

The confirmation page shows your completed enrollment.

Click "View My Product" to access the product features.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to

file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

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.