Credit Card Fraud Types in E-Commerce

Whitepaper

Web Shield Limited | 207 Regent Street, 3rd Floor | W1B 3HH London
www.webshieldltd.com | compliance@webshieldltd.com | Phone +44 (0) 207 6085675

Electronic commerce is an online business where the selling and buying of services or products are done over electronic systems, including the Internet and various computer networks. It is a strategy for a company to enter into the market even if it does not physically exist, hence increased productivity (Chaudhury, Abijit and Kuilboer, 2012). Online fraud is an illegal activity whereby the perpetrator schemes a plan to use internet elements to deny a person of estate, property, or right by concealing some or giving misleading information (F Jonathan, 2006). Such fraud occurs in message boards, chat rooms, Web sites and via email in forms of fraudulent transactions and deceitful solicitations. As rising numbers of consumers and businesses rely on electronic communication in order to conduct transactions; criminal activities utilizing the same media are similarly increasing (Chaudhury, Abijit and Kuilboer, 2012). Fraudulent schemes that are conducted over the Internet are difficult to track and prosecute. They also cost companies and individuals millions of dollars annually (G Mark, 2008). In accordance with an investigation conducted by the Federal Bureau (FBI), major online frauds are categorized into auction, retail fraud, and identity theft as well as securities fraud among others (Abijit, Kuilboer and Jean-Pierre, 2012). This paper focuses on several online fraud types in e-commerce that are conducted by using a credit card. The areas discussed in the paper include friendly fraud by the card holder, fraud with stolen credit cards and the fraud conducted by the online merchant that accepts cards.

Credit card fraud arises from illegal access to data including one's account number or a physical theft of the card. It is conducted in 3 ways: friendly credit card fraud by a card owner, fraud conducted by a merchant that accepts the card as well as fraud conducted by the issuer of the card. The increase in online credit card use has compromised many accounts making lapses in database costly (M Rogers, 2012). Although stolen credit cards can quickly be reported by the cardholder, a compromised account is likely to be hijacked for a long time by thieves before any fraud is conducted; hence it makes it

difficult to determine where the compromise comes from. However, cardholders can combat this crime by frequently confirming the security of their accounts.

The internet and the mail are major media for crime against merchants that sell and ship merchandise, and it affects real internet and mail-order merchants. In case the card is not physically present (card not present, also CNP) the merchant will have to depend on the cardholder .The said holder could be a fraudster who presents information indirectly via telephone, mail or online. Albeit there are ways to deal with this it presents a much higher risk than physical presence of a person, and indeed issuers of credit cards charge highly for CNP than when the card is present (K Phillip, 2009). It is therefore difficult to verify whether the legitimate cardholder is responsible for authorizing the supposed purchase. Shipping companies guarantee delivery to a specific location, but do not necessarily check identification because they are not directly involved in processing payments for the goods. Hence making this type of fraud difficult to trace and identify.

Credit card fraud also includes a majority of scams such as overcharging someone for items that they have purchased legitimately and charging extra fees for unauthorized credit cards. A general example would be pornographic sites that advertise free access, yet need credit cards" for purposes of verifying the age only (S Pat, 2011). The scammers thus, use the information on the credit cards to create fraudulent charges against the cardholder. A consumer is more legally protected when he or she uses a credit than a debit card. Customers should review their credit card statements on a monthly basis to ensure their accuracy. If there appears to be any misappropriations such as overcharging or, unauthorized charge appearing on one's account, it is necessary to contact one's credit card issuer promptly for any necessary corrective action. Consumers notice that immediately these scammers get their credit card information, the card may be cancelled but fraudulent charge attempts would still be made (Jean Pierre, 2012).In such cases, consumer and credit protection laws exist to protect against

merchandise for which payment has been completed, and are not delivered (Chaudhury, Abijit and Kuilboer, 2012). Albeit the loss is absorbed by the credit card business, these costs are passed on to customers as higher interest fees and rates.

As rising numbers of consumers and businesses rely on electronic communication in order to conduct transactions; criminal activities utilizing the same media are similarly increasing Chaudhury (Abijit, Kuilboer and Jean-Pierre, 2012). Fraudulent schemes that are conducted over the Internet are difficult to track and prosecute. They also cost companies and individuals millions of dollars annually. According to a report compiled by the Federal Bureau Investigation (FBI) and the National Centre for White Collar Crime in 2001, major online are categorised into auction, retail fraud, and identity theft as well as security's fraud among others (Abijit, Kuilboer and Jean-Pierre, 2012). Internet auction fraud is one the most reported offenses consisting of 35-45% complaints. It usually happens when advertisement of merchandise is conducted by people on auction sites but fail to deliver it or deliver an item with less value as opposed to the one described during the auction. A number of crimes are committed through auction sites and this call for business men to be careful with their transactions (Abijit, Kuilboer and Jean-Pierre, 2012). For example, a seller should be aware of people who send more money than the cost of the item then ask for a refund, those who want to overpay for items, as well as request items to be shipped to another country even though the purchaser is in a different country.

Criminals apply information on stolen credit cards for online purchase of goods which should be shipped to the actual cardholder. After the item is transferred, the fraudster receives tracking information through email (H Phillippe, 2013). They then contact the legitimate cardholder and identify themselves falsely as the merchant that transferred the goods, saying that the merchandise was mistakenly shipped and requests for permission to collect it as soon as it is delivered (Abijit, Kuilboer

and Jean-Pierre, 2012). The criminal then organizes the collection with a different shipment business. The victim may not notice that a different shipping business is taking the product because the shipping company does not also know that it has taken part in a fraudulent operation (L Kenneth, 2014). The cardholder may at a later protest to charges existing on his account, hence creating to the shipping company which is also unaware of the proceedings.

Moreover, when a cardholder purchases something from a supposed vendor and expects his card to only be charged once, a vendor may unnecessarily charge an amount that is three times more than the usual amount (Chaudhury, Abijit and Kuilboer, 2012). The vendor then hoaxes the cardholder into becoming a member of the vendors merchandise and that his membership would be renewed on a periodic basis (Kessler M, 2003). According to the vendor the renewal cannot happen in case the customer notifies him of a cancellation procedure contained in the membership agreement which the consumer agreed to while he conducted the initial purchase. Since the periodic charges are infrequent, unexpected, and small, they go unnoticed (N Daniel, 2006). When a cardholder makes a complaint to a bank that did not authorize the transaction, the bank will give a notice to the vendor who will defend himself saying that the consumer did not cancel the membership agreement that he allegedly accepted. Most card holders do not know what the cancellation procedure entails and the vendor can only reveal it to new customers to take advantage of them (H. Phillipe, 2013). However, the bank won't reverse the charges, but will instead offer to call off the credit card then reissue it now with a unique expiration date or account number.

Lastly, identity theft is another form of fraud that uses software with access to the Internet to defraud victims or take advantage of them, such as by stealing private information which can lead to theft. Identity theft fraud thus comes about as a result of using other people's credentials illegally and claiming identity for those credentials (F Jonathan, 2006). A common form of identity fraud is

distribution of illegitimate security software. Internet services have been used to solicit fraudulent transactions to prospective victims, using identity theft as a catalyst, for example, in transmitting the proceedings of these operations to financial institutions and to others that are also connected with the crime (K Phillip, 2009). Skimming is yet another type of credit card fraud. It refers to theft of information on credit cards to be used in seemingly legitimate transactions (G Mark, 2008). The thief procures a victim's number using simple methods for instance photocopying receipts and also more advanced methods including the use of a skimmer that swipe and stores a number of card numbers that are used in fraudulent activities. Skimming is majorly done in places such as restaurants and fuel stations. It is difficult to detect.

In conclusion, online fraud takes many forms in online business transactions. The most common include online auction and retail fraud, fraud conducted with stolen credit cards and friendly fraud made by the cardholder himself as well as those conducted by online merchants who accept the credit cards. Others include identity theft, cheque, overpayment and advance fee frauds. All these are generalized under computer frauds. They reduce customer trust and loyalty on e-commerce. However, if frauds are dealt with appropriately, the efficiency and effectiveness of online business is improved.

If you are interested on how your organization can protect your merchant portfolio in regard of fraudulent merchants, please get in touch with us directly:

Web Shield Limited

Regent Street 207, 3rd Floor

W1B 3HH London, UK

compliance@webshieldltd.com

www.webshieldltd.com

References

Chaudhury, Abijit; Kuilboer, Jean-Pierre (2012). *e-Business and e-Commerce Infrastructure*. McGraw-Hill. ISBN 0-07-247875-6

Frieden, Jonathan D.; Roche, Sean Patrick (2006). "E-Commerce: Legal Issues of the Online Retailer in Virginia" (PDF). *Richmond Journal of Law and Technology* 13 (2).

Graham, Mark (2008). "Warped Geographies of Development: The Internet and Theories of Economic Development" (PDF). *Geography Compass* 2 (3): 771..

Humeau, Philippe; Jung, Matthieu (2013). *In depth benchmark of 12 ecommerce solutions* (PDF).

Kessler, M (2003), "More shoppers proceed to checkout online", *USA today*,

Kotler, Philip (2009). *Marketing Management*. Pearson: Prentice-Hall. ISBN 978-81-317-1683-0

Laudon, Kenneth C.; Guercio Traver, Carol (2014). *E-commerce. business. technology. society. 10th edition*. Pearson. ISBN 978-013-302444-9.

Miller, Roger (2012). *The Legal and E-Commerce Environment Today* (hardcover ed.). Thomson Learning. ISBN 0-324-06188-9. 741 pp.

Nissanoff, Daniel (2006). *Future Shop: How the New Auction Culture Will Revolutionize the Way We Buy, Sell and Get the Things We Really Want* (hardcover ed.). The Penguin Press. ISBN 1-59420-077-7. 246 pp.

Seybold, Pat (2011). *Customers.com*. Crown Business Books (Random House). ISBN 0-609- 60772-3.