Mitigating Fraud

Fraud is a significant risk to any merchant's business. We recommend following consumer best practices to protect yourself and your business from financial and scam-related fraud.

- Ensure you are contacting your financial services providers through official channels. We will never contact you to ask you for your account details.
- Check shipping details on accounts. Be aware of details in the 2nd or 3rd lines of the shipping addresses that might be used to reroute packages.
- Review bills and bank statements to identify anomalies that could indicate fraud, identity theft, or if someone else has access to your account.
- Look for the "s" – When paying vendors online, check the URL to ensure it begins with "https://". The "s" at the end indicates a secure connection. Additionally, check that the name of the web page does not contain spelling errors or strange characters.
- Use caution when posting on social media. Sharing sensitive personal information can provide criminals with clues to answer your security questions or craft believable, targeted scam messages.

In-Person Fraud

POS Skimming: In these skimming attacks, threat actors place a removable device, known as a "skimmer", on an in-person (POS) terminal to harvest the magstripe track data from payment accounts that are used at the targeted terminals. The threat actors will extract the compromised PANs from these skimmers and conduct fraudulent transactions at various retailers or cash out to their own accounts. Actors increasingly utilize "deep insert shimmers" to perpetrate POS skimming. Deep insert shimmers are thin devices placed inside the POS card reader and are much more difficult to detect than skimming overlay devices, which are placed on top of the card reader.

Threat actors can use the cover of a crowded checkout area to place a skimming device on a POS machine out of line-of-site of employees. Additionally, threat actors often hide their installation of a skimming device behind an armful of large items or blocked by an associate creating a disturbance or carrying a large number of items. (Source: Visa Security Alert 2023)

To protect your store from fraudsters, use security best practices, including:

- If you suspect a scam, stop and talk to someone you trust about the situation before acting on the suspected scammer's request.
- Never accept an expired payment card.
- Be aware of customer behavior that could indicate fraud attempts but does not necessarily indicate criminal activity, such as:
    - Trying to distract you or rush you during checkout.
    - Using clothing or bags to block your view of the POS terminal during checkout.