From: **Rob Vine** rvine@mtpleasanttx.gov
Subject: RE: URGENT CONFIDENTIAL NOTICE – City of Mount Pleasant Financial Transparency Portal – Apparent Public SSN Exposure / Preservation Request
Date: April 28, 2026 at 8:29 PM
To: Kyle Moring [redacted], Candias Webster cwebster@mtpleasanttx.gov, Lea Ream lream@dtrglaw.com, Austin Beck abeck@dtrglaw.com

RV

Mr. Moring,

Thank you for brining this to our attention. We will investigate and work with our partners to ensure private information remains safe.

Robert G. Vine, CPM
City Manager

City of Mount Pleasant
501 N. Madison
Mount Pleasant, TX 75455

From: Kyle Moring <[redacted]>
Sent: Tuesday, April 28, 2026 7:44 PM
To: Rob Vine <rvine@mtpleasanttx.gov>; Candias Webster <cwebster@mtpleasanttx.gov>; Lea Ream <lream@dtrglaw.com>; Austin Beck <abeck@dtrglaw.com>
Subject: URGENT CONFIDENTIAL NOTICE – City of Mount Pleasant Financial Transparency Portal – Apparent Public SSN Exposure / Preservation Request

Mr. Vine, Ms. Webster, Ms. Ream, and Mr. Beck:

I am providing written notice of an apparent public exposure of Social Security numbers in the City of Mount Pleasant's OpenGov-hosted financial transparency portal.

Please treat this as a confidential security/privacy notice and preservation request. This is not a Texas Public Information Act request. Because the issue involves apparent Social Security numbers and other sensitive identifying information, I respectfully request that this notice, the attachment, and related evidence be handled as sensitive and limited to City personnel, counsel, records-management personnel, and technical personnel with a need to know. To the extent any related material is later reviewed under the Public Information Act or otherwise considered for release, I request that it first be reviewed for applicable confidentiality, privacy, security, and redaction requirements.

Public portal URL:

[redacted]

Summary of finding

Using ordinary public access only – no authentication, circumvention, exploitation, or nonpublic endpoint access

– I reviewed the City's publicly available Accounts Payable transparency dataset export.

The export contains 456,623 records and 102 columns. A pattern-based review identified 21 distinct apparent SSN-format values that pass standard validity-exclusion checks, appearing in 692 findings across 645 unique source dataset rows. Forty-seven source rows contain two distinct apparent SSN findings.

The apparent SSNs appear in Vendor Address 1, Vendor Address 2, Vendor City, Vendor Attn, Invoice Number, and Invoice Special Info fields. For records with populated check dates, the affected records range from March 7, 1995 through August 27, 2009; one finding row does not have a populated check date.

The records remained publicly accessible as of approximately 12:45 PM CST today.

I have not included any full Social Security number in the body of this email. I also do not represent that I have independently confirmed assignment of each apparent SSN to a specific individual, or that every affected individual is living. However, the values identified pass standard SSN validity-exclusion checks and appear in contexts indicating that they should be treated as sensitive personal information pending the City's review.

Employee-related records

The findings also appear to include identifiable City employee, former employee, or employee-related payment records. Without including any SSNs in this email, examples of named individuals appearing in affected records include [redacted] and [redacted]

I am identifying those names only to assist the City in prioritizing internal HR, payroll, records-management, legal, and notification review. The encrypted findings file contains the row-level references.

Immediate concern

The apparent exposure involves computerized records published through a public-facing City transparency portal. The City should immediately evaluate whether the exposure triggers any containment, preservation, remediation, individual notification, Attorney General notification, or other obligations under applicable Texas law, including Tex. Local Gov't Code §205.010 and Tex. Bus. & Com. Code §521.053.

The issue may also be relevant to public-information compliance. Tex. Gov't Code §552.147 specifically excepts Social Security numbers of living persons from required public disclosure, and the City should determine the status of affected individuals as part of its review. In any event, the apparent SSNs should be treated as sensitive pending legal review because they appear in identifiable payment records and may implicate other confidentiality, breach notification, fraud prevention, records-management, or remediation obligations.

Requested immediate action

I respectfully request that the City:

1. Immediately contain the exposure by taking the affected report offline, disabling public export/access, filtering the affected records, or otherwise preventing continued public access to the affected records while the City investigates;
2. Preserve, before or concurrently with remediation, the current public-facing report, underlying source records, OpenGov configuration, publication/ingestion history, audit logs, access/export logs, administrative action logs, and any remediation records;
3. Coordinate with OpenGov to determine how the affected records were published, whether the exposure remains active, and whether any third-party downloads, exports, or access events are reflected in available logs;
4. Review the affected records to determine the identity, residency status, and living/deceased status of

affected individuals, including whether any affected individuals are current or former City employees, and determine whether notice is required under applicable law;

5. Review the remainder of the City's transparency-publication set for similar personally identifiable information or sensitive personal information; and

6. Designate a City point of contact for secure evidence transmission and remediation coordination.

Evidence

Attached is an encrypted confidential findings file containing the unredacted apparent SSN occurrences and related record-identification information, including row number, source column, vendor name, invoice number, check date where populated, and the apparent SSN occurrence.

Because the attachment contains apparent Social Security numbers and other sensitive identifying information, I have not included the password in this email. Please designate a secure channel or specific administrative/legal recipient for password transmission. I can provide the password by phone or through another secure method the City identifies.

OpenGov notice

I am also notifying OpenGov separately as the apparent platform host/operator for the public portal so that OpenGov can assist with containment, preserve relevant platform records and logs, and coordinate with the City regarding remediation.

Please confirm receipt of this notice and identify the appropriate City contact for secure follow-up.

Respectfully,

Kyle Moring

[redacted] | [redacted]