Evolution in bank cards security, cardholder verification and its impact on fraud crimes

Zakaria Elsayed Abd Elhamid Abokabera
Expert of Forgery and Counterfeiting, Forensic medicine authority, Ministry of justice, Egypt

Abstract

A bank card (Credit, Debit, and Charged) is typically a plastic card issued by a bank to its clients that performs one or more of a variety of services that relate to giving the client access to funds, either from the clients' own bank account, or through a credit account. It can also be a smart card. Physically, a bank card will tell you the name of the card issuer on it, as well as the type and number. It will also have a magnetic stripe on the back encoding (various machines to read and access information). Security of a plastic card is an important factor to drive down fraud. This research exhibited the evolution of security in Credit, Debit cards starting from using magnetic-stripe, Chip and Pin, Biometric authentication, token payment, cardholder verification and its impact on fraud crimes.

Introduction

Security of a bank card is an important factor for organizations of card schemes. NFC, MIFARE have been there since the 1980s. In recent years, the research study has developed many types of bank card technology, such as magnetic stripe, smart card and smart card technology, also under the name of EMV chip technology. The research study has been the result of increased demand for a better card security system. Magnetic-stripe card

Magnetic-stripe card

A magnetic-stripe card is a type of physical card in which data is recorded on a band of magnetic material on the surface of a plastic card. Magnetic-stripe cards are used with readers manufactured using magnetic reading heads. Each stripe contains a magnetic tape encoded with a unique set of characteristics such as density and order. These characteristics allow the stripe to be read by more than one type of card reader. There are three tracks on magnetic-stripe cards, known as tracks 1, 2, and 3. Track 1 is usually encoded with the major worldwide network and often used for all three purposes: magnetic-stripe card readers, magnetic-stripe card readers, and contactless card readers, respectively. Each track is 360 millimeters long and contains 210 bytes of data. Track 1 contains the bank name, cardholder name, card number, and expiration date. Track 2 contains the magnetic-stripe card number, the track number, and a magnetic-stripe card validation code. Track 3 contains the magnetic-stripe card number, the track number, and a magnetic-stripe card validation code.

Chip and Pin

A Chip & Pin Card contains a small embedded microchip, which encrypts your account information, making it difficult to duplicate or access without the right key.

EMV

EMV is a globally standard for cards and debit payment cards based on chip card technology. EMV is used for credit cards and debit cards to enable cardholder verification and to reduce the risk of fraud.

Biometric authentication

Biometric authentication is a future of card, ATM and smartphone payment. Biometric authentication is a secure and reliable method of verifying a person’s identity. It can be used for a variety of applications, including access control, biometric authentication. There are several types of biometric authentication, such as fingerprint, iris recognition, voice recognition, and facial recognition.

NFC

Near Field Communication (NFC) is a global standard for contactless mobile payments. NFC enables mobile devices to communicate wirelessly with each other and with contactless payment terminals. NFC has two main components: a reader and a mobile device. The reader is a device that can read and write data to the NFC chip in the mobile device. The mobile device is a device that can be read by the reader. NFC-enabled mobile devices can be used for contactless payments, such as mobile wallets and electronic payment systems.

Methods of payment

1. Magnetic-stripe card
2. Chip and Pin
3. NFC
4. Biometric authentication

Results

- There are types of card fraud: skimming, counterfeiting, card cloning, phishing, CVC2 (Card Verification Code 2).
- The chart illustrates the total value of card fraud-suspecting cards issued in EMV (Single Run Payment Amounts) per annum from 2009 to 2013.
- The percentage of total card fraud increased to 32% in 2013 compared to 2009.
- There are now over 3.4 billion EMV payment cards in circulation, which is an increase of 43% on 2013.
- Chip card transactions increased by 29% compared to 2013.
- The number of contactless payments has increased significantly, with over 1 billion contactless payments in 2013.
- The rate of fraud has decreased by 28% for Chip cards and 30% for EMV cards.
- The use of biometric authentication, such as fingerprint, face recognition, and palm vein recognition, has increased significantly.
- The use of smartphone payments has increased significantly, with over 1 billion smartphone payments in 2013.
- The rate of fraud has decreased by 28% for Chip cards and 30% for EMV cards.

Conclusions

- Using magnetic-stripe cards in bank card is weak security element because it is easily skimmed and counterfeited as it allows easy access to the card's balance.
- Using NFC technology is more secure and reliable compared to magnetic-stripe cards.
- Using biometric authentication is the future of card, ATM and smartphone payment.

References

- Zakaria Elsayed Abd Elhamid Abokabera (Zakaria Abokabera)

Bibliography

Zakaria Elsayed Abd Elhamid Abokabera
Expert of Forgery and Counterfeiting, Forensic Medicine Authority, Ministry of Justice, Egypt

Email: zakariapharm@gmail.com
Mobile/WhatsApp: +20115699075