ATM Skimming Alert

One form of fraud that has been increasing across the country at banks, credit unions, and gas stations is the use of skimmers. A skimmer is a device that criminals attach to a payment terminal, most commonly on ATMs and gas pumps. If you use a terminal that has been compromised in such a way, the skimmer will capture data from your card and capture your PIN, usually through a small camera that is mounted near the terminal. With this information, the criminals can produce a duplicate card and begin withdrawing money from your account.

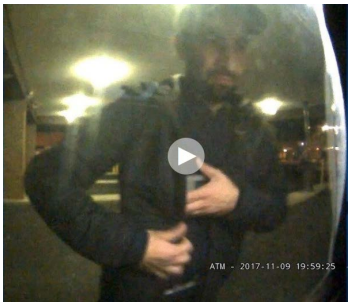
In Columbus this year, there have been a number of large banks that have been hit with skimmers, as well as several local credit unions**. During the week of November 6, 2017, Pathways also had a skimmer placed on one of our ATMs *(at our 750 Georgesville Road branch)* for a period of time.**

We were able to detect the issue shortly after it started and limit the impact to a very small number of our members. We have notified all of these members and we are replacing their debit cards for them. ***None of our members lost any money as a result of the incident; any fraudulent ATM transactions were promptly reimbursed.***

We have taken additional steps to help reduce the possibility of this occurring again on our ATMs, but if you use your debit card at ATMs and gas stations, you will want to be vigilant to help protect yourself.

ABC6 News Article & Video

Click the image on the right to view the ABC6 News article covering the skimming event and to help identify the thief.



How to Protect Yourself from Skimmers

If you use your debit card at ATMs and at gas stations *(and who doesn't)* you can't with 100% confidence completely eliminate the risk of having your card data compromised by a skimmer. But here are a few simple steps that can significantly reduce your exposure to the risk.

1. Most current skimmers rely on a hidden camera to capture your PIN as you enter it into the key pad. One effective way to foil this device is to shield the PIN pad with one hand as you type in your PIN *(see photo).* This won't protect you against more sophisticated skimmers that use keypad overlays, but currently you are much more likely to encounter a skimmer that uses a camera to capture your PIN. ***This simple step by itself will foil most skimmers that you are likely to encounter.***

2. Set up ***"Debit Card Alerts"*** in Pathways online banking for transactions over $100. This will generate an instant email/text alert anytime your debit card is used in any transaction over $100. If you get the alert and you *(or any of the authorized users on your card)* have not used the card, you may have a fraud issue. If this happens, you can call our card processor at 1-800-449-7728 anytime 24/7 and report it immediately. You can find detailed instructions on how to setup alerts at www.pathwayscu.com/resources/cardalerts/.

3. While the technology skimmers use is pretty simple, criminals are getting much more sophisticated in their ability to make the skimmers less detectable. However, it still pays to look over any card terminal you are using to see if there are any obvious signs that it has been tampered with or altered. If you find something that seems out of place *(a card reader that is loose, a hidden camera, or a keypad overlay),* take the cautious approach and do not use that terminal. Be sure to alert the business in charge of the terminal that there may be an issue as well.