ROCKLAND POST - UNBIASED AND ACCURATE NEWS AND INFORMATION

Haverstraw Police Inspect Local Businesses for Credit Card Skimmers

BY: Keith S. Shikowitz, Editor in Chief/Investigative Reporter

Credit card skimming devices are a problem for consumers and businesses. They scan your card and get the information off of them for a criminal to be able to use your card to make purchases.

Credit card skimmers are illegal devices placed on ATMs, gas pumps, or point-of-sale terminals to steal card data—often including the card number, expiration date, and sometimes the PIN—costing consumers and banks over $1 billion annually according to the FBI.

What a Credit Card Skimmer Is

A skimmer is a hidden device criminals attach on or inside a legitimate card reader to capture data from the magnetic stripe or chip. They are commonly found at ATMs, fuel pumps, and POS terminals, especially unattended or outdoor machines. Some setups include pinhole cameras or keypad overlays to record PIN entries.

How Skimmers Work

When you swipe or insert your card, the skimmer copies the card's data and stores it for later retrieval or wireless transmission. Criminals may use the stolen data to make fraudulent purchases, create counterfeit cards, or sell the information.

Newer "shimmers" can be inserted into chip readers to steal EMV chip data.



Officer checking for skimming devices

Due to the prevalence this type of crime, The Haverstraw Police Department, working alongside the Rockland County Intelligence Center, conducted another round of proactive inspections at local businesses to check for credit card skimming devices.

The inspections are part of an ongoing effort to protect residents from financial fraud and identity theft by identifying and preventing the use of illegal devices designed to steal customers' credit and debit card information.

The police investigation reported that no credit card skimming devices were discovered during the latest inspections.

The department says it will continue conducting proactive business inspections while working closely with local business owners and law enforcement partners to prevent crime and protect the community.

Officials emphasized the importance of these partnerships in helping safeguard residents and keeping Haverstraw businesses safe.

Types of Skimming Devices

Overlay skimmers: Fit over the existing card slot or keypad and mimic the original hardware.
Internal skimmers: Installed inside the machine's wiring, often invisible from the outside.
Keypad overlays: Capture keystrokes to steal PINs.
Cameras: Hidden near ATMs to record PIN entry.
Digital e-skimmers: Malicious scripts injected into online checkout pages (Magecart-style).

How to Spot a Skimmer

Look for misaligned or loose card readers, unusual bulkiness, or mismatched colors.
Compare the reader with nearby machines for differences.
Check for broken security seals on gas pumps.
Inspect the keypad—if it feels thicker or moves, it may be an overlay.

How to Protect Yourself

Use tap-to-pay, contactless cards, or digital wallets—these are harder to skim.
Prefer indoor or attended terminals; pumps near the store are safer.
Cover the keypad when entering your PIN.
Enable real-time transaction alerts from your bank.
If you suspect tampering, don't use the machine and report it to your bank or the FBI's IC3.

What to Do if You're a Victim

Contact your card issuer immediately to freeze or replace your card.
Review recent transactions and dispute unauthorized charges.
Change your PIN and monitor accounts for further activity.
Credit card skimming remains a widespread and evolving threat, making vigilance and secure payment habits essential.