https://doi.org/10.48009/1_iis_2010_280-285

E-BUSINESSES AT RISK: A LOOK AT THE IMPACT AND CONTROL OF E-BUSINESS FRAUD

Patricia Lake, Western Illinois University, Macomb, IL, PM-Lake@wiu.edu
Susan Behling, Western Illinois University, Macomb, IL , SD-Behling@wiu.edu

==========

ABSTRACT

Fraudsters have found ways to breach e-business inventory controls, ordering systems, distribution systems, and payment systems. System manipulation, stolen credit cards, and friendly fraud are discussed, along with their impact on e-business operations and profitability. A number of preventative measures are introduced, as well as actual cases of e-business fraud. The question is asked and briefly discussed: Is the educational system meeting the needs of e-business?

Keywords: E-Business; E-Business Fraud; E-Business Challenges

INTRODUCTION

E-business is a relatively new and fast paced approach to meeting consumer needs, introducing new products, and spanning geographic boundaries such as oceans and mountains. While there are many positive aspects of this new business model, fraud is becoming a serious concern for all e-businesses, with a significant impact on the bottom line. Since the introduction of e-business, fraudsters have become very clever at searching out and finding ways around financial and inventory controls, penetrating e-business ordering, distribution and payment systems, and illegally extracting goods, services and funds from the e-business community.

Fraud is broadly defined as an intentional deception made for personal gain or to damage another individual. The difficulty of checking identity online, the ease with which fraudsters can redirect browsers to dishonest sites, and the international dimensions of the web, all make internet fraud the fastest growing area of fraud [Wikipedia 2010]. E-businesses, which conduct some or all of their business online, are particularly vulnerable to internet fraud.

E-businesses face many challenges, especially in today's turbulent economy, and losses caused by fraud make it even harder for the business to be profitable and survive. Fraud can be perpetrated by anyone, and the scams can range from customers using innocent looking deceptions to elaborate money laundering and terrorist schemes. Some of these frauds can be detected and prevented with the use of automated systems, but even when fraudulent activities are identified and thwarted, businesses incur costs. Also, a business with fraud detection systems in place may lose customers who do not want to deal with the additional security procedures required to place an order. Firms, like 2Checkout, market services to help e-businesses detect and control fraud, and struggle to keep up with ever changing and constantly evolving fraud schemes and techniques. Of particular concern for e-businesses are international fraud schemes, as these tend to be much more complex and are generally more difficult to detect, document, and prosecute.

TYPES OF E-BUSINESS FRAUD

System Manipulation. Some things never change, and for fraudsters system manipulation is one of them. Many of the fraudulent activities that have been used for traditional businesses can be applied to e-businesses as well. False invoices, false inventory adjustments, and cash manipulation are just a few of the activities fraudsters are fond of using. This type of fraud is much more technical than using stolen credit cards or returning different items for credit than were shipped; however, it is a serious challenge for e-businesses.

Stolen Credit Cards. One type of fraud faced by e-businesses is perpetrated by terrorists and other criminals, with the goal of money laundering or the use of stolen credit cards to acquire goods. Fraud perpetrated by online terrorists is often done by individuals residing in third world countries where governments, laws and business practices provide a wide open arena to commit fraud. Terrorists can easily perpetrate the fraud because the internet removes all time and geographic boundaries and opens a vast new market of opportunities. Recent terrorist use of credit cards shows their vulnerability to misuse in financing illegal activities. With terrorists the objective is to avoid showing the true identity of the terrorist, and they utilize both "clean" and stolen cards for their illegal purchases [Simon, 2008]. The company 2Checkout, an international online payment service, has encountered many forms of fraud, especially in third world countries where people are fraudulently using credit cards (or credit

card account numbers) stolen from people living in the United States. These cards are a target for acquisition by fraudsters because the United States has more credit cards than any other country and Americans are normally provided a higher credit limit than individuals in other countries. These stolen cards are often used to buy an intangible service, like an immediate download or perhaps a membership or a hosting service [Goodchild 2009].

Friendly Fraud

There is also a rise in "friendly fraud" by everyday consumers. Friendly fraud describes a consumer who makes an internet purchase with his or her own credit card, receives the goods or services, and then issues a charge back through the card provider. An e-business fraudster will dispute the online order but will not return the item, or they will use the product and then return it. When a charge back occurs the merchant is always responsible (from the perspective of the card issuer), and the challenge for the merchant is that there is no way to verify the authenticity of the transaction. Merchants selling services can create a system to check for a chargeback, and when one occurs they can immediately suspend services. Merchants selling durable goods can require delivery signatures and other confirmations, but have no reasonable way to get the merchandise back [Wikipedia, 2010].

Friendly fraud is committed by the customer as a way to reduce the balance on their credit card but still use or keep the product. Customers accomplish friendly fraud by claiming they never received the product, the product was not what they ordered or not good quality, or they claim they never authorized the order. This is often referred to as the "It wasn't me" scenario. When the cardholder cancels the transaction after obtaining goods or services, the merchant is defrauded. Law enforcement generally views credit card fraud as a victimless crime and find it difficult to investigate and prosecute, so generally it is not helpful to the defrauded merchant [Poole, 2008]. Merchants have a double dilemma: credit card issuers are trying to push more of the bad debt back to the merchants and their recovery programs generally lack teeth. Some merchants have been contacting customers when they are sure the charge back is fraudulent to tell them they will no longer accept their orders, law enforcement has been notified of a fraudulent transaction, and they will share negative customer information with other e-commerce merchants. E-businesses have had some success taking this hard line; however, there continues to be significant losses from friendly fraud [Botelle, 2010].

The current recession continues to negatively impact both businesses and consumers, and these economic hard times may encourage consumers to commit what they see as a harmless act, but in reality is fraud. However, other consumers are knowingly committing fraud and use clever ways to get what they want without having to pay out the cash. Some e-businesses have reported instances in which customers ordered an item, cancelled their order, and then sent back boxes filled with rocks or camera cords, but no cameras. Tam [2009] reported in the *Wall Street Journal* that businesses have seen a 50% spike in friendly fraud since October 2008.

Fraud Effects on E-Business

Fraud has a huge effect on e-businesses. However, it should be noted that e-businesses are not the only ones affected. Consumers are also negatively affected because of the losses incurred and fraud prevention expenses passed on to the consumer.

E-commerce fraud costs retailers approximately $4 billion each year, according to the most recent results of an annual survey conducted by Cybersource, a provider of electronic payment and risk management services [Goodchild 2009]. One example of a company facing fraud losses is photo equipment supplier Calumet Photographic Inc., which reports "it averages about $130,000 a week in fraudulent orders through its website. About 30% of those are friendly fraud, while the rest are traditional frauds with stolen credit cards" [Tam 2009]. Companies that experience "friendly fraud" get penalized twice as they lose the revenue from the sale and most times never receive their product back [Tam 2009]. Not only does the business face expenses from the lost merchandise, it also incurs extra fees. If an online merchant has charge backs over one percent of sales it may result in fines from Visa or MasterCard [Goodchild, 2009]. Sebbe Jones, manager of fraud and disputes at 2Checkout, puts blame on the credit card companies stating, "The credit card companies, so far, haven't really provided merchants an avenue to challenge those types of things successfully" [Goodchild 2009].

While merchants are experiencing increased online sales each year of about 15 to 20%, the increase in orders also results in more orders that must be screened. According to Cybersource, about 20% of online merchants report having a budget increase to support a manual review of transactions, and to cope with higher order volume. For an e-business without strong profits to support additional order checking, it is very hard for e-businesses to prevent fraud

[Ecommerce Fraud Management Needs an Efficiency Increase, 2008].

Customers are affected because the costs incurred by the vendor are eventually passed on to them in the price of the goods. Also, the extra security measures add more time and steps for the customer to complete the transaction. With more than 16 million households shopping on-line, new customers are introduced to the challenges of shopping on-line every day [Introducing eArmor, 2009]. Consumers must keep in mind that the extra steps in the transaction processing are to help keep them and their personal information safe, and to hold down the added cost of fraudulent transactions.

Consumers can take steps to protect themselves and decrease the amount of time spent during the online ordering process by using third party checkout services such as Amazon Pay Now, PayPal, and Google Checkout. A consumer can set up an account and pay online with these popular checkout sites. The consumer benefits by reducing the amount of times they must enter personal information and security codes for each purchase, and reducing the number of accounts they have open. Another advantage with using third party checkout services is it limits the amount of businesses that have the customer's credit card and personal information. When the customer uses these services, sensitive information is not re-sent to the merchant, keeping them from having access to, and possibly exposing to fraud, the customer's credit card data and other information.

Preventing Fraud

Some e-businesses have come up with their own ways to control and prevent the fraud. For instance, businesses have started identifying customers that frequently charge back items and are now putting them on a special list so they can monitor future transactions. Also, some companies are taking pictures of every packaged order before shipping it to prove they sent everything that was ordered [Tam 2009]. However, the fact remains that e-businesses are at a disadvantage when fraud occurs.

Another alternative companies can use is paying for an automated fraud prevention system. This system of prevention is underutilized because some businesses are not willing to pay the extra cost. Other businesses may not be fully aware of the benefits of the system. Of the 43% of e-commerce companies that do not have an automated fraud prevention program, anywhere from 40-100% of their orders are checked manually [Introducing eArmor, 2009]. Manually checking orders is a labor intensive and expensive process for companies, requiring employees to spend time confirming orders. Ecommerce Fraud Solutions offers E-armor, a program that "combines rules, neural networks and related machine learning algorithms to determine scores to implement fraud control for e-businesses [Introducing eAmor, 2009]. Another company businesses can use for fraud control is Global Payments. Forbes.com rated Global Payments as one of the 400 Best Big Companies for its business services and supplies. Global Payments is much like E-armor and provides fraud monitoring and charge back protection from friendly fraud. Global Payments uses a knowledge base from the major credit card companies to compare, identify, and reverse charge backs for which an invalid authorization has been identified. The Global Payments website claims that it auto- resolves about half of all charge backs, and provides immediate online documentation of charge backs [About Global Payments, 2009].

Another security system available for internet vendors is 2Checkout, an online payment service for small-and-medium-sized businesses [Goodchild 2009]. 2Checkout runs the transactions through its Fraud Net system, which uses computer algorithms to score each transaction. Based on the score, the transactions are then sorted into reject, suspect, or approve categories. A transaction may be "suspect" if the first or last name of the billing address was not capitalized. If the CVV code failed, then this causes even more suspicion. The CVV code is the 3 to 4 numbers you can find listed on the back of your credit card. This non-embossed number must be visually read, and helps insure the person making the transaction actually has the card in their possession, preventing fraudsters from completing the transaction if they have only your credit card number. Another thing the system checks for is the device IP address and the language the browser is using. The system flags places such as Nigeria, Ghana, and Vietnam because of frequent fraud problems. The suspect and reject classified orders are manually reviewed by an employee of 2Checkout.

Even with automated systems, human intervention and suspect transaction review, and careful order processing scrutiny, fraud can still occur. Although places like 2Checkout are using high-tech up-to-date software, it seems the fraudsters are often a step

ahead. Some of the effective tools that were used just a few years ago aren't effective anymore. Some fraudsters have figured out how to change their IP address to match the location of the billing address, and as a result the fraudster will successfully pass through 2Checkout's screening the first few times. Once 2Checkout sees a connection between these orders it will check the PC print of the device making the orders, and can check to see if the orders are sent from the same device identification number. If the orders have been sent from the same identification number it will disallow future business with any orders associated with this device. Tools used today will surely be compromised in a few years. The challenge of preventing fraud will require ongoing efforts, and looks to be never ending [Goodchild 2009].

RESPONSES TO E-BUSINESS FRAUD

Governmental Response. The Cybersecurity Act of 2009 has been introduced into Congress to ensure the continued flow of commerce within the US and with its global trading partners through ensuring secure cyber communications. The bill provides for continued development and exploitation of the internet for commerce, for the development of information technology specialists to improve and maintain effective cybersecurity defenses, and for other technology-related purposes. The ultimate goal is to streamline the cybersecurity effort through all levels of government (Open Congress, 2009). It is not anticipated the enactment of this bill will provide immediate comprehensive benefits for e-businesses; however, with the added visibility and concern for security issues new fraud prevention products and systems should be forthcoming.

Internal audit

E-business impacts internal auditors and their audit activities and procedures. It requires them to learn new skills and gain specialized knowledge to insure the business has proper controls to mitigate e-business fraud. Auditors are an important business asset that helps to identify business risks and, as a result, management is able to make better decisions on how to handle those risks. According to a survey by one of the large accounting firms, the largest technology issue faced by two thirds of the companies surveyed is their increase in e-business activities. Respondents believed the level of e-business activity had increased by 81% in the last three years and will increase from this much larger base by a further 52% over the next three years [Williams 2002]. As a result of business increases like these, company internal auditors will need to be more knowledgeable about techniques and software outside their normal comfort zone. Auditors may find it to be to their advantage to gain skills and knowledge much like that of information technology auditors.

Cases of E-Business Fraud

There are numerous reports of fraud cases affecting e-businesses. Both Ice.com and K-Swiss reported on friendly fraud occurring in their businesses. The vice-president of risk management at Ice.com worked with the Fayetteville, Georgia, police department to catch a serial friendly fraudster. The customer bought a $9,000 piece of jewelry from the company and then claimed he did not receive the correct item. The customer took the jewelry item Ice.com sent him and then returned a cheap piece of jewelry claiming he had received that instead. The police helped resolve the fraud by questioning the customer, who then returned the correct item and did not end up facing penalties.

The shoe company K-Swiss employs a director of e-commerce to help prevent frauds. One case he resolved was with a customer who claimed he didn't receive his shipment of shoes valued at $400. K-Swiss's director responded by saying he would have someone go to the customer's post office to get a copy of the required paperwork and signature used to receive the shipment. The customer then retracted his claim [Tam 2009].

The company 2Checkout works with businesses that sell internationally, and as a result has seen many types of fraud perpetrated by online terrorists. They try to prevent terrorists from money laundering by indentifying the device making each sale. The company can then match all the sales by one device to a list of vendors who are all operated by the same person or group. Recently they found that a vendor was on the Office of Foreign Asset Control's Specially Designated Nationals List (OFAC SND). OFAC SND is a list of names and aliases of known terrorists. Their quick actions enabled them to shut down the vendor without ever paying him.

Another case by 2Checkout was with a vendor that sold computers at a discounted price. The employees of 2Checkout were on the watch because of the low prices and contacted customers to get their feedback. They found that customers were not receiving computers, but instead got a box of ripped up phone books. Fortunately, 2Checkout did not pay the vendor immediately even though he persistently requested payment claiming the products had shipped.

2Chekcout stopped the payment to the vendor and refunded the customer's money.

IS THE EDUCATION SYSTEM MEETING THE E-BUSINESS NEEDS?

It is clear that there are two critical issues that must be addressed by every e-business: 1) Cyber-security and the control and prevention of fraudulent manipulation of computer and telecommunications systems; and 2) e-business manipulation through false ordering and returns, and fraudulent and stolen credit cards. Experience with traditional hands-on business practices does not always prove helpful for e-businesses. Because they never see their customers, it is often difficult to verify that an order has been properly filled, processed and delivered. It is also challenging to compete in an increasingly complex global marketplace. All these forces lead to increased risk for e-businesses. Educational institutions have tended to focus on traditional business models for management training, and technology training has generally been on programming and systems development. While these are needed and worthwhile endeavors, perhaps it is time to consider incorporating the new e-business model into courses and programs. Universities could address these needs in several ways:

1. Establish cyber-security and information assurance courses of study. These will provide students with a working knowledge of the issues, problems, general solutions and specific security remedies available.
2. Develop and provide management training programs and seminars to introduce the issues and remedies associated with e-business fraud.
3. Conduct research on the topic of e-business fraud and publish results for other academics and e-business managers. This will make interested individuals aware of the current state of e-business fraud.
4. Introduce the topic of e-business fraud into accounting, management, and computer technology courses for undergraduate and graduate business students. This will create an awareness of e-business fraud problems, and issues for students that may be working for e-business professionals, other business professionals and/or e-business clients and customers.

Courses such as cyber-security management, system security software, e-business fraud, and e-business practices would be appropriate. This paper is an exploration of the fraud concerns found with e-business; therefore, there is no specific curriculum course recommendations, only general suggestions for possible further study.

CONCLUSIONS

Businesses and consumers must be knowledgeable of the e-business risks they face and be aware of the ways to mitigate those risks. Consumers can reduce risks and protect themselves by using trusted payment systems, which limit the amount of businesses that have their personal information. Customers should also act ethically when making purchases and businesses should protect themselves with automated fraud protection software. E-business fraud is a growing concern and threat to e-businesses. Management and auditors should be knowledgeable of current frauds and controls that help reduce the chance of fraud. If fraud is not mitigated and there are no consequences for fraudsters, it will result in the breakdown and possible failure of many e-businesses. Consumers will not feel protected when using the online services and will discontinue using them. E-businesses will have to continue to increase prices as costs from fraud increase. Businesses are already struggling as the recession is felt by everyone. Customers are cutting back on spending and product costs are soaring. As a result, e-businesses are facing many risks, and without effectively controlling fraud, many will fail to survive this economically difficult time.

Educational institutions can come to the aid of e-businesses by conducting e-business research, developing courses and programs for undergraduate and graduate students, and working with e-business managers. Providing an awareness of the issues, remedies and fraud prevention products and procedures would be a service to both e-businesses and the consumer.

BIBLIOGRAPHY

"About Global Payments," (2009). *Global Payment*, found 1 December 2009 at http://www.globalpaymentsinc.com/about/index.html.

"Ecommerce Fraud Management Needs an Efficiency Increase," (2008). *Ecommerce Cache: Varien*, 29 January, found 1 December 2009 at http://www.varien.com/ecommerce/ecommerce-fraud-management-needs-automation/.

"Friendly Fraud," *Wikipedia*, found 3 May 2010 at http://en.wikipedia.org/wiki/friendly_fraud.

"Introducing eArmor From eCommerce Fraud Solutions," *Ecommerce Fraud Solutions.com*, found 1 December 2009 at http://www.ecommercefraudsolutions.com/.

"Open Congress," (2009). Found 1May, 2010 at www.yourcongress.org/bill/111-s773/show.

"Types of Fraudulent Acts," *Wikipedia*, found 26 January 2010 at http://en.wikipedia.org/wiki/Fraud.

Botelle, B. (2010). "Live from the MRC Conference: Foiling Friendly Fraud," 22 March, found 3 May 2010 at http://multichannelmerchant.com/ecommerce/news/mrc-foiling-friendly-fraud-0322/.

Goodchild, J. (2009). "E-Commerce Fraud: the Latest Criminal Schemes," *NetworkWorld.* 16 July, found 1 December 2009 at http://www.networkworld.com/news/2009/071609-e-commerce-fraud-the-latest-criminal.html.

Poole, R. (2008). "Understanding Friendly Fraud," *Merchant Talk*, 5 June, found 3 May at www.merchanttalk.com/2008/01/05/understanding-friendly-fraud/.

Simon, J. (2008). "The Credit Card Terrorism Connection," *CreditCards.com.* 15 May, found 26 January 2010 at http://www.creditcards.com/credit-card-news/credit-cards-terrorism-1282.php.

Tam, P. (2009). "Businesses Get Tougher on 'Friendly' Fraud," *The Wall Street Journal WSJ.com.* 26 May, found 1 December 2009 at http://online.wsj.com/article/SB124329230494652391.html.

Williams, E. (2002). "The Impact of Globalization on Internal Auditors: The Evolution of Internal Auditing," *Prepared for The Institute of Internal Auditors Research Foundation Board of Trustees*.