WINSTON & STRAWN LLP

BLOG

# Payment Card Industry Security Standards Council Releases Updates Skimming Best Practices

OCTOBER 2, 2014

The Payment Card Industry Security Standards Council ("PCI SSC") recently released updated payment skimming prevention best practices. As described by the PCI SSC, skimming is the fraudulent and "unauthorized capture and transfer of payment data to another source" and can occur from many events, a few of which include: data from consumer payment cards (acquisition occurs directly from the consumer's payment card), data capture from the payment infrastructure at merchant location (point of sale), data capture from malware or compromised software (ATMs, ECRs, mobile devices), or data capture from wireless interfaces (Bluetooth or Wifi). The guide provides pictures and watch outs for common skimming techniques. For example, it shows an image of a tampered credit card machine with an additional wire on the PIN board. PCI SSI explains that merchants should be aware of the addition of overlays (stickers that cover the key board area) on such devices because criminals use such overlays to hide wires and/or evidence of tampering.

**Tip: This new guideline, intended for the technology teams in companies, may provide help for retailers who are working to combat skimming. It also represents the expectations from the payment card industry.**

1 Min Read

## Related Locations

Chicago

## Related Topics

Data Breach

## Related Capabilities

Privacy & Data Security

*This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.*