Credit Card Skimming – A business and customer nightmare

> "Hey man; how do like your job at that fast food place?" "It's alright. It gives me a bit of cash for some bills, and I get to eat for half price." "So, do you work much in the drive-thru?" "Yeah, I …
>
> Tags: Business Strategy and Profitability, Loss Prevention, Operations Management
>
> "Libby" Libhart

"Hey man; how do like your job at that fast food place?"

"It's alright. It gives me a bit of cash for some bills, and I get to eat for half price."

"So, do you work much in the drive-thru?"

"Yeah, I work the drive-thru cash quite a bit. Why do you ask?"

"Well, how would you like to make a LOT of easy money while you're working the drive-thru?"

"Keep talking; I'm listening."

"OK, here's the deal. I know these guys that will give you a credit card skimmer that fits in your pocket. All you have to do is run a credit card through it at the same time you swipe a customer's card as you ring up a sale. You get to decide when you think it's safe and won't get caught. You get paid $25 for every card you swipe in the skimmer. What's beautiful is that it doesn't matter what kind of credit card it is. You get paid for all of them. You meet with me after your shift, give me the skimmer and I pay you for all the information you've swiped. I'll give you another empty skimmer and we do it all over again. It's that simple. Are you in?"

"Oh yeah, I'm all in. Sounds great; let's go!"

This conversation could possibly be taking place with your employees. Credit card skimming is an epidemic in quick service and fast casual restaurants as employees such as the one above are recruited or planted by organized crime rings. The primary targets for the collusion are low-wage employees that handle customer credit card transactions. In this case, it is happening through the drive-thru cashier. They handle a lot of credit card transactions in relative isolation. The customer information captured on the portable skimming device is used to make fraudulent credit cards. Customer identities are stolen to produce other fraudulent documents such as driver's licenses and credit applications. The result is often a trail of unhappy customers with credit messes to clean up, large amounts of stolen merchandise, and a public relations nightmare for the company.

As described in the article "Wrestling with a million dollar baby," credit card skimming at several high-end restaurants in the New York metro area received a great deal of negative publicity when patrons were scammed in a $1 million theft scheme. Their high credit limit cards were targeted, identities stolen, and fraudulent credit cards were produced. The retail purchases of expensive, easily fenced items were converted to cash. Twenty eight servers and non-employee conspirators were eventually caught and criminally charged.

In May, two Popeye's employees were arrested for skimming the credit cards of 70 customers. Last month a McDonald's drive-thru cashier was convicted of skimming more than 270 customer credit cards in just three weeks. More than $51,000 in fraudulent charges were made on customer's credit accounts. In court documents the ex-McDonald's employee stated that he was recruited to capture the customer credit information on a portable skimmer in exchange for $600, two laptop computers and a video game system. Four others also were convicted in the theft scheme and face two years in prison. Meanwhile hundreds of customers are unraveling damage to their credit and other identity theft issues. These are just a few examples of skimming fraud and the devastating losses that are associated with the crime. Another victim in all of this is the restaurant. The negative publicity of the crimes originating from restaurant employees handling customer credit cards erodes the public trust, adversely affecting business.

As a restaurant owner, there are several steps to avoid this crime and what you can do if it does occur:

Understand that the theft scheme exists and how it is perpetuated.
Prohibit unauthorized portable skimmers on the premises in company policy.
Know what a portable skimmer looks like. There are pictures of various types on-line.
Train all supervisors on the scam and what to look for.
React quickly to complaints from customers or law enforcement that a credit card may have been compromised.
Pinpoint the time and date of suspected customer transaction, if possible.
If original receipt is available, identify employee that handled the transaction.
Compare time and date of suspected transaction with employee schedules.
Review CCTV recorded video, if available.
If multiple incidences have occurred, develop a chart comparing times/dates with employee schedules.
Review the chart for an employee that was predominately present when crimes occurred.
Cooperate with law enforcement and credit card processing companies.
Consider bringing in loss prevention professional to assist with the investigation.
Prepare a statement for any media inquiries stating cooperation with law enforcement investigation.
Avoid speculation until the facts are known.

Reports indicate that credit card skimming scam losses total more than $200 million a year, just in the restaurant industry. It's clear that no restaurant company is immune. When the schemes are uncovered, the thefts and losses have been staggering. Retail and restaurant management training on skimming fraud schemes is essential in slowing this crime trend. Consult with your credit card processer or a loss prevention consultant for training sessions on preventative measures, recognizing the scheme, identifying the culprits, and taking the appropriate action. It's a crime of opportunity that can be prevented through education, training, and proper supervision.

For more information on security, safety, loss and crime prevention for restaurants, visit www.LossBusters.com. For daily tips on restaurant loss prevention, follow on Twitter @LossBusters