Analysis of security risks to network transactions

Pronkin Leonid,
Pudalev Timofey,
Holmatov Farruh,
Yavnoshanov Dmitriy students of Siberian Federal University,
Krasnoyarsk, Russia, E-mail: pudalev@gmail.com

The relevance of the topic of this article is the need for disclosure of the types of frauds committed with plastic Bank cards and suggest methods for their protection and information stored in it for issuers and holders of plastic Bank cards.

Keywords: remote transactions, Bank plastic card, safety plastic Bank cards, fraud.

Under card fraud refers to intentional fraudulent actions of some parties, based on the use of banking cards and aimed at the unauthorized acquisition of funds placed on the card accounts of the cardholders or due to merchants for transactions on the cards.
Card fraud is often referred to as fraud (from the English. Froud-fraud, deception)

Fraud can be divided into two groups: fraud on the part of card issuance and fraud on the part of their service. The first group includes the fraud associated with unauthorized use of the card Issuer (stolen/lost cards, counterfeit cards, lost cards, received by the Bank not the honest way resulting from the use of stolen credentials / documents "reliable" person, etc.,) the second group includes fraud, the initiator of which was a commercial enterprise (fake/ distorted slips, re-input operation, etc.) In the last 10 years, the average loss of the Bank from operations on plastic cards are 7-12 cents per $100 of turnover on cards (7-12 pb).

As noted above, fraud is divided into two groups: fraud on the part of card issuance and fraud on the part of service cards. The main types of the first group:

- stolen/lost card (Lost/Stolen Cards or L/S);

- lost map (Not Received Items, NRI);

- fake card (Counterfeit);

- card Not Present fraud (CNP fraud);

- card received by fraudsters on stolen documents/personal data (ID Theft).

Stolen/lost card.

The oldest and most natural form of fraud people have lost, are losing, and will lose the card. Sometimes the card stolen. In Russia, according to the National Agency fin. studies (NAFI), approximately 19.8% of cardholders ever they were lost. Until the discovery of the loss and lock in the system passes the time and used by the attackers, in whose hands was the map.
Before informing the Bank about the loss of the card which blocks the card Issuer, the responsibility for this type of fraud usually borne by the card holder.

Not received the card.

Cards stolen during the transfer from the Bank to the client. All responsibility for the fraud in this case lies with the Issuer. According to the leading payment systems on this type of fraud accounts for 1-3% of the total fraud. In particular, according to MasterCard for the second quarter of 2013 on lost cards accounted for 1.1% of all card fraud in Europe and of 2.33% in the world.

Fake cards.

The attackers made a fake card personalized on the basis of previously stolen details real card (usually stolen from the magnetic stripe of the card) and do a fake operation, posing as a real map.

Fake cards began with a technology cut card numbers and shifted in their seats on the panel of the card. Occurrence and distribution of electronic terminals main method counterfeit cards have been skimming (skimming)- copy data from the magnetic strip of a real card. The copied data is later transferred to another map that criminals are made on the blanks cards acquired in different ways (use bonus cards to various retailers, real Bank card with encoded magnetic stripe, white plastic, painted on the printer, blank, stolen, factories and banks.

The real-card attackers are using:

- unscrupulous shop staff, who quietly for card holders copies the contents of the magnetic stripe card using a special device (skimmer) with reader magnetic stripe and is able to store information about several dozens of cards;

- ATM skimming (waybill is used keyboard/miniature video camera or installed software ATM malicious program that saves data from the magnetic strip and values PIN)

- skimming at POS terminals;

- steal data from the database processing centers and commercial enterprises;

- interception of data during transmission via the communication channels
viral attacks in order to steal personal data (Trojans, worms);

- phishing and wishing used by hackers to the collecting Bank customers ' personal information.

In connection with the migration to chip evident more rapid growth in the use of counterfeit cards (especially European cards at ATMs in comparison with POS-terminals. Considering the fact that many countries migrate program Chip&PIN was easier to copy data from the magnetic strip and PIN and then using these data to issue cards on the white plastic.

Card Not Present fraud.

There are three main types of CNP transactions : Mail Order/Telephone Order (MO/TO) transactions, transactions, e-Commerce (EC) and recurrent payments (card holder concludes with trading point agreement on a regular periodic direct debit of funds from its account for receiving from a trade point services using a plastic card).

In the operation of the EC accounts for about 60% of the total CNP fraud, MO/to transaction - 30% on recurring payments remaining 10%. The growth of EC in the world at the beginning of the new Millennium is about 25% per year, in Europe -40% per year. It is expected that by 2015 the volume of B2C in the world will reach 450 billion euros.

To commit fraud in the case of CNP transactions is sufficient to know the most simple card details-card number, expiration date, and the value of the CVC2/CVV2. Therefore, all CNP transactions must be done in real time, and the responsibility for fraud on such transactions payment system lay on its banks. The exception is when banks and their online store use secure Protocol EC, known as 3D Secure and used in the leading payment systems under the brands of MasterCard SecureCode and Verified by VISA.

Card received on stolen documents or personal data (ID Theft).

To implement this type of fraud is mainly used two schemes of fraud: fraudulent applications and interception account.

Fraudulent applications: the scammer is using someone else's ID (found/stolen/forged) for filing an

application for obtaining a credit card with indication of the address to which the card can be easily and safely obtained.

Interception account: attacker information about the details of the card/account, for example, found in his Bank statements of the cardholder, then call the Bank and report the change of address, and later requests a new map with the delivery of her "new" address.

A large value fraud also has the job of servicing banks with commercial enterprises.

In the conclusion of our article we would like to note that new technologies for protection of Bank plastic card and the remote transaction implemented in the fight against criminals, will evolve with each new case new fraud, payment systems. Banks and also attackers will be involved in the development of information security of the Bank cards as this process will evolve every day.

Bibliography

1. Bank smart cards – Goldovskiy I., "Alpina Publishers", 2010.

2. Nilson Report January 2015/Issue 1055 HSN Consultants, Inc.2015 The Nilsen Report