BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 22-073 **July 2022, Issue #82**

BusinesSafe Threat Topic: Point of Sale Fraud

According to a report by the Federal Trade Commission, in 2021 Florida consumers reported approximately 162,988 fraud reports and lost nearly $347 million to fraudulent incidents. As businesses move towards cashless payments during point-of-sale (POS) transactions, criminal actors may try to use fraudulent activity such as stolen credit card information from cyberattacks or other criminal activity to target unsuspecting consumers and businesses. While not all encompassing, this article will provide an overview of some common fraud tactics involving POS transactions, indicators of such tactics and prevention, and ways to report incidents.

Common Methods of Attack:

- **True Fraud** – True fraud involves a criminal actor using stolen credit card information to make a purchase either in-person or online. An updated version of this fraud involves the criminal actor opening a new credit card account using the cardholder's stolen identity acquired either through the initial theft, prior data breaches, or identity theft.
- **Chargeback Fraud** – This fraud is also known as "friendly fraud" or "first party fraud." The fraud begins with a customer using a credit card to make a legitimate purchase for a good or service. The customer will contact the bank or credit card company to deny having made a purchase. The customer performing this act of fraud is intentionally and maliciously denying the card payment. If the retailor is unable to furnish proof of a legitimate payment, the retailer may have to cover the chargeback amount and fee.
- **Card Testing Fraud** – Online retailers can experience card testing fraud when criminal actors make numerous small payments or purchases in order to verify whether a stolen credit card number is valid. In some cases, bots have been used by cybercriminals extensively to test multiple card numbers simultaneously. Due to the purchases being made in such small amounts, it often goes undetected. Once a card number is validated, the criminal actor may conduct larger transactions from the retailer.

POS Fraud Indicators:

- A customer attempts to purchase a small number of items multiple times using the same name and email address, but uses different credit cards.
- A store receives a call from an alleged customer to either place an order or verify a previous order, yet the caller can't verify or confirm any of the previously provided billing information apart from the credit card number.
- A customer is exhibiting unusual behavior while paying for items.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8651, HSEC:1 FSIN:1.5.1, 1.10, 3.1, 3.1.1, 3.1.2, 3.2.1 FFC:1.2, 4.1, 4.2, 4.4

- The credit card that is being offered as payment has varying fonts, the numbers do not line up, there is no magnetic stripe or chip, and an odd signature section.

Tips to Protect Your Business and Consumer:

- Retailers should require an identification card or driver's license to verify identity.
- Retailers may require customers to provide PINs or CVV codes on all transactions to ensure identity.
- Retailers should ensure all chip readers are up-to-date with technological upgrades.
- If a customer is purchasing online, verify address and billing information with information on file. If a customer uses guest access, have a security measures in place to ensure validity of the purchase.
- Retailers should verify the machines used have the Point to Point Encryption (P2PE) to keep customers data safe from cyber criminals
- Retailers should implement procedures to help identify known POS fraudulent activity.
- Train employees to identify potentially fraudulent purchases including how to detect fraudulent credit card usage.
- Retailers should check POS equipment before and after each shift to ensure the machine has not been tampered with or damaged.

Ways Victims Can Report:

- Individuals and businesses can report POS fraud to their local police department.
- For victims of online scams, you can contact the Florida Attorney General's Office of Citizen Services either by calling the Attorney General's Fraud Hotline at 1-866-966-7226 or by filing out an online complaint form at My Florida Legal.
- The Federal Trade Commission gives citizens the resources and ability to report various scams on their website.
- Report consumer complaints and tampering at gas pump POS machines through the Florida Department of Agriculture and Consumer Services online Consumer Complaint Form or by calling 1-800-HELP-FLA (435-7352) or 1-800-FL-AYUDA (352-9832) en Español.

Resources:

- The Federal Trade Commission offers multiple resources and guides to help protect small businesses against cyberattacks and scams.
- The Florida Department of Agriculture and Consumer Services offers more information for individuals and businesses on a variety of scams and fraud.
- The Florida Division of Consumer Services offers information on frauds and scams.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8651, HSEC:1 FSIN:1.5.1, 1.10, 3.1, 3.1.1, 3.1.2, 3.2.1 FFC:1.2, 4.1, 4.2, 4.4