Credit Card Fraud Devices

INTRODUCTION

Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The goal could be to pay into another account that is under criminal control or to receive goods or services. Unauthorized credit card fraud occurs when the account holder does not give permission for the payment to proceed and a third party completes the transaction. Authorized credit card fraud occurs when the legitimate customer themselves processes payment to another account that is controlled by a criminal. Unauthorized individuals may use someone else's credit card information to make purchases, conduct other transactions, or open new accounts, which is referred to as credit card fraud. Account takeover fraud, new account fraud, cloned cards, and cards-not-present schemes are a few instances of credit card fraud. Phishing, information skimming, and information sharing by a user often without their knowledge lead to this unlawful access. There are various forms in which card information is stored. The card's primary account number (PAN), which is also often embossed or engraved, is stored on a magnetic stripe on the back in a machine-readable format. Although there may be other fields, the most typical ones are the cardholder's name, card number, expiration date, and verification CVV code. Some of these are legal tools employed for illegal activities. The mere possession of these devices is prohibited in several jurisdictions. As shown in figure 1, four broad categories can be used to group the devices:

- The magnetic data stripe on plastic cards contains information on credit cards, including the number, expiration date, and owner information (e.g., name, address).On credit cards, blank card material, driver's licences, and any other item with a magnetic data stripe and/or a chip, encoders affix false information.
- Users using three-track readers can decode and validate data from all three tracks of the credit card's magnetic data stripe. Account information is stored on tracks 1 and 2 of a magnetic data stripe in the US. The card issuer may save optional information on the cardholder in Track 3. Authorizers at the point of sale in retail establishments keep track of transactions and also check credit restrictions.

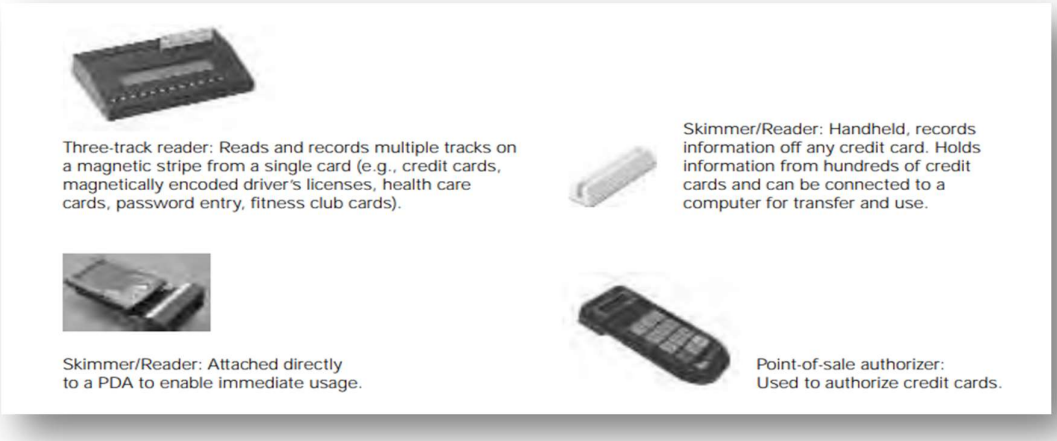

Figure 1 : Credit Card Fraud Devices

Value of the credit card fraud device

- Investigators should be aware of the following:
  - Use or possession of the device may be proof that a subject is engaged in credit card fraud, identity theft, or other fraudulent behaviour.
  - These devices data can be utilised to create timelines and historical activity records.

- Subjects are permitted to: –
  - While doing work-related duties at a retail location, possess a device and utilise it to collect customer data.
  - Possess a device to encrypt stolen or fraudulent information on counterfeit credit cards or other counterfeit papers with magnetic stripes. The offender may use the stolen or fraudulent information themselves or may sell the customer information to a third party to commit identity theft.

Identifying and obtaining the credit card fraud device

- Handheld credit card skimmers and encoders that resemble regular credit card readers are also available. To download data, they might be connected to a computer or PDA (e.g., credit card numbers and other account information).
- A skimmer could resemble a tiny, square gadget with a credit card swipe track that resembles a pager.
- Point-of-sale equipment can be found on, near, or on people using credit cards as well as on, near, or on computers. — Some legal gadgets might be utilised for illegal ones. For instance, the information from a visitor's credit card can be obtained using a hotel room key encoder. A blank credit card or another card with a magnetic stripe can then be programmed with this data.
- These gadgets might be made or are obtainable in stores.

Special investigative considerations and other factors

- Other storage media acquired during the investigation contained data pertaining to the device's use (e.g., information collected by a skimmer could be downloaded to a PDA or computer).
- A significant number of blank magnetic stripe cards might be a sign of fraud or other wrong doing. Any data on these cards should be examined with a credit card reader.

Scenario

A restaurant has been identified as the typical point of compromise for multiple clients' credit cards by a credit card company looking into fraudulent activities. The investigator witnesses one waiter utilising a small, black device to swipe credit card data while processing transactions while conducting the inquiry. Analysis of the skimmer reveals that it has hundreds of credit card numbers that have been stored.