E-commerce fraud prevention

Business

Introduction The fact that e-commerce is becoming the dominant form of making business cannot be denied. The rapid expansion of the Internet facilitates the development of the new forms of e-business and e-commerce applications, making products and services more available and accessible to the customers worldwide. Obviously, the dramatic transformation of e-commerce into a routine activity would have been impossible without the creation of the application that would never exist in the physical world. Today, entrepreneurs and businesses online have a unique opportunity to access and use a variety of e-commerce applications, which make their businesses more efficient and help them to meet the most sophisticated customer needs. However, supply chain management solutions would not suffice, to bring e-commerce to the current point of evolution: today, businesses and entrepreneurs online can use a variety of other applications, including e-tailing and procurement. Problem Statement There are still some barriers that are to be overcome in order to make e-commerce more efficient.

The first problem is connected with the danger of being hacked. There are many computer genius in the whole world who can easily hack any site and then to insert a bug there. The consequences are the following: the site has to be relocated and therefore all the clientele is lost. Everything is to be started from the beginning. Another disadvantage is that a big percentage of orders are forgery. It happens because some teenagers want to joke, or because a customer occasionally gives incorrect data.

Then a vendor spends for delivery in vain. And the last disadvantage is that individual approach is hardly possible within e-commerce. Any individual approach needs understanding, being flexible and needs to be able to react when the environment changes. All of this is impossible to carry out with a computer, only a live communication can bring necessary results. As mentioned above e-commerce has negative sides, still customers are even endangered when shopping on-line.

The first problem is that a customer is always asked to fill his/her private information. This information can be hacked or misused from the Internet space. The next problem is that a customer has only a visual image of a product but he cannot touch it, turn it and try it. This is usually true when speaking about clothes and footwear. Such items are better to buy with the face-to-face contact.

And the next disadvantage is that sometimes a customer has to wait for several weeks to get his product. Economic crisis in the world exerts a negative influence on the modern society. Even during the period of recession, people are looking for different ways of earning money. Unfortunately, these intentions are not always legal ones. Unfortunately, the growth and development of e-commerce resulted in the growth and expansion of fraud in the Internet. In order to commit a fraudulent transaction, it is enough to know the system of a credit card’s work.

Merchants on the web have their own filters tracing fraudulent actions of potential on-line criminals. Nevertheless, fraud protecting system should be controlled by a merchant. The main functions of such kind of system are to: complete the lists of good and bad customers; create processing control activities; restrict access of unwanted IP addresses banning or zip codes and many other parameters (Talbott, 2011). There are a lot of users, who are involved in criminal activities on the web. It should be noted that web merchants are at a great risk nowadays. It is necessary to take into account potentially hazardou signs for e-merchants and recommend possible safeguarding practices to them.

On-line Fraud Identification There are multiple steps to be taken in order to prevent fraud. First of all, it is relevant to identify it. A great number of orders, occurring from one user ID or a credit card number can be considered as the first red flag for web merchants. The second reason to be on alert is to see the street address, which can be invented by the customer. Therefore, it is relevant to useGooglemap to investigate what kind of addresses, whether invented or not, are indicated by customers (Talbott, 2011). Moreover, in case the customer indicates anonymous email account, then a merchant may think about a potential fraud. The merchants should avoid different kinds of fraud. First of all, these are card-no-present fraud, when the customer indicates the number of a non-existent card. Gift cards are often used by fraudsters to make huge purchases online. Moreover, the fraudster may use information from a stolen debit or credit card.

The e-commerce industry is connected with fraud rings. It is difficult for merchants to trace fraudsters. Mobile commerce presents another challenge for merchants. Merchants are challenged by new threats and fraudsters know this fact. Costs of FraudFraudulent order values have higher price, which is $250 in comparison with $150 for valid orders. Manual review is more complex than automated review and it requires more money than it was supposed earlier.

Crimes committed on the internet are 92%; payment cards and services lead to crimes commitment (90%). Visa registers more than 350 million cards. There is a need to protect card payments and e-commerce transactions are easily identified. Online merchants are enrolled in MasterCard’s Secure Code program saying that: “ 2, 775 issuers, 202 acquirers, 23, 000 merchants and 10. 5 million cardholders worldwide are using Secure Code” (eCommerce Fraud Losses Projected to Grow to $3.

6 Billion in 2008). 176, 000 of internet fraud were fixed in 2005. Nowadays this percentage is increasing. It is possible to claim about the growth of fraud during the period of crisis and recession. E-Commerce and E-Fraud It is necessary and very hard for any company to prevent fraud in case of digital goods (software, music and video) delivery, because it occurs in real time and it is hard for merchants to identify fraud.

It is possible to re-screen the order for potential fraud identification. In accordance with recent data: “ If upon further investigation the order is found to be fraudulent, the card should be credited back for the goods that were purchased. This protects the victim from the charge and the company from eventual chargeback” (Eisen, 2009). Fraudulent orders should be identified and a potential chargeback for the company should be introduced. The e-commerce is operating using a covert device ID; the risk engines are operating with the use of the environment and connect analysis tools for adding complementary cases of fraud (Eisen, 2009).

Another relevant solution is to take into account ID technologies, which are implementing digital fingerprints of the devices. For example, the company determines a transaction and it can identify 85% of potentially fraudulent transactions and the important role is played by ID technologies. In accordance with the modern data: “ the result: criminals will unlawfully carry off $3. 6 billion in goods and services this year-up from $3. 1 billion in 2006” (eCommerce Fraud Losses Projected to Grow to $3.

6 Billion in 2008). Moreover, a kind of fraud can be identified by the human intelligence. Thus, the companies have an opportunity to penetrate into the depths of internet technologies and find out the secrets of monetary gaining from fraudulent practices. In order merchants could trace a Cyber Thief it is relevant to identify a potential fraud. For example, those orders, which occurred late at night, are believed to be recognizable signs of a potential fraud.

When the orders are placed from another country, this fact may be too suspicious as well. There is a need to identify a fraudulent e-mail address, because it is a wide-spread practice nowadays to post the orders from unknown or anonymous e-mail addresses. The cost of express shipping should be also taken into account by e-commerce merchants. In case a fraudster makes the order, he will not take into account the real price of shipping and he may pay even more for shipping than for an order itself. When the large quantities of one product are ordered by the fraudster, he may not take this fact into account as well. Therefore, merchants should pay attention to the fact, when the same order is requested in a huge quantity.

Solution: Safeguarding Practices Therefore, it is evident that modern fraudsters can perform their criminal online actions in case a merchant is unaware of the aforementioned preventive factors. There are some safeguarding steps to be taken by merchants to avoid fraud. First of all, there is a need to develop “ held orders” department, where it is possible to review the orders manually (Bustos, 2011). An important role is played by the “ in-house databases”, where fraudulent orders can be traced in accordance with the address. Chain calls developed among merchants, operating in the same sphere, are very important as well, because in such a way it is possible to share fraudulent addresses or the names of fraudsters.

Another relevant step is to contact the Credit Issuing Bank (CIB) for them to confirm the name of the credit card’s user. Another step is to document the customer’s phone calls. Thus, it is an option to create a chain of customer’s phone calls and possibility to trace their fraudulent actions if any. Cyber shoplifting notices should be also taken into consideration by e-merchants as well. It should be noted, that as the Internet and online business is evolving, so do various forms of e-commerce applications.

Today, the so-called recommender e-commerce applications are turning into the dominant way of bringing customers and businesses closer to each other. Recommender applications are those that work to suggest products to clients and give them with the information needed to make a purchasing decision. The criteria used to recommend products and services vary, as well as the specific forms of recommendation – from personalized product information to community critique. Conclusion It would be fair to assume that the development of recommender applications in e-commerce mark the new stage in the development of online businesses worldwide. In order to protect businesses from on-line fraud, it is relevant for e-merchants to refer to the environment of the potential customers, their personal data, addresses, contact phone numbers et cetera. Moreover, there is an opportunity to implement various digital technologies to prevent e-commerce fraud.

In any case, there is a great risk for modern e-commerce to be cheated. Nevertheless, every merchant individually should make their own lists of invented e-mail addresses or post addresses and share this data on-line with other business partners. A chain-safeguarding is a perfect option to deal with the modern e-commerce fraud.