

---

## **Skimming - Credit and Debit Card Fraud**

---

### **The Scenario**

Within a 3 week timespan, 25 employees and service members at a DoD installation reported fraudulent activity on their credit and/or debit cards. According to the police department, the fraudulent activity included unauthorized purchases and withdrawals from accounts and ranged from \$200 to \$600. Those who reported the fraudulent activity were positive that they had only used their cards while on the installation, this included usage at establishments such as the food court at the Exchange, gas station and commissary.

The investigation was assigned to the fraud division within the police department. The police department solicited the assistance of forensic auditors to also investigate and find any areas on the installation which may be vulnerable to this type of fraud. The investigators and auditors knew that they were possibly dealing with a card skimming scheme where the perpetrators installed equipment to capture credit/debit card information as patrons used credit/debit card machines. The auditors used data mining techniques to gather data from the victims of the credit/debit card fraud to draw connections between them, which led to fraud investigations at businesses in which all the victims frequented. In addition to the information from the victims, the police examined all the credit/debit card machines at the installation, interviewed store employees, and reviewed video from the surveillance cameras at various locations.

Skimming devices were found recovered at two of the self-checkout lanes at the commissary, three gas pumps, and an ATM that was not located within a financial institution's branch office, but at a separate kiosk. The one thing these locations had in common was that they lacked or only had a few attendants able to keep watch over payment and withdrawal terminals. Also, found near the credit/debit card machines were hidden cameras (hidden by a brochure rack or other promotional materials), which were used to record Personal Identification Numbers (PINs) as they were entered by the customer.

Some of the skimming devices were hard to detect because they matched the valid card readers. In other instances, the devices were easier to detect because they were loose. The devices were used to obtain the electronic data from the magnetic stripe on the cards and hidden cameras were used to capture the PINs. Information obtained from the cards was downloaded and used to commit fraud at a later time.

Now that the skimming devices had been seized, the investigators had to determine who was responsible for installing them. Even though the interviews with employees did not yield any leads, video from the security cameras provided vital information for the investigation. The security cameras provided images showing the perpetrators tampering with credit/debit card machines. Other video footage captured the perpetrators swapping the modified debit and credit card machines while store staff members were distracted. The perpetrators were eventually caught as they tried to install other skimming devices.

The police credited vigilant patrons for being alert and reviewing their accounts often. The police department advised patrons to monitor their bank accounts on a regular basis

to ensure the accuracy and legitimacy of transactions. In addition, they provided several precautions customers could take to avoid becoming a victim of credit/debit card fraud: The precautions included:

- Inspecting credit/debit card machines before using them. If anything is loose, bent or damaged, don't use it. You can gently tug on the device to see if it is loose.
- Using your hand or body to shield your PIN from onlookers when you are conducting transactions at a bank machine or at the point-of-sale.
- Reporting any unauthorized purchases immediately.
- Regularly checking your bank and billing statements to verify all transactions have been properly documented. If entries do not accurately reflect transaction activities (e.g. if there are missing or additional transactions), you should contact your financial institutions and police immediately.

Furthermore, the police advised customers to trust their instincts. A couple of the victims said that they had a feeling when they were using the machines that something wasn't right. If something doesn't look right or feel right, don't use the credit/debit card machine.

Based on these events, a lot of people realized that all businesses are at risk and capable of inadvertently being involved in fraudulent activities. Even though the perpetrators had been caught, the investigators and forensic auditors knew that as long as there are vulnerable credit/debit card devices out there, skimming will continue. The auditors recommended that the installation continue to use video camera monitoring as a tool to capture those involved in fraudulent activities.

**General Comments / Lessons Learned:** Card skimming can happen anywhere and it involves the unauthorized copying of electronic data from your credit/debit cards. Thieves use all of the information they have gathered to manufacture counterfeit cards, make purchases and withdraw funds from your accounts. Some skimming devices can be very sophisticated and hard to detect. One of the best ways to protect yourself against skimming and other types of fraud is to frequently review your accounts. Monitor accounts on a regular basis to detect fraudulent purchases, and immediately report them.

## **FRAUD INDICATORS**

- **Unauthorized purchases in your accounts.**
- **Loose, bent or damaged credit/debit card machines.**
- **Objects placed nearby the credit/debit card machine that might be concealing something, such as a camera.**
- **Your instinct suggests something is awry even if you cannot determine what exactly looks suspicious.**