Credit Card SHIMMING

consumer *brief*

The stealing of personal data from credit cards, known as skimming, has been a persistent and growing problem for several years. The introduction of chip and pin credit cards to the United States was supposed to reduce the risk of skimming. Unfortunately, it appears to have resulted in a new and more technologically advanced crime – shimming.

The chips can't be replicated. That's why in order to steal consumer's information, scammers need to capture data by tapping directly into an EMV chip.

HOW DOES IT WORK?

Individuals seeking to steal personal information from credit cards through shimming look like normal bank customers seeking to use an ATM; instead, they attach an ultra-thin reader card, called a "shim," to a card they insert in the ATM. Once inserted, the shim gets implanted over the ATM's internal card reader which then stores information from subsequent users of the ATM by "contact" with the card's chip. Those who placed the shim in the ATM merely need to extract the shim from the ATM to retrieve the stolen personal information which can then be used to create fake credit cards with fraudulent magnetic strips.

HOW CAN SHIMMING BE DETECTED?

The shim reader cards are incredibly thin and can be difficult to notice. They also can be used at nearly any ATM, unlike older "skimming" devices which were generally deployed in outdoor machines. But consumers can become aware of the presence of shims if they have difficulty inserting their cards into an ATM. If a card does not fit easily into the ATM, consumers should not not use the machine and should immediately report the situation to the bank or the establishment where the ATM is located.

TIPS

- Use ATMs that you are familiar with. You may notice subtle differences the next time you insert your card, which could alert you to potential shimming.
- Because criminals tend to install shimmers where they are less likely to be detected during the installation process (for example, ATMs that are not well lit or point of sale terminals that don't have a lot of supervision), make sure that you are using ATMs and/or cash registers that are out in the open and in well-lit and public areas.

- Only use cards with "chip" technology. Chip cards have additional safety features that make the cloning of cards more difficult, although not impossible. The goal is to make it as hard as possible for criminals to steal personal information.

Continued

- If your card fits too tightly into the card acceptance slot, stop the transaction, remove and secure your card, and immediately contact your financial institution or the establishment where the ATM is located.
- Frequently check your bank account and credit card statements for irregularities and unauthorized withdrawals. If you find any, immediately notify your bank or the issuer of your credit card.
- Try to use a credit card that offers fraud protection and alerts without additional fees.
- If the issuing bank has an app that will alert you to recent purchases, use it. Respond immediately if you see unauthorized purchases. This can prevent further illegal usage of your information.
- If you are going to use a card, opt for a credit card. Many credit cards offer extra protections, such as extended warranties or protection against theft, breakage or loss. Plus, if you need to dispute the charge, the credit card issuer may withhold payment until the dispute is cleared up.

IF YOU BECOME A VICTIM

Contact the three major credit bureau Fraud Hotlines at:

Equifax:	800-525-6285 www.equifax.com
Experian:	888-397-3742 www.experian.com
Trans Union:	800-680-7289 www.transunion.com

New Jersey Office of the Attorney General

DIVISION OF CONSUMER AFFAIRS

NEWARK
124 Halsey Street
P.O. Box 45025
Newark, NJ 07101
973-504-6200
800-242-5846
(toll free within N.J.)

E-Mail:
AskConsumerAffairs@dca.lps.state.nj.us

website:
www.NJConsumerAffairs.gov