# Don't Let Skimmers Steal Your Cash

By Bo Holland, Founder & CEO, Debix | AllClear ID

Identity thieves are placing credit card skimming devices everywhere, but particularly on gas pumps and on outdoor ATMs. These devices are small and hard for the typical person to detect, but they can be financially lethal. Skimmers are designed to capture credit and debit card information when one is scanned through for a purchase, and then they either transmit the information via a Bluetooth device to a nearby laptop, or store it locally for the thief to pick up at a later date. This information can then be used online or uploaded onto a counterfeit card for making purchases.

Skimmer devices are made to look exactly like the regular card scanner that is already on the ATM or gas pump, and they attach perfectly to the face of the machine. Most people never even notice that there is anything different with the machine they're using. The skimmer doesn't stop you from making your purchase or ATM transaction, so everything works as usual ; this makes it that much harder for the victim to realize anything is wrong.

Almost anyone with criminal intent could use this type of scam because it's very easy to pull off without getting caught. As a low-risk, high-reward crime, it attracts criminals even more. They can take your account information when you stop to get gas on your way to work in the morning, and steal hundreds or thousands of dollars from you by the time you get home that evening.

A scam like this can and does happen all over the country, but the highest concentration of the cases our AllClear ID's investigation team are seeing occur in Southern California, Arizona and Miami.

What can you do to protect yourself from skimming? Be cautious any time you use the pay-at-the-pump option at gas stations or an outdoor ATM. It is always safer to go inside the gas station and pay at the desk or use indoor ATMs for bank transactions, because it's harder for criminals to tamper with an indoor machine.

Also, it's easier to catch fraudulent activity on your accounts early before too much damage is done. While most banks and credit card companies attempt to notify you of suspicious charges on your account, they don't always catch everything. The best thing you can do is regularly check your statements yourself, and immediately notify your bank or credit card issuer of any fraudulent charges. You don't have to wait to get your monthly statements in the mail – it's easy to check your accounts online and most banks allow you to set up alerts that will send you an email or text message for important transactions. But make sure your computer is secure from malware and hackers that may try to steal your account numbers and passwords. Learn how to secure your computer and the sensitive information on it at the federal government's www.onguardonline.gov website.