MORNING STAR PSA OF THE WEEK
Tax Identity Theft Awareness Week[1]

This week is designated as Tax Identity Theft Awareness Week, and we would like to take this opportunity to remind you of the increased threats of identity theft during this time of year. Tax season is a busy time for fraudsters, as documents containing personal information like W-2s and 1099s are being mailed or posted online. If compromised, this information can be a source for identity theft and the creation of synthetic identities; tactics often used by fraudsters to file false returns and fraudulently apply for credit.

Fraudsters gain access to valuable personal and payroll information by impersonating the IRS or other tax entities via phishing, malware and various forms of business email compromise. For instance, recently fraudsters claiming to represent the IRS have contacted potential victims asking for personal information, threatening that the victim's Social Security number could be suspended or canceled if they did not comply. It is important to understand that the IRS does not contact taxpayers by email, text message or social media channels to request personal or financial information, including passwords and PIN numbers. Any such attempt should serve as an alarm.

Provided below are some considerations for your protection during tax season:

- If you receive an email claiming to be from the IRS requesting W-2s or other tax related information:
  - Don't reply.
  - Don't open any attachments or links, as they may contain malicious malware code that can infect your computer or mobile phone.
  - Forward the full email to the IRS at phishing@irs.gov.
  - Delete the original email.
- If you are a victim of a W-2 scam (you received an email and responded with the requested W-2 information):
  - Email the IRS at dataloss@irs.gov and send the full email to phishing@irs.gov.
  - Email the Federation of Tax Administrators at statealert@taxadmin.org to learn how to file a report.
  - Notify employees of the compromise so they may take steps to protect themselves from identity theft.
- If possible, do not act on any email requesting sensitive information such as account numbers, changes to payment terms, or other tax-related information. Validate the request by contacting the presumed sender using their established contact information – not the contact information included in the email.
- Establish internal controls for distributing tax-related documents or information.
- In the event of a data breach, you may be required by state law to notify the state and all affected parties. You should have a data breach response plan in place, as some state laws have a very short notification deadline requirement.

[1] Although we are not in the endorsement business I want to acknowledge that this letter was modified from a letter originally sent out to businesses by Regions Bank.