

Is Your Debit Card a Fast Pass to ID Theft?

By Tom Spring, PC World

1 | 2 | [Next >](#)

Using your debit or credit card to pay for goods could be expensive if a scammer is bugging your store's keypad. It's happened in six states so far.

Living cashlessly is convenient. We swipe our credit and debit cards to buy gas, lunch, coffee, and groceries. But now, data thieves--eager to exploit U.S. consumers' dependence on plastic--are targeting keypads that we don't think twice about swiping our cards through.

Authorities in a number of states have reported local instances of a new high-tech crime: Crooks replacing or "bugging" checkout keypads at grocery and convenience stores. The rigged keypads record your credit card number or the personal identification number (PIN) that you key in when using your debit card. The crooks later return to collect the keypads--sometimes by ripping them from checkout aisles--and use the intercepted data to siphon large sums of money from unsuspecting store patrons.

Usually, the keypad devices show no outward signs of tampering. But inside, authorities say, scammers attach skimming devices that pass along customer data to the merchant (just as a normal keypad would), but also collect and store every credit card number, name, and debit card PIN entered on them.

The Cost to Consumers

The amounts that authorities suspect keypad thieves of stealing vary. Las Vegas police say that the total take in a crooked keypad scam in their jurisdiction may have been in the "millions of dollars"; representatives from the other affected states--California, Florida, Massachusetts, Pennsylvania, and Rhode Island--put the estimated cost to consumers at around \$100,000 in each case. The magnitude of the actual losses may never be known, authorities say.

Sound Off: ID theft protection tips for a 'Regular Joe'

In Las Vegas, for example, hundreds of people had their financial information stolen when they stopped at convenience stores to grab a snack or fill up their gas tanks, according to the Las Vegas Metropolitan Police Department. Both in-store point-of-sale keypads and gas-pump keypads were compromised in a number of locations in the city, police say. Law enforcement officials are still investigating complaints, but no arrests have been made.

In Rhode Island, the Coventry Police Department says that it had better luck catching keypad crooks. In February, with help from U.S. Secret Service agents, four suspects from California men were arrested for having replaced checkout-lane keypads with the equivalent of electronic bugs. Investigators discovered bugs designed to steal customers' account information in keypads at Shop & Shop grocery stores in Bristol, Coventry, Cranston, Providence, and Warwick, Rhode Island, and in Seekonk, Massachusetts.

Subsequently, Coventry police, together with Rhode Island State Police, arrested the men

Tech Showcase: Video, Audio & Slide Shows



[Insider Secrets: GPS basics](#)
[First Look: Nokia E61i PDA](#)
[First Look: Dell Inspiron 531](#)
[First Look: Hercules Mobile DJ MP3 player](#)

[More Showcase titles ...](#)

advertisement

Most Popular on MSN Tech & Gadgets

[iPhone: Lots to love, but flaws too](#)
[Top executives face e-mail attacks](#)
[Slide show: A history of cell phones](#)
[11 iPhone gotchas](#)
[25 Web sites to watch](#)
[iPhone alternatives](#)

[More News & Features ...](#)

Product Shopping Center

Consider this...



[Logitech AudioStation speaker system with iPod dock](#)
 Just add your iPod to create a full-function stereo that fills any room in your home with high-performance sound. [Compare prices at MSN Shopping.](#)

More on MSN

Live Earth concerts	Grilling guide
Win in Las Vegas	Dog central
Inside MSN	Wimbledon coverage

when they returned to collect compromised keypads from affected stores, says detective Marcos Saenko, a member of the financial crimes unit of the Coventry police. The four suspects, all of whom are natives of Armenia, face two federal charges each: credit-card fraud and aggravated identity theft. Conviction on the first charge carries a penalty of up to five years in prison, while a finding of guilt on the second charge carries a mandatory two-year sentence.

[Mari Frank](#), attorney and author of "[Safeguard Your Identity](#)," says that theft of customer data at the point of sale is one of the most dangerous security risks facing consumers. "If someone gets your financial information, your entire bank account can be wiped out," she says.

Checkout Line Quandary

Unfortunately, protecting yourself isn't easy.

"There really isn't much anyone can do if the store has been compromised," says William Oettinger, who works with the Las Vegas Metropolitan Police Department and the Secret Service's electronic crimes task force.

Content by:



CONTINUED: [Copycat Credit Card Con](#)

[1](#) | [2](#) | [Next >](#)



[Print this article](#)

More About Security From Tech & Gadgets

[Is Web 2.0 safe?](#)

[Is it a virus? Get a 2nd opinion](#)

[Banking by phone](#)

[More Security articles...](#)

Got a question? [Post it to the Security & Antivirus message board.](#)