Lynn Fitch
ATTORNEY GENERAL

STOP THE SKIM

Protecting Your Business and Customers From Fraud

Across Mississippi, businesses are increasingly targeted by criminals using skimming devices to steal sensitive information, including bank card data and SNAP benefits.

These crimes not only harm your customers but can also damage your business's reputation and trust. By understanding how skimmers work and taking proactive steps to inspect your equipment, you play a vital role in protecting both your business and your community from financial fraud.

For more resources and information on how to protect your business and customers from the dangers of cyber crime, visit:

Scan Me

KNOW THE THREAT

Types of Skimmers:

Overlay Skimmers

- Attached directly to a Point-of-Sale (PoS) terminal using double-sided tape.
- Record magnetic-stripe data and PINs, often using Bluetooth to send stolen info.
- Powered by small batteries and can stay in place for long periods.
- Thieves return later to collect stolen data using a mobile device.

Deep Insert Skimmers

- Hidden inside ATM or gas pump card slots using thin metal tools.
- Collect card data and often pair with a false panel that hides a pinhole camera to record PIN entries.
- Devices are battery-powered and temporary. Thieves remove once the data is gathered.

Prevent Fraud:

Routine Terminal Checks

- Inspect all terminals at least twice daily.
- Keep a log with dates, times, and staff initials.
- Look for loose parts, new panels, or mismatched colors.
- Include standalone ATMs in your checks.

If You Find a Skimmer

- Stop use immediately. Cover the terminal to prevent transactions.
- Do not touch the device to preserve evidence.
- Contact local law enforcement right away.
- If your agency needs assistance, email the **Mississippi Cyber Fraud Task Force** at **cftf@ago.ms.gov**
- Ensure your security cameras are functioning and time-stamped correctly.
- Download video footage of suspects—don't record it with a cellphone.