A Survey of E-Commerce; Its Security Issues and Way-Out

Agbaraji C. Emmanuel[1] and Agwah C. Benjamin[2]
Department of Electrical and Electronic Engineering, Federal Polytechnic Nekede, Owerri, Imo State, Nigeria

***Abstract* - Electronic Commerce is trading of products or services conducted through the Internet as its market place. It has provided numerous benefits to business owners and their customers thereby making it a vital business transaction means in the societies globally. E-commerce has suffered a lot of security failures such as identity theft, hacking, card fraud, phishing etc. The objective of this paper is to survey the e-commerce, its security vulnerabilities and recommend the best way to address the issues. The results of the survey showed that identity theft recorded lowest with 13.5% while lost/ stolen merchandise recorded highest with 40% from 2010 to 2013. Secondly, fraudulent transactions through alternative payments recorded the lowest in average with 19.75% compare to others while Credit card recorded highest in average with 62.25% from 2010 to 2013. It was therefore concluded that there is higher security failure in lost/ stolen merchandise and credit card fraud. However, ThreatMetrix can detect stolen credit cards in real-time and also it can secure customer user accounts to ensure they are not compromised. Therefore, ThreatMetrix was recommended to be deployed in all e-commerce transactions to protect the merchants and the customers from the most occurring security failures.**

Keyword - Chargeback; Customers; E-Commerce; E-Commerce Security; Internet fraud; Merchants

I. INTRODUCTION

Electronic commerce, commonly known as E-commerce or e-Commerce, is trading in products or services conducted via computer networks such as the Internet. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web at least at one point in the transaction's life-cycle, although it may encompass a wider range of technologies such as e-mail, mobile devices, social media, and telephones as well [1].

E-commerce has brought about remarkable developmental changes in the general buying and selling process globally by providing a lift to the traditional business transaction processes. Today, individuals, private and public owned establishments can run their business transactions through the internet without physical involvements. Prices of business goods and services can now be placed on the web sites with clear photos and descriptions, which enable buyers to make selections and purchase as well through the internet transactions. Hence, e-commerce makes business transactions easier and cheaper irrespective of the distance between seller and buyer compared to the physical process. Advances in information and communication technologies and the emergence of the internet have revolutionized business activities enabling new ways of conducting business referred to as electronic commerce [2; 3]. Electronic commerce (e-commerce) describes the process of buying, selling, transferring, or exchanging products, services, and/or information through computer networks, principally the Internet [3]. Electronic commerce can also be defined as "the sharing of business information, maintaining of business relationships, and conducting of business transactions by means of telecommunications networks" [2]. The Increase mobility and changing online shopping practices, advert and other business transactions are creating shifts in the role e-Commerce plays in overall retail operations. A subset of e-business is e-commerce, which describes the buying and selling of products, services, and information or making transactions via computer networks, including the Internet.

Electronic commerce activities include the inter-organizational processes of market-based sell-buy relationships and collaboration (known as business-to-business, or B2B, commerce) and consumer-oriented activities (business-to-consumer, i.e., B2C, and consumer-to-consumer, or C2C), as well as the intra-organizational processes that support them [2]. Electronic commerce as a way of doing business has significant advantages; organizations are embracing e-commerce as a means of expanding markets, improving customer service, reducing costs, and enhancing productivity [4]. Efficiencies are experienced in marketing and advertising; ecommerce makes disintermediation possible, eliminating the middleman [3]. Other efficiencies include reduced inventory and round the clock access at no additional cost. Ecommerce enables higher customization [5] allowing organizations to improve customer service. A vital benefit of ecommerce is access to global markets which enables businesses to expand their reach. The Internet allows for unconstrained awareness, visibility and opportunity for an organization to promote its products and services [6].

However, the security problems arising from e-commerce vulnerabilities keeps increasing with time due to the continuous increase in fraud and hacking practices. Customers and merchants have suffered tremendous categories of loss in their e-commerce transactions as a result of one failure or the other in the electronic commerce transaction. There are two major key players or ends in the e-commerce: the customer and the merchant or the business owner. Security failures can occur in any of the ends. Since e-commerce uses the internet as its market place therefore; it suffers all the security problems encountered by the internet users. Moreover, the internet fraud has generally been at the increase as the internet and computer technology (ICT) grows. Hence, in order to achieve the benefits of e-commerce in the society, the internet fraud prevention must be given adequate attention to protect merchants and customers in e-commerce transactions.

Internet fraud prevention is the act of stopping various types of internet fraud. Due to the many different ways of committing fraud over the Internet, such as stolen credit cards, identity theft, phishing, and chargeback, users of the Internet must make sure to avoid such scams. Internet fraud must be prevented on two ends. First, there is the basic user who may be susceptible to giving away personal information in a phishing scam, or have it be acquired by rogue security software or a keylogger [7]. In a 2012 study, Mcfee found that 1 in 6 computers do not have any sort of antivirus protection, making them very easy targets for such scams [8]. Business owners and website hosts are also engaged in the ongoing battle of preventing Internet fraud. Due to the illegal nature of fraud, they must ensure that the users of their services are legitimate. Websites with file hosting must work to verify uploaded files to check for viruses and spyware, while some modern browsers perform virus scans prior to saving any file (there must be a virus scanner previously installed on the system) [9]. However, most files are only found to be unclean once a user falls prey to one.

II. LITERATURE REVIEW

Joved and Vinod [10] suggested that electronic commerce, or *e-commerce*, refers to the purchase and sale of goods and services over the Internet. Fundamentally, e-commerce is about the people, process, and technology involved in allowing a consumer or business to purchase goods or services from another business or individual. They stated that for centuries, traditional commerce has involved physical brick and mortar businesses, stores, shopping malls, catalog sales, and so on. In the last hundred years, other channels for commerce, such as telephone and television sales were established. With the growth and widespread availability of the Internet in the 1990s, a sizeable commerce activity moved to the World Wide Web. Today, consumers go to their favorite e-commerce sites to not only to buy and sell, but to conduct research, review, or comment on products and services. A recent comScore presentation [11] reports that nearly 70 percent of customers consider the Internet to be an important factor in making buying decisions, and 60 percent have gone online to do research before purchasing items in a store.

Electronic commerce is a shorthand term that clinches a complex and continuous growing amalgam of technologies, infrastructures, processes, and products. It brings together whole industries and narrow applications, producers and users, information exchange and economic activity into a global marketplace called "the Internet." Hence, the internet is the major factor which provides the services of electronic commerce to the sellers and buyers of business goods and services. Therefore, increasing the availability of internet directly helps to expand the electronic commerce market place. There is no universal definition of electronic commerce because the Internet marketplace and its participants are so numerous and their intricate relationships are evolving so rapidly [12]. Nonetheless, one of the best ways of understanding electronic commerce is to consider the elements of its infrastructure, its impact on the traditional marketplace, and the continuum of ways in which electronic commerce is manifested. This approach shows clearly how electronic commerce is intricately woven into the fabric of domestic economic activity and international trade. Electronic commerce as it has evolved today requires three types of infrastructure:

- *Technological infrastructure to create an Internet marketplace.* Electronic commerce relies on a variety of technologies, the development of which are proceeding at breakneck speeds (e.g., interconnectivity among telecommunications, cable, satellite, or other Internet 'backbone;' Internet service providers (ISPs) to connect market participants to that backbone; and end-user devices such as PCs, TVs, or mobile telephones).
- *Process infrastructure to connect the Internet marketplace to the traditional marketplace.* This infrastructure makes payment over the Internet possible (through credit, debit, or Smart cards, or through online currencies). It also makes possible the distribution and delivery (whether online or physical) of those products purchased over the Internet to the consumer.
- *Infrastructure" of protocols, laws, and regulations.* This infrastructure affects the conduct of those businesses engaging in and impacted by electronic commerce, as well as the relationships between businesses, consumers, and government. Examples include technical communications and interconnectivity standards; the legality and modality of digital signatures, certification, and encryption; and disclosure, privacy, and content regulations.

Electronic commerce can be considered as a package of innovations [2]. The dependent variable is adoption of ecommerce. Adoption of ecommerce is defined as the use of computer networks, principally the internet, for sharing of business information; maintaining of business relationships; and conducting of business transactions [2; 3]. The likelihood of ecommerce adoption was put into operations as a dichotomy: whether the business has or has

not adopted ecommerce. According to Lavin et al [13] a business is defined as having adopted ecommerce if it is achieved interactive ecommerce status. There are six-phase ecommerce status indicators relevant to ecommerce in mostly the developing countries; which are: no ecommerce, connected e-commerce, static ecommerce, interactive ecommerce, transaction ecommerce, and integrated ecommerce.

Security of E-Commerce

Mark and Donald [14] stated that security is a major concern for e-commerce sites and consumers alike. They argued that Consumers fear the loss of their financial data, and ecommerce sites fear the financial losses associated with break-ins and any resulting bad publicity. Not only must e-commerce sites and consumers judge security vulnerabilities and assess potential technical solutions, they must also assess, evaluate, and resolve the risks involved.

The internet and its services have suffered a lot of security problems especially in the recent times. Since the electronic commerce makes use of the internet as its market place, it has equally suffered the same security issues causing a lot of loss in the transaction and thereby reducing the trust and dependability of the technology. It is unfortunate that online fraud collectively costs merchants billions of dollars each year, and it is not going away. A recent *Internet Retailer* survey (Fraud rates increase for 24% of web retailers over the past year) shows that 24% of respondents say that fraud rates for online transactions have increased over the past year [15]. Meanwhile, fraud rates have stayed the same for 63% of respondents; just 12% say fraud rates have decreased [15].

Unfortunately, just as merchants, internet service providers, and computer system and software manufacturers find ways to bolster protection in one area of the e-commerce, criminals soon find new weak spots and techniques, triggering another round of costly fraud and detection measures. Operating a secure online store and general business transaction is challenging, to say the least. Yet, by minimizing losses due to fraud and using security to build online business through customer confidence, merchants can increase the profitability of their e-Commerce initiatives.

E-Commerce Security Issues

There are many points of failure, or vulnerabilities, in an e-commerce environment. In some e-commerce cases, a customer contacts a business web site for e-commerce transaction and then gives his or her credit card details and address information for shipping a purchase and these personal information the customers give out can be used against the owner by fraud stars [14]. Typically, authentication begins on the customer's home computer and its browser. However, security problems in home computers offer hackers other ways to steal e-commerce data and identification data from users due to either lack of good anti-virus or breakdown of firewalls etc. Some current examples include a popular home-banking system that stores a user's account number in a Web "cookie," which hostile Web sites can crack [16], ineffective encryption or lack of encryption for home wireless networks [17], and mail-borne viruses that can steal the user's financial data from the local disk [18] or even from the user's keystrokes [19]. Whereas these specific security problems will be fixed by some software developers and Web site administrators, similar problems will continue to occur with increasing rate. Alternatives to the home computer include point-of-sale (POS) terminals in bricks-and-mortar stores, as well as a variety of mobile and handheld devices with continually updated anti-virus and operating systems.

According to Mark and Donald [14], the user's Web browser connects to the merchant or business owner on the front end. When a consumer makes an on-line purchase, the merchant's Web server usually caches the order's personal information in an archive of recent orders. This archive contains everything necessary for credit card fraud. Further, such archives often hold 90 days' worth of customers' orders. Naturally, hackers break into insecure Web servers to harvest these archives of credit card numbers. Several recent thefts netted 100,000, 300,000, and 3.7 million pieces of credit card data. Accordingly, an e-commerce merchant's first security priority should be to keep the Web server's archives of recent orders behind the firewall, not on the front-end Web server [20]. In addition, sensitive servers should be kept highly specialized by turning off and removing all nonessential services and applications such as FTP, e-mail etc. Other practical suggestions to secure Web servers can be found in [21; 22; 23].

Furthermore, the back end may connect with third party fulfillment centers and other processing agents through the same internet connection. Arguably, the risk of stolen product or information is the merchant's least important security concern, because most merchants' traditional operations already have careful controls to track payments and deliveries. However, these third parties can release valuable data purposely or otherwise through their own vulnerabilities. The description above is the simplified model of e-commerce architecture, nonetheless, a number of security problems still exist. It was even note that encrypted e-commerce connections do little to help solve any but network security problems and whereas other problems might be addressed by encryption, there are still vulnerabilities in the software clients and servers.

Types of Frauds Threatening E-Commerce

Typically, all online retailers and other e-commerce transaction users are scared of online fraud. Keeping the business and customers safe should always be at the top of your priority list of every business owner. Often times, e-commerce business owners are troubled about what types of fraud they should look out for to protect their business

and customers. The following is list of fraud and tips on how you can protect yourself from such breaches:

1. *Card fraud* – this is probably the most common of online scams. Essentially a thief gets their hands on someone's card details and uses those to pay for goods on the Internet. Fortunately thanks to schemes such as 3D Secure ("Verified by Visa" or "MasterCard SecureCode") most consumers will have set up a special password to protect themselves from such occurrences. If that is not the case then you as a business can help by monitoring your sales and using advanced fraud tools to spot suspicious transactions. If you feel that the person using a card is potentially a thief, you can simply refuse to authorize the purchase [24]. According to Wikipedia [1], Credit card fraud is the unauthorized use of a credit card to make a transaction. This fraud can range from using the credit card to obtain goods without actually paying, or performing transactions that were not authorized by the card holder. Credit card fraud is a serious offense, and punished under the charge of identity theft. The majority of this type of fraud occurs with counterfeit credit cards, or using cards that were lost or stolen. Approximately 0.01% of all transactions are deemed fraudulent, and approximately 10% of Americans have reported some type of credit card fraud in their lifetimes [25].
2. *The man-in-the-middle attack* – this is where a cyber-criminal eavesdrops on a session between your shop and the customer and records the cardholder data being exchanged. The best way to stop such attempts is by using an SSL certificate. All payment service providers will use such protection on their payment gateways and you will also need to obtain one for your website. This should eradicate most attacks [24].
3. *Identity Theft* - Identity theft, also called identity fraud, is a term used to refer to a crime in which someone steals and uses another person's personal information and data without permission. It is a crime usually committed for economic gain. Stolen personal data includes Social Security Number's (SSN), passport numbers, or credit card numbers, which can easily be used by another person for profit. It is a serious crime that can have negative effects on a person's finances, credit score and reputation. There are three specific types of identity theft aside from the broad term. Tax-related identity theft is when a criminal uses someone else's SSN to get a tax refund or a job. Child identity theft is when a criminal uses a child's SSN to apply for governmental benefits, open bank accounts, or apply for a loan. Medical identity theft is when a criminal uses someone else's name or health insurance to see a doctor, get a prescription or other various medical needs [26].
4. *Hacking* – this is a very bad scenario where a fraudster gains access to the control tools of your website. This gives them unrestricted access to all of the pages, including the payment page. You can minimize the damage from such an attack by allowing your payments provider to host your payments page on their server. From the customer's end he or she should ensure that the latest version of the CMS (Content Management System) is always used on which the website is built and that the hosting is secure. Regularly change passwords to the website and make sure that any third party software and plugins used are also secure and trustworthy.
5. *Phishing* - Phishing is a scam or fraudulent activity by which an e-mail user is duped into revealing personal or confidential information which the scammer (phisher) can use illicitly [27]. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware [28]. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. There are four main types of phishing techniques: *link manipulation*, *filter evasion*, *website forgery*, and *phone phishing*. Legislation, user training, public awareness, and technical security measures are all attempts to control the growing number of phishing attacks. The damage caused by phishing ranges from denial of access to email to substantial financial loss. It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately US$929 million. United States businesses lose an estimated US$2 billion per year as their clients become victims [29]. The address that the individual knows is the company's genuine website can be typed into the address bar of the browser, rather than trusting any hyperlinks in the suspected phishing message this will help to prevent phishing. Nearly, all legitimate e-mail messages from companies to their customers contain an item of information that is not readily available to phishers. It is up to the customer to use his or her discretion to separate genuine emails from phishing emails and prevent phishing attacks [30].
6. *Malicious Code* – there are different types of malware used by criminals. The most common include key-loggers or spyware (captures data as the user enters it), backdoor (gives the hacker remote access to your computer), command and control (looks for and executes commands). The best way to protect one from such attacks is to keep any software on the computer up to date, use an anti-virus programme and perform regular scans on the machine.
7. *Chargeback* - A chargeback is not necessarily a fraudulent activity. In its most basic sense, a chargeback is when an issuing bank, a bank where consumers acquire credit cards, reverses a prior charge from a bank account or credit card at the request of a cardholder because there was a problem with a transaction. The problem could be anything from a situation where the consumer did not receive the

product they purchased [31], to one where the cardholder was not satisfied with the quality of the product, to a situation where the cardholder was a victim of identity theft [32]. The concept of a chargeback rose as a measure of consumer protection taken by issuing banks and credit card companies. Chargebacks were a measure to protect cardholders from identity theft and the unauthorized transitions from identity theft. Chargebacks also provide inventive to producers and sellers to provide products of consistent quality and efficient customer service.

However, with the rise of technology [33], and the resulting increase in online and telephone transactions and commerce, it has become easier to commit fraud via chargebacks. Chargebacks are an interesting concept because the process protects consumers from identity theft fraud, but opens the door for consumers to commit chargeback fraud. Chargeback fraud is also known as "friendly fraud." Friendly fraud is the term for when a consumer authorizes a transaction for an online purchase on his or her credit card, receives the product or products the consumer paid for, but then later the same consumer files for a chargeback [31]. The fraudulent filing for a chargeback results in a consumer keeping and avoiding paying for the products they ordered.
The best way to prevent friendly fraudsters is for producers to require signatures for the delivered packages upon their arrival. This will provide very specific information to the producers about the delivery. The only drawback to signature confirmation is the fact that it increases shipping costs, which still hurt producers' bottom line [34].

III. SECURITY METHODS

The electronic commerce merchants continually provide solutions to the security issues to protect their business and customers, unfortunately, the fraudsters and hacker work with the same pace to break possible security methods. However, the best security in e-commerce can be achieved with proper carefulness in applying the most updated security method. The following are some certified security methods [15].

Encryption

Privacy is handled by encryption. In PKI (public key infrastructure) a message is encrypted by a public key, and decrypted by a private key. The public key is widely distributed, but only the recipient has the private key. For authentication (proving the identity of the sender, since only the sender has the particular key) the encrypted message is not encrypted again, but this time with a private key. Unfortunately, PKI is not an efficient way of sending large amounts of information, and is often used only as a first step — to allow two parties to agree upon a key for symmetric secret key encryption. Here sender and recipient use keys that are generated for the particular message by a third body: a key distribution center. The keys are not identical, but each is shared with the key distribution center, which allows the message to be read. Then the symmetric keys are encrypted in the RSA manner, and rules set under various protocols. Naturally, the private keys have to be kept secret, and most security lapses indeed arise here.

Encryption also involves using the key pair but in reverse. Once your message is completed you encrypt the file using the recipient's public key ensuring that only the recipient can ever access that message with their private key

Digital Signatures and Certificates

Digital signatures meet the need for authentication and integrity. To vastly simplify matters (as throughout this page), a plain text message is run through a hash function and so given a value: the message digest. This digest, the hash function and the plain text encrypted with the recipient's public key is sent to the recipient. The recipient decodes the message with their private key, and runs the message through the supplied hash function to that the message digest value remains unchanged (message has not been tampered with). Very often, the message is also times tamped by a third party agency, which provides non-repudiation.

What about authentication? How does a customer know that the website receiving sensitive information is not set up by some other party posing as the e-merchant? They check the digital certificate. This is a digital document issued by the CA (certification authority: Verisign, Thawte, etc.) that uniquely identifies the merchant. Digital certificates are sold for emails, e-merchants and web-servers. Digital signature shall be discussed in detail in subsequent units of this course.

Secure Socket Layers

SSL stands for Secure Sockets Layer. This is the technique in which web servers and web browsers encrypt and decrypt all of the information that they transmit and receive. Secret decoder rings time. Both ends establish and use the same scheme for making sure that no one else is listening to their conversation. Information sent over the Internet commonly uses the set of rules called TCP/IP (Transmission Control Protocol / Internet Protocol). The information is broken into packets, numbered sequentially, and an error control attached. Individual packets are sent by different routes. TCP/IP reassembles them in order and resubmits any packet showing errors.

SSL uses PKI and digital certificates to ensure privacy and authentication. The procedure is something like this: the client sends a message to the server, which replies with a digital certificate. Using PKI, server and client negotiate to create session keys, which are symmetrical secret keys specially created for that particular transmission. Once the

session keys are agreed, communication continues with these session keys and the digital certificates.

PCI, SET, Firewalls and Kerberos

Credit card details can be safely sent with SSL, but once stored on the server they are vulnerable to outsiders hacking into the server and company network. A PCI (peripheral component interconnect: hardware) card is often added for protection, therefore, altogether is adopted: SET (Secure Electronic Transaction). Developed by Visa and Master-card, SET uses PKI for privacy, and digital certificates to authenticate the three parties: merchant, customer and bank. More importantly, sensitive information is not seen by the merchant, and is not kept on the merchant's server. Firewalls (software or hardware) protect a server, a network and an individual PC from attack by viruses and hackers. Equally important is protection from malice or carelessness within the system, and many companies use the Kerberos protocol, which uses symmetric secret key cryptography to restrict access to authorized employees.

Transaction Fraud Prevention

In transaction fraud prevention security approach, e-commerce sites must make instant decisions about card-not-present (CNP) interactions by deploying some proven techniques such as the ThreatMetrix. The ThreatMetrix detects stolen credit cards in real-time by combining device attributes, malware detection and sophisticated analytics with the user identity and transaction details. This real-time analysis offers online merchants an additional layer of protection to reduce the costs of fraud while protecting the online experience for legitimate customers. Reduce costs of transaction fraud charge backs and fees. It also performs the following duties [35]:

- Protect transactions and customers from malware targeting their credit cards and online identity.
- Reduce lost sales from false negatives with advanced device identification and context-sensitive fraud detection.
- Address payment card industry (PCI) standards for preventing data breaches.

Account Take-over Protection

Electronic commerce consumers often lack the client-side security they need to protect themselves from account compromise. Using ThreatMetrix, the customer can identify a variety of attacks designed to steal user account credentials, the precursor to e-commerce fraud. ThreatMetrix detects Trojans, phishing attacks, man-in-the-browser (MitB) attacks and other attacks on computers, smartphones, tablets and other web-enabled devices. It also detects activity from already compromised accounts. By using the account takeover prevention solution, the customer gains instant visibility into the integrity of his or her user accounts and their credentials. With ThreatMetrix the customer can secure user accounts, ensure they are not compromised or a source of e-commerce fraud. ThreatMetrix detects compromised accounts across multiple dimensions, including [35]:

- Automated logins from bots and compromised devices.
- Phishing attacks and detection of compromised accounts being used to commit fraud.
- Malicious software, including web-based and machine resident malware.
- Access from suspicious locations, unrecognized computer settings or from masked machines.

TrustDefender Cybercrime Protection Platform

The TrustDefender Cybercrime Protection Platform's unique and game-changing approach leverages the collective power of the Global Trust Intelligence Network. ThreatMetrix detects web fraud by analyzing online identities and their associated devices, using anomaly and velocity rules to make real-time decisions. It builds a comprehensive online persona of each user attempting an online transaction, by combining online identities and device fingerprints while also detecting anomalies and malware-based compromises. Business policies allow configuration of user trust levels to fit each organization's business model. Shared intelligence across millions of daily transactions processed by the Global Trust Intelligence Network provides predictive analytics, to protect online businesses and reduce customer friction. The TrustDefender Cybercrime Protection Platform is the only solution that offers all of these critical components and provides them in a single, integrated solution. This collective approach ensures that customers have maximum visibility into the activities of fraudsters and hackers [15].

IV. E-COMMERCE FRAUD RESULTS AND DISCUSSIONS

There are numerous statistical reports concerning the incessant and creasing rate of fraud against e-commerce transactions. E-commerce security failures had been categorized by fraud types which are can be: identity theft, friendly fraud, fraudulent request for return/refund, or lost or stolen merchandise. The statistical report in figure 1 shows that identity theft occurred lowest with 13.5% average from 2010 to 2013 compared to other fraud types. It gradually increased from 11% in 2010 to 17% in 2013. This signifies that fraud through identity theft has been in good control but there is an increase in security failure toward such fraud type.

There is an average decrease in the growth of friendly fraud and fraudulent request for return/refund from 20% in 2010 to 18% in 2013 which shows that the security measures applied are effectively working towards reducing the occurrence of such frauds.

The report shows that lost or stolen merchandise recorded highest with an average value of 40% from 2010 to 2013. It was shown in the result that it recorded lowest with 36% in 2013 and highest with 45% in 2010. This signifies that despite the unsteady nature of the fraud type and high occurrence, there was success in the recent result towards reducing the occurrence of such fraud. The distribution of fraud types is shifting towards those associated with the greatest costs. Lost and stolen merchandise declined from 45% to 36% over the past year. This type of fraud may be factored into shrink, and does not typically burden merchants with additional costs beyond replacing and redistributing merchandise. ID fraud, which can result in greater liability for merchants, rose from 12% of fraud in 2012 to 17% in 2013 [36].

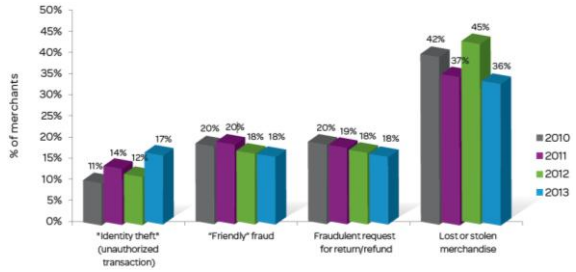

Figure 1: Percent of Fraudulent Transactions Attributable to Fraud Types [36]

Figure 2 shows the percent of fraudulent transactions attributable to payments methods among merchants accepting specific payment methods. From the report, fraudulent transactions through alternative payments (PayPal, BillMeLater, eBillme, Google checkout etc.) recorded the lowest in average with 19.75% compare to others while Credit card recorded highest in average with 62.25%. The result also shows that fraudulent transactions through credit card reduced from 66% in 2010 to 58% in 2013 showing slight success in reducing its occurrence.

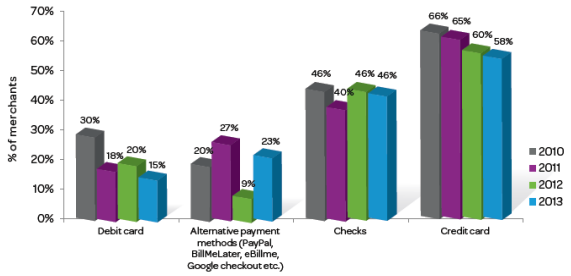

Figure 2: Percent of Fraudulent Transactions Attributable to Payments Methods among Merchants Accepting Specific Payment Methods [36].

The result illustrated in figure 3 also shows that fraudulent transactions committed through credit/ debit card recorded highest with 75% from 2012 to 2013. While refund fraud and voucher/ gift fraud recorded the lowest with 3% each.

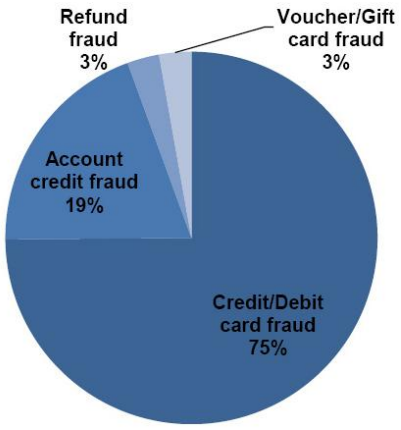

Figure 3: Fraud incidents by type of payment methods [37]

Mobile merchants are incurring the greatest fraud losses as a percent of revenue among all merchant segments (0.75% in 2013). This is the only segment to have not benefitted from a decrease in fraud as a percent of revenue from 2012 to 2013, yet mobile merchants are seeing an increase in revenue through this channel (from 14% in 2012 to 19% in 2013) [36].

V. CONCLUSION AND RECOMMENDATIONS

Electronic Commerce is a business method which makes use of the internet as its market place where the merchants showcase and market their business products and services and the customers can make selections and purchase the goods and services using their payment detail and address information. It has numerous benefits which can help both the merchants and the customer to make their transactions quickly with ease and low cost. However, the problem of security has affected the e-commerce progress in the society at large. The security problems of e-commerce can be attributed to the failures of internet which provides the market platform, the merchant and the customer ends. There are many types of fraud which have troubled the users of e-commerce which can be in the form of the following: Card fraud, the man-in-the-middle attack, Malicious Code etc.

The results of the survey carried out on the e-commerce security shows that identity theft as a fraud type recorded lowest with 13.5% while lost/ stolen merchandise recorded highest with 40% from 2010 to 2013. It was therefore concluded that there is higher security failure in lost/ stolen merchandise. Since ThreatMetrix can detects stolen credit cards in real-time by combining device attributes, malware detection and sophisticated analytics with the user identity and transaction details, it should be deployed generally to solve the security problem in the lost/ stolen merchandise.

From the results, fraudulent transactions through alternative payments (PayPal, BillMeLater, eBillme, Google checkout etc.) recorded the lowest in average with 19.75% compare to others while Credit card recorded highest in average with 62.25% from 2010 to 2013. Therefore, it was concluded that more fraudulent

transactions are carried out through credit/ debit cards. Since ThreatMetrix can secure customer user accounts to ensure they are not compromised or a source of e-commerce fraud and also detects compromised accounts across multiple dimensions. Therefore, ThreatMetrix was recommended to be deployed in e-commerce transactions to protect the merchants and the customers.

REFERENCE

[1] Wikipedia. "E-Commerce", http://en.wikipedia.org/wiki/E-commerce, Retrieved June 22, 2014
[2] Zwass, V. "Electronic Commerce and Organizational Innovation: Aspects and Opportunities", International Journal of Electronic Commerce, 2003.
[3] Turban, E., King, D., Lee, J., & Viehland, D., "Electronic Commerce: A Managerial Perspective", New Jersey: Pearson/Prentice Hall, 2004.
[4] Wenninger, J., "The Emerging Role of Banks in E-Commerce", Current Issues in Economics and Finance, 6(3) 2000.
[5] Choi, S. & Winston, A., "Benefits and requirements for interoperability in electronic marketplace", Technology in Society, 22, pp33–44, 2000.
[6] Senn, J. Business-to-business e-commerce. Information Systems Management, Spring, 2000, pp23–32,
[7] Wiki. "Internet Fraud Prevention", http://en.wikipedia.org/wiki/Internet_fraud_prevention, Retrieved July 2, 2014
[8] Tomsh, 2012. "1 in 6 Windows PCs Have Zero Antivirus Protection", http://www.tomshardware.com/news/M,15826.html, Retrieved July 1, 2014
[9] Mozillazine, 2012. "Browser.download.manager.scanWhenDone", http://kb.mozillazine.org/Browser.download.manager.scanWhen Done, Retrieved July 3, 2014
[10] Javed S. and Venod S., "A Prescriptive Architecture of Electronic Commerce and Digital Marketing", Microsoft Corporations, Version 2.0, 2010.
[11] comScore, "State of the U.S. Online Retail Economy Through Q1 2009", comStore, Inc., 2009.
[12] OECD 1999, "The Economic and Social Impact of Electronic Commerce", www.oecd.org/dsti/sti/it/ec/act/SACHER.HTM, Retrieved July 2, 2014
[13] Lavin A. Xaveria F. and Lindh J, "Factors Affecting E-Commerce Adoption in Nigerian Banks", Jonkoping International Business School, Jönköping University, 2006.
[14] Mark S.A and Donald T.D., "Privacy and Security Issues in E-Commerce", Elsevier Science (USA), 2003.
[15] Gerald C. O., "E-Business Security", National Open University of Nigeria, 2009.
[16] Graves, P., and Curtin, M. 2000, "Bank One Online Puts Customer Account Information At Risk." http://www.interhack.net/pubs/bankone-online, Retrieved July 3, 2014
[17] Borisov, N., Goldberg, I., and Wagner, D. "Intercepting Mobile Communications: The Insecurity of 802.1", Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, 2001, 180–189.
[18] Roberts, P. 2002, "Bugbear Virus Spreading Rapidly" PC World Online, October 2, 2002.
[19] Neyses, J.. "Higher Education Security Alert From the U.S. Secret Service: List of Keystroke Logging Programs." http://www.unh.edu/tcs/reports/sshesa.html, Retrieved July 1, 2014
[20] Winner, D. "Making Your Network Safe for Databases", SANS Information Security Reading Room, July 21, 2002.
[21] Tipton, H., and Krause,M."Information Security Management Handbook", New York: CRC Press, 2002
[22] Garfinkel, S., "Web Security, Privacy and Commerce." Cambridge, MA: O'Reilly and Associates, 2002
[23] Garfinkel, S., Schwartz, A., and Spafford, G. "Practical Unix Internet Security", Cambridge, MA: O'Reilley, 2003
[24] "Top Types of Fraud Threatening Your E-Commerce", http://www.paypoint.net/ideas/business-support/online-fraud-types/, Retrieved July 6, 2014
[25] "Credit Card Fraud Statistics", http://www.statisticbrain.com/credit-card-fraud-statistics/, Retrieved July 6, 2014
[26] "Consumer Information: Identity Theft", http://www.comsumer.ftc.gov/features/feature-0014-identity-theft, Retrieved July 6, 2014
[27] Merriam-Webster Dictionary http://www.merriam-webster.com/dictionary/phishing, Retrieved July 6, 2014
[28] Niels, P., 2014, "Safe Browsing. Google Blog", http://googleonlinesecurity.blogspot.jp/2012/06/safe-browsing-protecting-web-users-for.html, Retrieved July 6, 2014
[29] Paul L. P., 2013, "How Can We Stop Phishing and Pharming Scams?" http://web.archive.org/web/20080324080028/http:/www.csoonline.com/talkback/071905.html, Retrieved July 6, 2014
[30] Wayback Machine, 2006, "Anti Phishing Tips You Should Not Follow", http://web.archive.org/web/20080320035409/http:/www.hexview.com/sdp/node/24, Retrieved July 6, 2014
[31] "Chargeback Guide", https://www.paypal.com/us/webapps/mpp/security/chargeback-guide, Retrieved July 6, 2014
[32] "Chargebacks: A Survival Guide" http://www.cardfellow.com/blog/chargebacks/, Retrieved July 6, 2014
[33] "Chargeback Fraud", https://chargebacks911.com/chargeback-fraud/, Retrieved July 6, 2014
[34] Sarasota F.L, 2012, "Common Charge Backs Often Associated to Friendly Fraud", http://fraudpractice.com/News-Friendly-Fraud-Chargebacks.html, Retrieved July 6, 2014
[35] ThreatMetrix, 2014, "Less fraud, more orders. Use real-time defenses to minimize credit card fraud and account takeover risks while keeping the customer experience hassle-free", http://www.threatmetrix.com/industries/e-commerce/, Retrieved July 6, 2014
[36] LexisNexis, "Merchants Struggle against an Onslaught of High-Cost Identity Fraud and Online Fraud" Annual Report, LexisNexis Inc., 2013
[37] "Retail Crime Survey-E-Commerce Retailers Fight Online Fraud", Payments Cards and Mobile (PCM), http://www.paymentscardsandmobile.com/retail-crime-survey-e-commerce-retailers-fight-online-fraud/, Retrieved July 7, 2014