Employee Credit Card Skimmers

Credit card "skimming" is an alarmingly escalating form of fraud that is victimizing consumers, causing havoc with merchants, and costing the industry hundreds of millions of dollars every year. Generally, a cardholder turns over physical possession of his or her card to a retail or restaurant employee, who then swipes the card through a small, illegal card reader, called a "skimmer". The skimmer copies the data encoded on the card's magnetic stripe. This information is then used to manufacture counterfeit cards. The average skimmed credit card will generate some $2,000 in fraudulent charges before being detected.

The retailer or restaurant is not actually the target, or the victim, except in the form of 'ill will' from the now-former customer.

This can be especially damaging to a business. Not only have they lost the original customer; they've now potentially lost countless other customers based on the victim telling everyone he/she knows about the bad experience they had at the business.

Plus, penalties for merchants can be severe if the security of their credit card terminals is compromised, ranging from large fines by the issuer to complete exclusion from the system, which can be a death blow to businesses such as restaurants where credit card transactions are the norm.

How can businesses protect themselves?

Merchants must ensure the physical security of their terminals. Check the equipment regularly.

Be sure to supervise your employees actively. Pay attention to what they're doing and saying. No need to micromanage, but be tuned in and aware.