



September 3, 2008

## Credit card shaving: Scammers go low-tech with trick

Glue sticks and sharp knives power this scam

By Lisa Rogak

Forget high-tech hacking. One new credit card scam relies more on X-Acto knives and glue sticks than wi-fi and laptops, but helps criminals steal your money just the same.

### Credit card shaving

Shaving is a low-tech form of card theft where thieves sort through sets of 16-digit numbers to find one that matches an existing card, and then verifying that number either by trying to make a purchase online or by phone. The scammers can also buy a list of valid credit card numbers from black market sites online. Once they have their hands on a valid account number, they then create a new card with those numbers by shaving the numbers off of gift cards or expired credit cards and gluing them onto a defunct or stolen card. The magnetic strip is gouged with a knife or pen so that a store clerk has to manually enter the account number on a keypad, and the charge goes through.

If they're successful, months can pass before a cardholder discovers the fraud. After all, if your wallet hasn't been stolen and you haven't misplaced a card, you may be puzzled to discover that your card has been compromised even though it's safely tucked away the entire time.

While it might not be the simplest way to commit an identity theft, card shaving is on the rise. "Desperate times mean desperate measures," said Robert Siciliano, CEO of IDTheftSecurity.com and author of "The Safety Minute: Living on High Alert." "In this economy, we are seeing scams of all kinds resurfacing, including credit card shaving."

### Both merchants and consumers are gatekeepers

Card shaving's growth comes partly as a reaction to increased high-tech credit card security steps, experts say. "As regulations and security tightened on electronic credit card processing networks, it became increasingly difficult for hackers to penetrate them," says Shyam Krishnan, an industry analyst with the Smart Cards group at Frost & Sullivan, a high-tech research and consulting firm. And so they turned to other low-tech scams, such as card shaving.

Because the scam requires clerks to enter the card number manually, merchants are the first line of defense in catching the perpetrators. These fraudulent cards usually look suspicious to begin with -- the numbers and letters often haphazardly glued on -- and that alone should raise red flags with store clerks and cashiers. However, many shaving scammers primarily use the cards in busy bargain stores where clerks are too harried to pay much attention and verification systems are so outdated that they don't require a matching ZIP code or other personal data.

"If merchants physically inspect all cards, they'll minimize the incidents of counterfeit cards being used," says Tom Harkins, chief strategy officer at Secure Identity Systems.

It's in the merchant's best financial interest to keep a watchful eye. After all, any charges made with the number would likely be disputed by the card's rightful owner, leaving the merchant with little option but to absorb the loss through a chargeback. That's why Siciliano recommends that merchants refuse service if the card doesn't scan. "Manually typing the card number in when there is even a hint of suspicion is risky," he says.

Merchants should also turn the card over and ensure the back of the card has the proper marks. For sales conducted without a card for online or phone transactions, Harkins advises merchants to protect themselves by requesting the three-number security code on the back of the card (four digits and on the front of American Express cards). "If it doesn't match, ask additional questions or investigate the customer before completing the transaction," he says.

Inevitably, some of the scammers will succeed, and unless the cardholder has a firm handle on his or her



account, the crime can go entirely unnoticed. Experts say this further reinforces the need for cardholder diligence on a regular basis. "It's vital to check your balances and accounts on a regular basis and report any suspicious purchases to help identify the theft quickly," says Krishnan.

### **Disposable card numbers are one solution**

Another way consumers can fight shaving is with a credit card account that generates a new number for every new transaction. Citibank offers Virtual Account Numbers to cardholders for online purchases while PayPal provides the Secure Card in the form of a MasterCard debit card. While these can only be used online, Qsecure is rolling out a SmartStripe credit and debit card that looks like any other card. However, a chip embedded in the card's magnetic stripe automatically generates a different number for each purchase.

### **ABOUT SECURE IDENTITY SYSTEMS**

Secure Identity Systems is the leading provider of managed total identity theft protection systems that safeguard financial institutions, businesses, individuals, and households. For more information, visit [secureidentitiesystems.com/](http://secureidentitiesystems.com/).