

## Is Your Credit Card Vulnerable at ATMs and Gas Stations?

2-23-16

The next time you use an ATM or pay at the pump beware of a skimming scam. The Middlesex County Prosecutor says thieves are planting tiny cameras over the card readers at banks and gas stations and secretly recording your credit card numbers — even passwords. The executive director of the [New Jersey Gasoline C-Store and Automotive Association](#) says skimmers are being found at gas pumps. Sal Risalvato joined NJTV News Anchor Mary Alice Williams to discuss how skimming fraud works.

**Williams:** Can you tell us exactly what is skimming?

**Risalvato:** Skimming is a very surreptitious way of stealing your credit card information and then using that information to quickly make purchases fraudulently before anybody can find out that their credit card information has been stolen.

**Williams:** How prevalent is this?

**Risalvato:** It is growing as a problem and it's being found in more and more locations. Not just gas pumps, but ATMs and anybody that takes a credit card — any cashier that takes a credit card can have a skimming device. The cashier may not even know that the skimming device has been put on the credit card reader.

**Williams:** It's that small? Have we seen an increase in this? Why do you think that is?

**Risalvato:** Because there's just a group of people out there that are evil and they keep coming up with new ways to beat technology. That's why last year we were asked to go to what's called the EMV type credit cards with chips in them, so that you have to put your credit card into the credit card reader and it reads a chip and then when it reads the chip you are supposed to put in a PIN number. Now at ATMs you are required to put in your PIN number, but not all retailers yet are requiring the PIN number to be put in.

**Williams:** [Not all the chip readers are working yet](#). But let me ask you this: what makes sidewalk ATMs or gas pumps vulnerable?

**Risalvato:** What makes them vulnerable is it's easier for someone to sneak the card reader, the skimmer, into the card reading apparatus.

**Williams:** I know if there's fraud at a bank, an ATM, the bank covers it. What about gas stations? Do you take the loss if somebody's information is swiped?

**Risalvato:** If the credit card was not processed properly then the burden of the fraud is on the retailer. But today the burden of fraud is not just the amount of money that's stolen, it is also the identity theft. So today when there's a breach of credit card data and an identity is stolen there's a cost that goes with that that goes beyond the card for stolen merchandise.

**Williams:** Is there anything customers can be doing to protect themselves at this point? What are you telling people?

**Risalvato:** One of the things that they can do is always use a PIN. Not everybody has a PIN with their credit card, but they should get one. They should look for retailers who require a PIN before they insert their credit card. They should never give their credit card to a cashier or an attendant. They should never lose possession of their credit card and therefore they have greater control over that credit card. When they put their PIN numbers in they should always shield it from the possibility that a camera could be watching and recording the PIN number that they put in.