Good afternoon,

I am writing to advise you of upcoming changes that impact your transaction processing. As a user of Tender Retail Point-of-Sale payment solutions, you will need to make changes to the TD Merchant Solutions (TDMS) host destination IP addresses and ports, to continue processing transactions. You may also need to make changes to your Tender Retail middleware. Please review the summary of changes below and the action required for each change.
Note: The following information is technical in nature. Should you require support please contact your internal support team, POS software provider and/or Tender Retail (if applicable).

Part I: Change from VeriSign to DigiCert Certificate

To enable secure and encrypted transaction processing, a digital certificate is included with your software. The current certificate (Verisign) will be expiring in September 2020. As a result, TDMS is adding additional gateways with new destination IP addresses and ports to support the new certificates (DigiCert). To support this change, TDMS requires that you are processing transactions on the latest version of POS software/middleware application that supports the new certificates. You will also need to ensure that your network infrastructure will be allowed to process traffic to the new destination IPs and ports.

1) Ensure all your registers/terminals at every location (including Franchises if applicable) are operating on the minimum required version of Tender Retail payment middleware application (4.2.17 build 519 or higher) which includes the new certificates.

2) Allow your business enough time to complete the software deployment based on the number of registers/terminals and/or locations.

3) Change the TDMS host destination IP addresses and ports according to the table below. If your firewall is configured to restrict IP addresses and/or Port access, you will also be required to add these **new** IP addresses and Ports to your firewall rules.

4) Once the required changes have been made and deployed, please send a confirmation email to TD.TDMSSupport@td.com with the information below. **This confirmation email should be sent by March 31, 2020.**
   a) Merchant name
   b) Provide a copy of the latest "{terminal ID}_{date}.dg" log file

New TDMS Host Destination IP Addresses and Ports:

Description	IP Address 1	IP Address 2	TCP Port(s)
Financial Transaction Processing Host	162.223.156.206	162.223.157.206	32620
Parameter Downloads (TMS Host URL)	162.223.156.202	N/A	34971

Part II: Changes to Manual Card Entry Functionality

Manually keying credit card information into a point-of-sale (POS) device when the cardholder is present significantly increases your risk of completing fraudulent transactions and losses incurred from Chargebacks. To help protect your business, TDMS is advising Merchants to remove the option to manually enter credit card information for transactions where both the card and cardholder are present at the time of a sale (known as a ""Card Present" transaction). This also includes removing Force Post functionality, which is a change being mandated by the Payment Card Networks.

Why is TDMS making this change and how will Merchants benefit?
Recently there has been a significant increase in fraudulent transactions where credit card information is manually keyed into the POS device during Card Present (face-to-face) transactions. With the advancements in chip technology there is no legitimate reason for a Merchant to manually key a credit card number when the cardholder is present. Additionally, as outlined in your TDMS agreement , Merchants are responsible for all Chargebacks (and associated fees) resulting from manually keyed or unauthorized transactions. Removing the functionality for manually keyed transactions when the cardholder is present will help protect your business and decrease your risk of processing fraudulent card-present transactions.

While TDMS is making these changes to help protect our Merchants, you are also required to take all reasonable steps to ensure that the card, cardholder, and transaction are legitimate.

How should payments be processed when the cardholder is not present?
If TDMS has approved and your POS software solution supports transactions to be processed over the telephone or to accept credit card payment information through the mail (known as "Card Not Present" transactions), the correct transaction type needs to be initiated (e.g. select Mail Order/Telephone Order on the POS screen).

If your business requires you to process Card Not Present transactions and you have not yet been approved, please contact me directly. Changes to your POS software solution may also be required to support Mail Order/Telephone Order transactions.

Please ensure you are processing transactions correctly based on the type of transaction being completed (Card Present vs. Card Not Present). If changes are required to your POS software (e.g. remove the "Manual Purchase" option, add "Telephone Order", etc.), please contact your POS Software Provider.
Thank you for choosing TD Merchant Solutions for your payment processing needs. If you have any questions regarding the above changes, please contact me directly or the TD Merchant Solutions Integration Support Team at TD.TDMSSupport@td.com.

Regards,
Allison Lau | Account Manager |TD Merchant Solutions
T: 604.654.3155 | F: 604.654.3133 | E: allison.lau@td.com