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 has resulted in a new and more technologically advanced crime – shimming.

HOW DOES IT WORK?

Individuals seeking to steal personal information from credit cards through shimming insert an ultra-thin reader card, called a "shim," into the card reader slot. Once inserted, the shim blocks the ATM's internal card reader and stores information from subsequent users of the ATM by reading 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, do not not use the machine. Immediately report the situation to your bank and 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 terminals that don't have a lot of supervision), make sure you are using ATMs that are out in the open and in well-lit, public areas.
- You should still 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.

- 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.
- Use a credit card that offers fraud protection and alerts without additional fees.

Continued

- 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.
- Use credit cards rather than debit cards. 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 to the seller until the dispute is cleared up.

IF YOU BECOME A VICTIM

Contact the four major credit bureau fraud hotlines at:

Equifax: 1-800-685-1111
www.Equifax.com/personal/credit-report-services

Experian: 1-888-397-3742
www.Experian.com/help

Trans Union: 1-888-909-8872
www.TransUnion.com/credit-help

Innovis: 1-800-540-2505
www.innovis.com

If you have a question and/or complaint concerning a consumer-related issue, or would like to check the license or complaint history of any professional or business, you may contact the **New Jersey Division of Consumer Affairs** by mail, phone or online.

Consumer Service Center
124 Halsey Street
P.O. Box 45025
Newark, NJ 07101

1-973-504-6200
1-800-242-5846

E-Mail:
AskConsumerAffairs@dca.njoag.gov

NJConsumerAffairs.gov