The Skinny On Skimmers

As a way to get rich quick, fraudsters are using card skimmers to target the financial services industry.

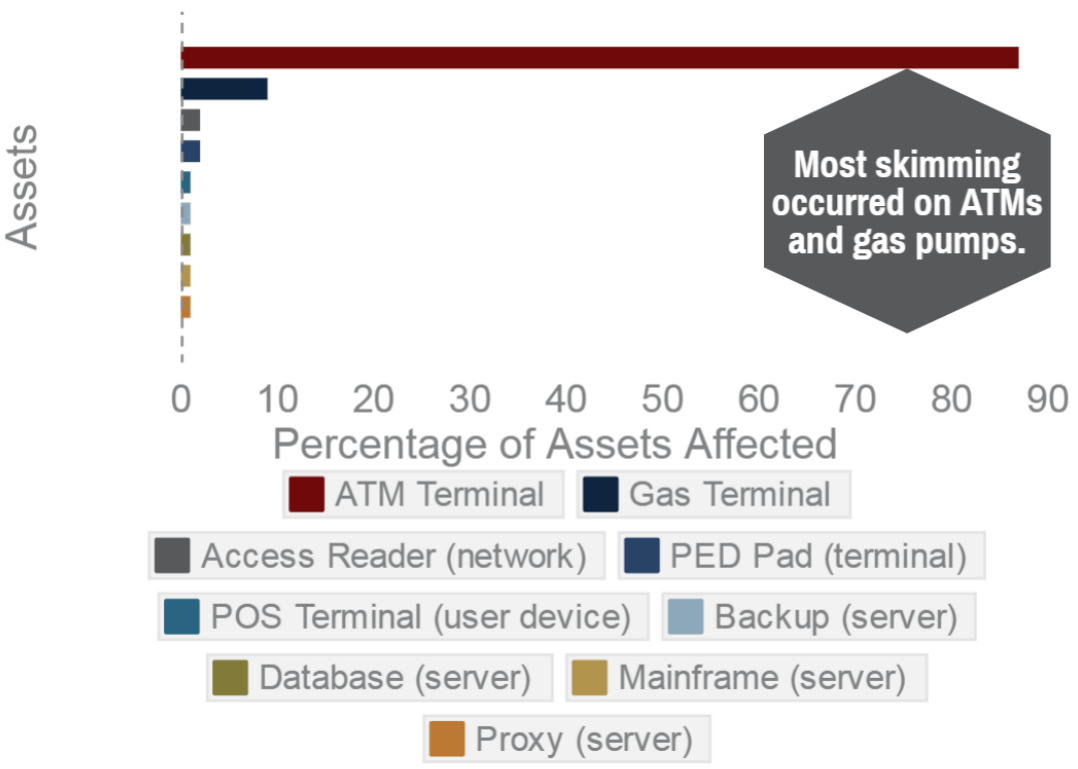
Q: What Is A Payment Card Skimming Device?

A: An object physically implanted onto a card-reading device that lifts magnetic stripe data when a user swipes a payment card.

Q: Why Should Credit Unions Care?

A: Increasingly sophisticated skimmers and technologies such as Bluetooth and cellular transmission make it easier to retrieve stolen data without physically returning to the tampered device.

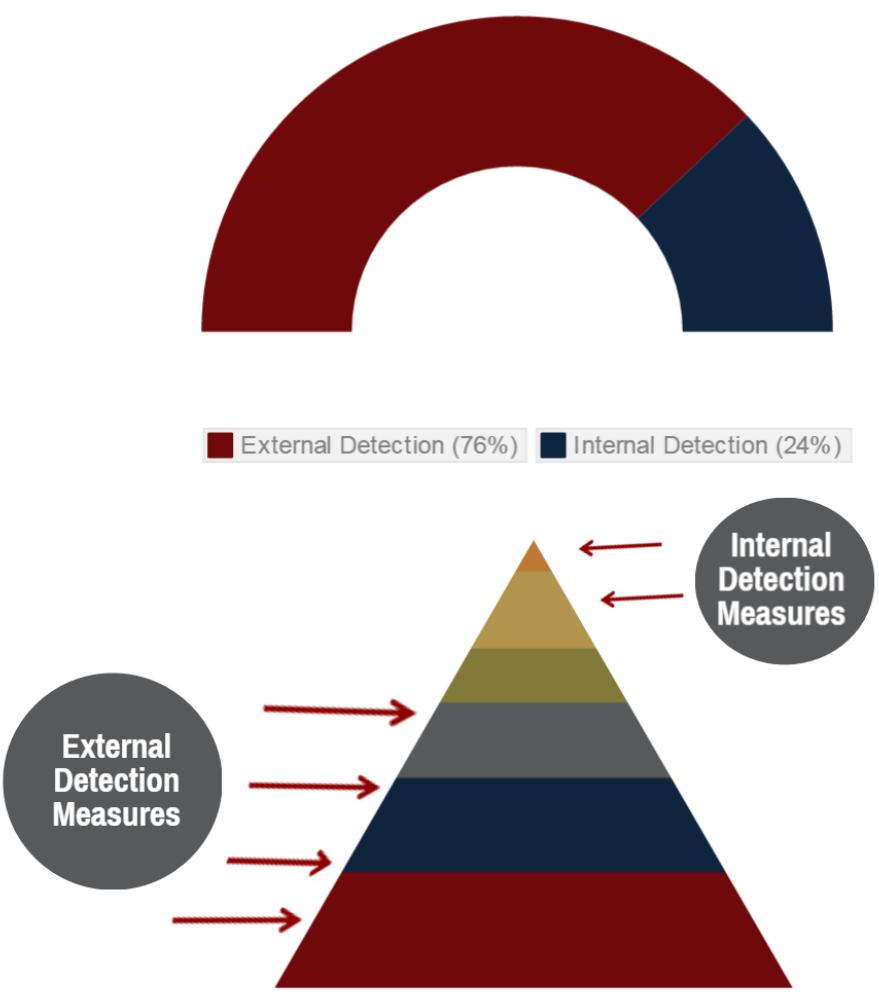
WHERE ARE CARD SKIMMERS?

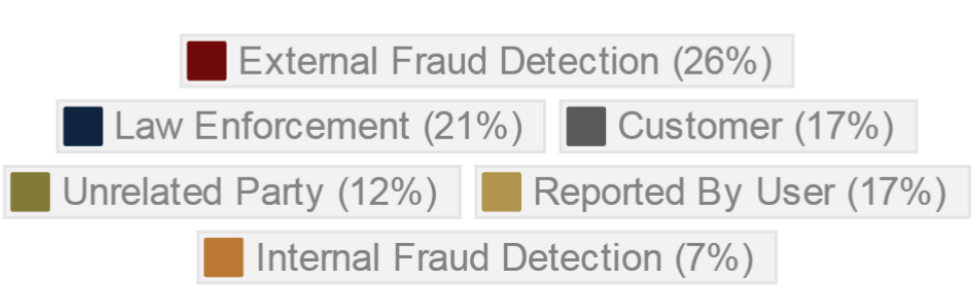


Did You Know?

In 2013, 87% of skimming occurred on ATMs. Some skimming devices now send an SMS alert to fraudsters each time the ATM is used.

HOW DO YOU FIND CARD SKIMMERS?





3 Ways To Mitigate Card-Skimming Risk

No.1 — Design or buy tamper-resistant ATM terminals.

No. 2 — Use tamper-evident controls on ATM terminals.

No. 3 — Watch for tampering on ATM terminals.

3 Ways Members Can Increase Data Security

No.1 — Protect their PIN. Namely, tell members to cover their hand to block the cameras that might be recording them as they enter their PIN.

No. 2 — Trust their gut. Remind members to stay alert and if something looks off at the ATM, do not swipe their card.

No. 3 — Use their voice. Ask members to say something when they see something.

The Bottom Line

Even standard offerings, such as ATMs, are vulnerable in today's cyber landscape. Vigilance and awareness are crucial to fortifying all aspects of your credit union's services and operations.

CALLAHAN & ASSOCIATES

Source: Verizon's 2014 Data Breach Investigations Report