Merchants Bank

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

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

<<b2b_text_1(NOTICE OF [SUBJECT HEADER])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Merchants Bank is writing to inform you of a recent event that may involve some of your information. While we are unaware of any actual or attempted misuse of your information, we are providing you with information about the event, our response to it, and steps you may take to help protect your information, should you feel it necessary to do so.

What Happened? On March 27, 2023, Merchants Bank became aware of suspicious activity concerning an employee's email account. Upon becoming aware of the activity, Merchants Bank immediately launched an investigation into the nature and scope of the event with the assistance of third party forensic specialists. Our investigation determined that an unauthorized actor gained access to a Merchants Bank email account between March 21, 2023 and March 27, 2023. While we have no indication that files containing your information were viewed or accessed by the unauthorized third party, we are unable to rule out the possibility that some information within the account may have been impacted during the period of unauthorized access. Therefore, in an abundance of caution, Merchants Bank undertook a comprehensive and time-intensive review of all potentially impacted files with the assistance of third-party data review specialists to determine if they contained sensitive information. On April 28, 2023 we determined that your information was present within the impacted email account.

What Information Was Involved? Our investigation determined that your name and <<b2b_text_1(data elements)>> were contained within the impacted email account.

What We Are Doing. We take this event and the security of personal information in our care very seriously. Upon learning of the activity, Merchants Bank immediately took steps to ensure the security of our systems and investigate the event. As part of our ongoing commitment to the privacy of information in our care, we are implementing additional technical security measures to strengthen the security of our systems. We are also reviewing and enhancing our existing data privacy policies and procedures. We are notifying regulators, as necessary.

Although we are unaware of fraudulent misuse of your information as a result of this event, as an added precaution we are offering you access to twenty four (24) months of identity monitoring services through Kroll at no cost to you for (24) months. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Personal Information*. We encourage you to activate these services as we are unable to act on your behalf to do so.

What You Can Do. We encourage you to remain vigilant over the next 12 to 24 months against incidents of identity theft and fraud by reviewing your account statements, monitoring your free credit reports for suspicious activity, and reporting any suspected identity theft your financial institution. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to better safeguard against possible misuse of your information.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions or concerns, please call our dedicated assistance line at TFN. This line is available Monday – Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding major U.S. holidays). You may also write to Merchants Bank at 210 S. Main Ave., P.O. Box 199, Rugby, ND 58368.

Sincerely,

Merchants Bank

Steps You Can Take To HELP Protect Personal Information

Enroll in Monitoring Services

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.

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 help 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.

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 help 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.