# SAFEGUARD AGAINST SKIMMING

## EVERY DAY,

**Millions of purchases using debit and credit cards are conducted using payment card terminals throughout the world. Accepting card payments is safe, convenient, and essential to the smooth operation of any business.**

However, card fraud is a global problem and card skimming using payment card terminals could also occur at the University of Minnesota. Without the right safeguards in place, any area that uses terminals is potentially at risk. The impact of skimming is significant – it can lead to loss of money, loss of customers, and undermine the reputation and credibility of your business and the University. It is vital that you know how to prevent and detect skimming so you can protect your customers and your business from this type of fraud.

This information is a part of the University of Minnesota's program to increase awareness on how to safeguard your terminals against skimming. Additional security awareness resources can be located on the University of Minnesota Payment Card Industry Data Security Standards (PCI DSS) website.

## WHAT IS SKIMMING?

Card skimming is a crime. Using sophisticated skimming techniques, criminals steal or skim data from a customer's card during a transaction using a terminal. More experienced criminals could also attempt to get the customer's PIN at the same time. Once they have this information, it is used in various ways to take money from the customer's account.

### HOW ARE CARDS SKIMMED?

Payment card terminals do not save customers' card or PIN details. To skim cards using a terminal, criminals need to apply an overlay, attach external devices such as flash drives, or swap your terminal with one they have already modified. Either way, they need to get access to your terminal.

To do this, criminals may:

- Pretend to be a technician that has come to service your terminal.
- Distract you or make a disturbance so that attention is taken away from the terminal.
- Look for a terminal that has been left unattended or is not locked down.

Often criminals will modify terminals to skim cards and capture customers' PINs. However, criminals may also try to steal PINs by other means including:

- Hiding a pinhole camera in a box or other item close to the terminal.
- Placing a pinhole camera behind a hole in the ceiling or walls.
- Using a security camera in your area to record customers entering their PIN.

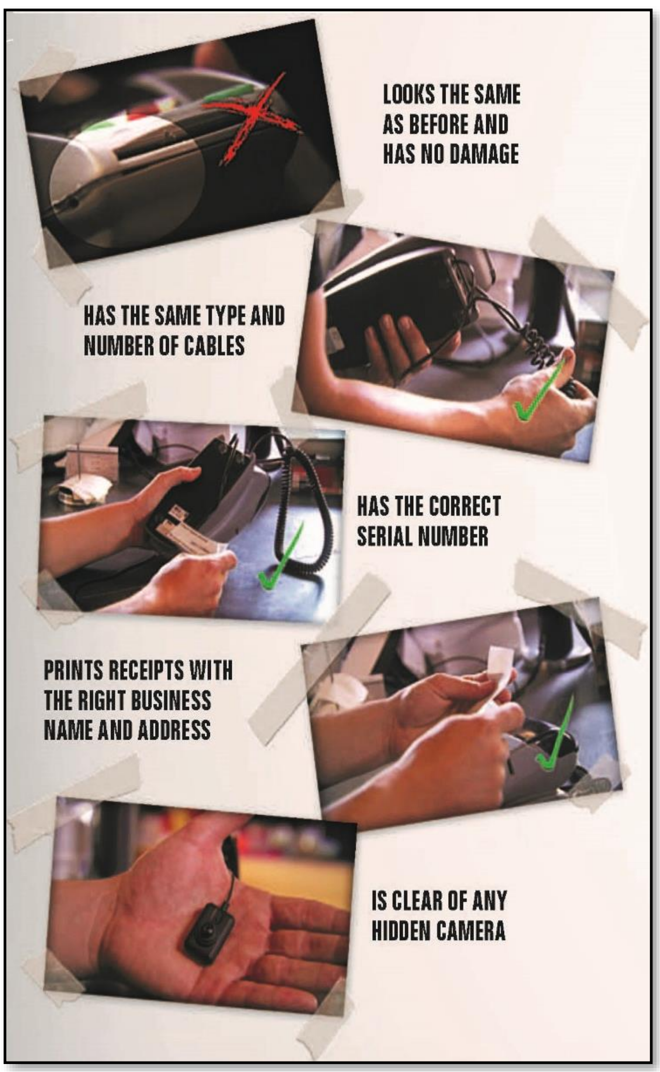
# HOW DO I SAFEGUARD AGAINST SKIMMING?

**You can reduce the risk of skimming in your area by taking a few simple steps.**

### 1. CHECK YOUR TERMINAL

Take careful note of the little things that are unique to your terminal and the area around your terminal. Regularly check that your terminal:

a) *Looks the same as before and has no damage.*
b) *Has the same type and number of cables.*
c) *Has the correct serial number.*
d) *Prints receipts with the right business name and address.*
e) *Is clear of any hidden camera.*




### 2. TAKE ACTION

Be constantly aware of your terminal and how it is being handled - protect it like you would cash. It is preferred that your terminal be physically attached to a counter: If your terminal is not attached to a counter:

- Make sure you put the terminal out of sight and reach of customers if you must leave the immediate area.
- Lock the terminal away at night.

If you see anyone acting strangely near the terminals or security cameras in your area:

- Do not approach the person.
- Watch them closely without putting yourself in danger.
- Contact your supervisor as soon as it is safe to do so.

Importantly, you can help safeguard against skimming by telling your supervisor immediately if:

- You notice anything different or suspicious during your daily checks.
- A visitor arrives to service or replace a terminal or security camera.
- Your terminal is missing.
- You see anyone acting strangely or committing a crime.

If you notice anything different or suspicious, take action. **Tell your supervisor immediately.**

# IMPORTANT INFORMATION FOR SUPERVISORS

## 1. KNOW YOUR TERMINALS

It is essential that you and your staff are completely familiar with your area's terminals so that you can **spot any changes quickly and take action**. Any change to a terminal is an important sign that skimming may have occurred.

It is strongly recommended that you:

- Record the following information about your terminals:
  - brand, model and serial number;
  - location where a particular terminal is kept in your area;
  - a description of all cables connected to the terminal;
  - details of any security stickers and where they are placed on the terminal.
- Give your staff forms to help them complete their daily checks.
- Ensure your staff check their terminal regularly, and that you check every terminal in your store periodically to ensure accuracy.

## 2. SECURE YOUR TERMINALS

Preferably, physically secure your terminals to a counter. If that is not possible, provide a secure place – out of sight and reach of customers – for staff to put the terminal if they need to leave the immediate area. An unattended terminal is an easy target for criminals. Protect your terminal like you would cash.

## 3. BEWARE OF HIDDEN CAMERAS

Be mindful that **criminals may use cameras** to record customers' PINs, so:

- Do not place objects that might hide a pinhole camera near any terminal.
- Ensure that any security cameras adequately cover the terminal area – but are not able to record the PIN entered by a customer.

## 4. ACT ON ANYTHING SUSPICIOUS

If any of your staff notice changes to a terminal or suspect a camera may have been used to record PINs:

- Double check all information.
- Disconnect and remove the terminal.
- Store the terminal in a secure location.
- Initiate your area's Payment Card Incident Response and Continuity Plan.

**Immediately report any concerns to University Information Security at abuse@umn.edu.**

## 5. VERIFY SERVICE VISITS

Your staff should direct all visits by technicians and other service contractors to you. **All visitors should be asked to present their security identification (ID).** If the visit was not booked, or the ID does not match arrangements, contact Accounts Receivable Services.

## 6. KNOW YOUR STAFF

Criminals are known to bribe or intimidate staff into helping them with skimming. To protect your staff and your business:

- Inform staff how to respond if they are approached by anyone suspicious.
- Watch for any unusual behavior among your staff.
- Conduct background checks on new staff.

## 7. PROVIDE STAFF TRAINING

Ensure your staff are informed and aware of how they can safeguard against skimming:

- Provide them with a copy of this brochure.
- Ensure a copy of the "Keep it Safe" brochure is posted next to the terminals.
- Regularly check that employees are following the practices recommended in this brochure and other resources.