International Journal of Information Management 32 (2012) 501–503

Contents lists available at SciVerse ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Viewpoint

Credit card incidents and control systems

Jose M. Pavía[a,*], Ernesto J. Veres-Ferrer[a], Gabriel Foix-Escura[b]

[a] Department of Applied Economics, Universitat de Valencia, Spain
[b] Risk Department, Banco de Valencia, Spain

ARTICLE INFO

Article history:
Available online 21 April 2012

Keywords:
Risk management
Card fraud
Phishing
Skimming
Carding

ABSTRACT

Credit and debit cards have spread and skyrocketed all around the world to become the most popular means of payments in many countries. Despite their enormous popularity, cards are not free of risk. Technology development and e-commerce have exponentially increased internal credit card incidents. This paper identifies and quantifies the different types of credit card fraud and puts into question the effectiveness of the role assigned to cardholders in its detection.

1. Introduction

Technological developments have changed the way we view money, especially with relation to its use as a method of payment. It has evolved from being considered a physical active (gold, coins or notes) to the idea of money being a figure in an account. This change in framework, that has modified the way monetary policy is designed on a large scale, has influenced the behaviour of small businesses. In the last thirty years, the use of credit/debit cards has spread and skyrocketed all around the globe, gradually becoming the most popular and most efficient means of payments in many countries.

As examples, there were almost 800 million cards in circulation in 2010 in Japan alone, the total amount of card payments (excluding e-money cards) made in the Eurozone surpassed one trillion of euros in 2010, the total US revolving debt (98 percent of which is made up of credit card debt) reached $812.1 billion in January 2012, and the average number of cards per inhabitant in UK was about 2.33 in 2010 (Banco de España, 2011; Euromonitor International, 2012; European Central Bank, 2012; Federal Reserve, 2012). In fact, according to the American Bankers Association, "*it is estimated that there are 10,000 payment card transactions made every second around the world*" (Schulz & Woosley, 2009).

In spite of their enormous popularity, plastic cards are not free of risk. Credit card issuers as much as card owners are aware of the possible problems that can arise from an incident involving a card. For instance, the May-2009 Unisys Security index pointed out credit and debit card fraud as the first concern of Americans, superseding fears of terrorism. Further, according to a report by VISA in 2010, worldwide card fraud accounts for around 0.055% of the sum of all credit card payments and likewise, according to issuers and police, security measure costs (including investment in technological developments, security and the fight against fraud) are equivalent to 0.06% of the value of all card transactions. Since 1958, when the first widely accepted plastic charge card was issued by American Express, issuers have been virtually running a race without end in the fight against fraud.

If, traditionally, early detection of a card incident was important because of its extensive use as means of payment in high street shops, the rapid expansion of e-commerce and online banking has made it essential (see, e.g., Bang, Lee, Bae, & Ahn, in press). Both the issuer and the cardholder are interested in an early alert and prevention of incorrect use of the card to avoid the unintended economic consequences that could result (Chung & Suh, 2009).

The range of the profile of the incidents is wide, from external incidents, such as robbery, theft or mislaying a card, to internal incidents, such as duplication, cloning or piracy of passwords, via phishing or skimming. With the development of technology and e-commerce and the growing use of the Internet, the increase of internal incidents has been exponential.

2. Cards and fraud

Stolen or lost cards, which account for around 12% of all incidents, are the traditional methods leading to fraudulent use of a card. This practice, however, is declining due to the effectiveness of the basic countermeasures. In face-to-face transactions, the identification of the cardholder by way of their signature and the use of

* Corresponding author at: Facultad de Economía, Area de Métodos Cuantitativos, Universidad de Valencia, Campus Els Tarongers, 46022 Valencia, Spain.
E-mail addresses: pavia@uv.es (J.M. Pavía), Ernesto.Veres@uv.es (E.J. Veres-Ferrer), gabriel.foix@bancodevalencia.es (G. Foix-Escura).

0268-4012/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijinfomgt.2012.03.003

Chip and PIN cards are procedures that are showing as quite effective. Furthermore, the cardholder can actively cooperate from the start against this type of fraud by being conscious of the theft or robbery and thereby setting in motion the alert procedures.

Phishing, which in 2010 represented around 22% of all incidents, is a type of fraud that has appeared with the popularity of e-banking and e-commerce. The most common occurrence of phishing consists in the substitution of the web interface of a legal transaction where the clients introduce their card details and their Personal Identification Number (PIN). Afterwards, the stolen information can be used in an electronic transaction or directly to clone credit cards. In this type of fraud the cardholder initially has limited possibility of detecting the fraud other than by being alert to any "odd" or unusual changes in the interface when making an internet payment. It is normal, however, for the phishing to be preceded by e-mails with enticing advertising in order to attract the greatest possible number of clients to the fraudulent website. Hence, in addition to countermeasures such as improving the web security of the banks, the use of systems with variable passwords (using, for example, coordinate cards) or the verification of websites as "safe trade" by the card provider, information and training campaigns addressed to cardholders would also be effective.

Application fraud is a minor type of fraud (representing less than 2%) and is based on stealing an identity. Once the card has been achieved, it is quickly used up to its maximum limit and then disposed of. This type of fraud is the full responsibility of the card issuers. The countermeasure seems obvious; do not give cards to unknowns. One has to bear in mind, however, that many cards are conceded through an impersonal commercial transaction and in busy areas such as train stations, airports or shopping centres.

Falsification accounts for the greatest type of card fraud (62%), included in which are the different fraudulent ways of obtaining all the personal details needed to achieve a legal card which afterwards can be duplicated or cloned and used without the permission of the owner. This information is usually obtained from automatic cashpoints or from points-of-sale terminals (POS).

At cashpoints, a micro-camera was traditionally placed over the keyboard which enabled the card information to be read: name, number and expiry date and even the PIN that the cardholder enters. This practice, however, has been disabled with the simple introduction of an additional code (CVC) found on the reverse of the card.

The counterfeit networks, however, have evolved and now the latest method of falsification is known as skimming. Skimming consists of placing an electronic device (in the cashpoint or at the POS) that reads the magnetic band of the card and copies all the data during the transaction. The skimming devices are homemade and no two are alike. The "modus operandi" of these bands of counterfeiters consists in studying closely the device to be disrupted, installing the skimming device at an opportune moment (or with the help of an employee as accomplice) and leaving it to function over time. Once the band achieves the number of cloned cards it desires, the device is considered to be paid off, all the cards are then cloned at the same time and these are distributed quickly in different markets. The business of these bands of counterfeiters focuses on the sale of counterfeit cards, not in their use. The band distributes cards that only have a certain purchase limit and last only a few days—the amount of time estimated that it takes the lawful cardholder to be aware that his/her card has been cloned.

A priori, this "modus operandi" obstructs the work of the police and the alert mechanisms, as months can pass from when the card is copied till it is used fraudulently. Indeed, due to the high number of cards that are cloned in each outbreak (e.g., 1700 cards were cloned in only one cashpoint in Murcia, Spain; Cózar Barreiro, 2010) and their wide distribution (e.g., according to García Sánchez, 2010, between 2005 and 2010, 68% of frauds committed with Spanish cards were carried out abroad; the US, Canada, Australia, the UK and France being the countries where the greatest losses were registered), it is not easy to find a common link in all of them.

Although, obviously, the countermeasures to combat falsifications are also applied in the technological devices used in the transaction process (e.g., by increasing the standards of security in the automatic cashpoints, including anti-intrusion software in the POS or by using Chip and PIN cards that have, as well as an additional verification point, more complex cryptography), the countermeasures that are being introduced recently follow the line of favouring the participation of the cardholder in the security and of combining this with the use of other devices independent of the payment system. This is the case with the notification of a purchase made by mobile phone via an SMS. For example, by imposing the restriction that, for certain types of purchases or amounts, the cardholder should be the person who must accept the charge by way of their mobile phone or by alerting the user (also by SMS) when an unexpected transaction occurs, with the normal behaviour of the cardholder previously determined using, for example, neural network systems (see, e.g., Quah & Sriganesh, 2008).

The fight against fraud, however, is never-ending. As soon as one form of counterfeiting is annulled, another one is created. The most advanced system of counterfeiting is known as carding in which the card is neither copied nor cloned but used directly to create a new one. The counterfeiters know the algorithms for creating a new card and by using an existing card they can create new cards just as if they were VISA or Mastercard, etc. This is a completely new system which neither the cardholder nor the issuer can do anything about as it is done completely behind their backs.

3. The role of the cardholder in an alarm system

Excluding the latest new fraud system where the card issuers are obliged to develop new procedures capable of tackling this new threat, it is apparent that the majority of the countermeasures that could be most effective in the fight against fraud rest with the cardholder. The question that we should therefore ask ourselves is up to what point the provider can confide in the cardholders when creating a credit card control system.

As is well-known, a control system is defined as the set of actions, functions, behaviours and responsibilities that permit, through their interaction, the detection of the occurrence of a specific at-risk situation. The goal of any control system is to be able to react to any eventuality, implementing the actions deemed appropriate (Alhawari, Karadsheh, Talet, & Mansour, 2012). Any warning system, therefore, aims to achieve real-time detection and attempts to reduce the delay in the response by using clear and manageable indicators that allow the alarm systems to react quickly. The delay in the detection of the event and the proper identification of the risks (real or potential) are therefore key indicators in the design of any effective warning system. In particular, for efficient operation, control systems are characterised by being understandable, rapid, flexible and economical (Alberts & Dorofee, 2004; Richard, Fremont, & James, 1973).

Thus, in order to consider the holders of credit cards and debit cards issued by a financial institution as a warning system to detect any incident relating to their cards and to study whether they make an efficient control system, the focus would be on the speed of the response. The omission in considering the other three requirements is acceptable as they are naturally satisfied in this case. The process is well understood by the entity and also by the cardholder, in as much as the latter is aware of the existence of possible damages resulting from an incident, even if s/he may not know exactly what the specific consequences are (Lopez-Nicolas & Molina-Castillo, 2008). Flexibility is guaranteed by the capacity of almost all