BEWARE OF SKIMMING FRAUD

Vigilance by consumers can help protect against credit card fraud.

Skimming has been described as one of the most significant problems facing the credit card industry, as it can happen anywhere a credit card is accepted. The best way for consumers to protect themselves from skimming is by paying attention to the details of credit card usage.

When a credit card is skimmed, data on the card, including the account number, is electronically transmitted or stored. The credit card information can then be encoded onto a lost, stolen, or counterfeit credit card and used anywhere in the world.

Since there are legitimate uses for many of the devices used to read or skim credit cards, paying attention to where you use your credit cards can also help prevent fraud. Examples of skimming instances include:

- A collusive store employee completes a valid sale, and then captures a second (unauthorized) swipe covertly on a portable device before returning the card to the cardholder.
- A skimming device is added to the front of an ATM or gas pump and captures the credit card information as the consumer attempts to use the machine.
- A skimming device is added inside an ATM or gas pump and captures information during a valid transaction. In many cases a covert camera is also set up to capture the card holder's personal identification (PIN) number.

To protect against these instances of skimming, the Secret Service advises consumers to pay attention to their cards at the point of sale.

- Ensure your credit card is swiped only once at a register.
- Conceal your PIN as you enter it into an ATM or credit card reader.

The U.S. Secret Service was originally founded in 1865 for the purpose of suppressing the counterfeiting of U.S. currency. Over the years it has grown into one of the premier law enforcement organizations charged with investigating financial crimes. The agency has taken a lead role in the emerging arena of cyber crime, establishing partnerships with the public and private sectors to address such issues as protection of critical infrastructure, Internet intrusions and associated fraud.

If you suspect you may be a possible victim of skimming or other financial fraud, contact local police and/or local U.S. Secret Service field office.