Credit Card Security

- Only use an ATM (Automatic Teller Machine) in an environment where you feel comfortable.
- Be aware of your surroundings and of people that may be loitering near the ATM.
- Be prepared to make your transaction and have your card ready when you approach an ATM.
- Be careful that no one can see you enter your PIN at the ATM and stand directly in front of the ATM to minimise the chance of your transaction being watched.
- Don't leave your cash, card or anything else behind after you complete your transaction. Take your receipt with you or place it in the secure bin provided at the ATM.
- Do not count or display any money you receive from the ATM. Immediately put your money into your pocket or purse and count it later.
- If the card reader on an ATM is obstructed or has a device protruding from it, do not use the ATM and notify the financial institution of the problem.
- If anything about an ATM or other equipment appears unusual, do not use it. Fraudsters have been known to use fake equipment to steal cards or capture PIN details.
- When entering your PIN, ensure no one can see your actions. Be aware of the location of security cameras and mirrors that may allow others to observe you.

Shield your Pin with your hand when carrying out a transaction. This will help to prevent criminals from noting your number via a tiny camera over your head. Such a camera can be inserted into the shop ceiling with the aid of corrupt employees or coerced individuals. They then use a card cloned from details stolen from your card's magnetic strip to take advantage of the Pin.

As the chip and Pin system can sometimes make these cards difficult to use in the UK, fraudsters often send them to countries where the system has not been introduced, such as the US.

Do not let your card out of your sight when making a transaction. Portable skimming devices such the one shown below can be used to copy the information off your credit card.

Also check to see if there is anything unusual about the chip and Pin terminal. A second, false keypad can be fitted over the genuine one:

Portable skimming device

False keypad

What is an ATM skimming device?

An ATM skimming device is a physical attachment that has been illegally installed onto an ATM to covertly gather customer bank card details together with the corresponding security Personal Identification Number (PIN) to illegally attain funds

How do I identify an ATM skimming device?

An ATM Skimming device may stand out and look ‘out of place’. Some ATM skimming devices may be as small as the top of a pen. Many of these skimming devices can be electronically monitored by the criminal who may be in the vicinity of the ATM.

Photo 1: False slot fixed to the original card slot (same colour and sticker). Contains additional card reader to copy information and duplicate your card.

Photo 2: The side of the box facing the ATM screen has a reflective glassy hole. That’s a camera!