The City of Sun Prairie
300 E Main Street
Sun Prairie, WI 53590

30681

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notification of Data Privacy Incident

Dear <<Name 1>>,

The City of Sun Prairie, Wisconsin ("**Sun Prairie**" or "**we**") understands the importance of cybersecurity and protecting your personal data. Unfortunately, the purpose of this letter is to inform you that there has been a compromise to the confidentiality of your sensitive personal data that we retained in connection with your application for a municipal license. Although there is no evidence that your sensitive personal data has been misused, out of an abundance of caution, Sun Prairie is providing you complimentary credit monitoring and identity theft protection services and we encourage you to enroll in these services.

Background: What happened?

As you know, in order to apply for a license to operate certain types of businesses or perform certain types of professional services in Sun Prairie (e.g., liquor sales, pawn shops), an applicant needs to submit a professional license application for review and approval by us. This application contains sensitive personal data about the applicant that we use for identity verification and other legal compliance purposes. When Sun Prairie approves such a license, it publishes, for transparency purposes, details about the license applicant and their business or processional service on opengov.com (the "**OpenGov Platform**").

On August 29, 2023, we were informed that the OpenGov Platform that is hosted on the City of Sun Prairie website was displaying full and complete applications for certain municipal licenses - instead of only summaries of the applications and our approval. These applications contained sensitive personal data on the applicant. However, it does *not* appear that this information could be found through a typical "search engine" query (e.g., a Google search); but rather, to be able to view this applicant information, an individual would have to access Sun Prairie's city website, then launch the OpenGov Platform, and then search for a license holder by license number or license holder address. This process would have allowed them to view all materials related to the license application, including the applicant's sensitive personal data.

What Personal Data/Information Was Involved?

The sensitive personal data in a license application that was accessible through OpenGov Platform consisted of the following: your first and last name, date of birth, driver's license number and any stored images of the driver license. There was no other sensitive personal data compromised in this incident. We do not collect or store your social security number, passport number, or other similar government identifiers, any financial information that would give someone access to your financial accounts, or any biometric or health-related data, and therefore such data sets were not impacted by this incident.

What are we doing?

Please know that Sun Prairie acted swiftly to address this privacy incident. Specifically, after being notified about this issue, we immediately made technical configuration changes to the OpenGov Platform and terminated all search functions within the OpenGov Platform. Further, we are reviewing our municipal license application and approval practices to determine whether we need to implement additional internal controls and safeguards. We are also implementing certain types of privacy and security training so that Sun Prairie personnel are better positioned to address information security and privacy threats and issues.

Credit Monitoring Services

Although there is no evidence that your sensitive personal data has been misused, out of an abundance of caution, Sun Prairie is providing you **complimentary credit monitoring and identity theft protection services for 12 months offered through Equifax**.

The enclosed sheet provides instructions for enrollment in these **Equifax Complete™ Premier services**.

What You Can Do

Although there is no evidence that your sensitive personal data has been misused, there are several steps that you can take to better protect yourself and your sensitive personal data more generally. We recommend you remain vigilant and regularly review your credit card bills, bank statements, and credit reports for any unauthorized activity. Promptly report incidents of suspected identity theft or fraud to your local law enforcement agency, the Federal Trade Commission, your state Attorney General, your financial institution, and to one of the three nationwide consumer reporting agencies to have such incidents removed from your credit file. You should change your passwords regularly, and refrain from using easily guessed passwords and re-using the same passwords for multiple accounts. Be vigilant against third parties attempting to gather information by deception, and exercise extreme caution when clicking on unknown or suspicious website links. See the attachment for additional information with respect to certain security services that may be available to you.

* * * * * * * * * *

We deeply regret that this privacy incident occurred. However, from the start, we moved quickly to contain the incident and conducted a thorough investigation. We are working hard to ensure that individuals impacted by this incident have answers to questions about their personal data. If you have any questions, please contact us at the following: licensing@cityofsunprairie.com.

Sincerely,

Elena Hilby
City Clerk

Additional Information: Data Security

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111.
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742.
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800.

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 Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. 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 Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

If you are a resident of Massachusetts, you (i) have the right to file and obtain a copy of a police report, (ii) you are allowed to place, without charge, a security freeze on your credit reports, and (iii) you may contact and obtain information from and/or report identity theft to your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

Note: The delivery of this notice has not been delayed as a result of a law enforcement investigation.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a personal identification number ("PIN") that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com.
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com.
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com.

To request a security freeze, you will need to provide the following information: (i) Your full name (including middle initial as well as Jr., Sr., II, III, etc.), (ii) Social Security number, (iii) Date of birth, (iv) If you have moved in the past five years, provide the addresses where you have lived over the prior five years, (v) Proof of current address such as a current utility bill or telephone bill, (vi) A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.), (vii) If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three 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 five business days and 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.

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 one business day after receiving your request by toll-free telephone or secure electronic means, or three 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 three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act (the "FCRA"), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC published a list of the primary rights created by the FCRA, which is available at (https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes the following:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months. You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days, if you are on welfare, or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score. You have the right to dispute incomplete or inaccurate information. Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers. You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity-theft victims and active-duty military personnel have additional rights.

* * * * * * * * * *

<<NAME 1>>
Enter your Activation Code: *<<ACTIVATION CODE>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

Equifax Complete™ Premier

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

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] 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[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- 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[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

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.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.