Search information

Received 2023/02/25
Accepted 2023/06/15

Printed ISSN: 2352-989X
Online ISSN: 2602-6856

Fraud and its Techniques in e-commerce

BOUHEDDA Kheireddine

University of Yahia Fares-Medea (Algeria),
bkheire2015@yahoo.com

ABSTRACT

An e-commerce scam is defined as a deception designed by deceivers to take advantage of or rob stores, companies, and even people via the Internet. Defrauders criminally target merchants and other online e-commerce activists to obtain some type of financial or personal gain, causing losses to multiple parties. In other words, technological growth and the general change in online activities have made it easier for fraudsters to obtain personal and financial information that they can use to commit fraud. this research paper, tries to highlight the most important methods and techniques used by cybercriminals in the fraud process, and this is according to the following research problem: Are the fraudulent methods in electronic commerce that criminals take one, or multiple? this research paper aims to know the criminal methods or methods in e-commerce that fraudsters pursue, and this is to avoid falling into them. This analysis is embodied in the context of content analysis.

Keywords: E-commerce, commercial fraud, financial crimes, communications network

INTRODUCTION

The beginning of the twenty-first century brought new technology known as the "Internet revolution”, this latter carried out a new business known as “electronic commerce” which is still relatively new. Today, the Internet is the mother that gave birth to electronic commerce, and it is behind the most important scientific achievements that emerged at the beginning of the twenty-first century. The booming e-commerce technology is a revolution in the trading system, breaking through time and space. Some statistics show that e-commerce reached 29 trillion dollars in 2017. This large volume of e-commerce activity has resulted in many criminal activities. E-commerce companies can be exploited for criminal purposes in several ways, whether by defrauding the customer for not delivering goods or services, purchasing goods or services using stolen bank card data, creating e-commerce businesses as a front for illegal transactions, or misusing markets. Over the Internet to transfer criminally (illegal) money. This research paper, is an attempt to highlight the most important methods used by cybercriminals in the fraud process, and this is according to the following research problem: Are the fraudulent methods in e-commerce that criminals take one, or are they multiple? The aim of this research paper is to know the criminal methods or methods in electronic commerce, and this is to avoid falling into it. This analysis is embodied in the context of content analysis.

2. Methodology of the Study

The researcher collected research material information regarding, e-commerce fraud and crime on the internet that merge since the end of the twenty century. The researcher investigates data from many sources such as books, articles, websites, and reports, that related to the problem question and the objective of the study. Qualitative methods are used to discuss the problem question, in a holistic approach. The researcher selected examples of each method of fraudsters that have been used since the emergence of e-commerce criminality.

3. A Short Overview of the Development of e-Commerce

According to the editor-in-chief of the International Journal of E-Commerce, Vladimir Zwas, e-commerce shares commercial information, maintains commercial relations and conducts commercial transactions through telecommunications companies. E-commerce has existed for more than thirty years, and it arose from the electronic transmission of messages through the Berlin Air Bridge In 1948, these have their origins in the Berlin Blockade of 1948-1949 and the airlift over a system of ordering goods primarily via telex. (Zwass, 2016) In this sense, the resulting computer-to-computer Electronic

Data Interchange (EDI) works with most simple electronic business transactions. (Zwass 2016)

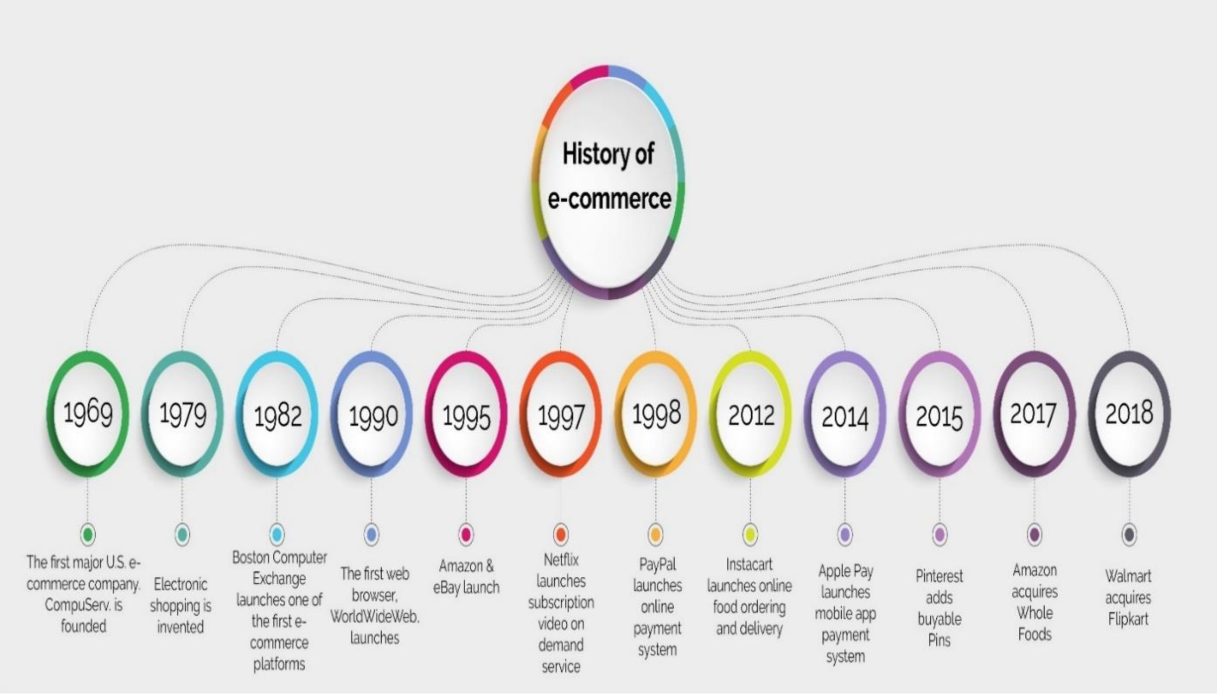
In the 1960s a collaborative effort among industry groups produced the first attempt at common electronic data formats. However, the formats were only intended for the purchase, transmission, and, financing of data and were used primarily for transient actions within the industry. Work on national electronic data interchange standards did not begin until the late 1970s. Which developed well in the late nineties. (Kutz, 2016) Before that, the operation of the EDI system was expensive due to the high cost of private networks, and therefore the absorption was largely limited to rich multinational companies, using their financial strength to pressure and persuade smaller suppliers to implement EDI systems, often at a very high cost. (Kutz 2016)

With the widespread adoption of the Internet, the introduction of the World Wide Web in 1991, and the first browser in 1993, most e-commerce has turned to the Internet. (Zwass 2016) By 1996 there were no more than 50,000 companies in Europe and 40,000 in the United States of America using EDI, representing less than 1% of the total number of companies worldwide. (Zwass 2016) Recently, with the global spread of smartphones and access to fast broadband internet connections, much of e-commerce has moved to mobile devices, which also include tablets and computers. Thus, the history of e-commerce is related very much to the Internet, in other words, is intertwined with the history of the internet. The Internet was opened to the public in 1992. To history amazon was the first e-commerce site to begin selling products online, hundred after that have followed since. After we have discussed a brief history of electronic commerce, it is worth knowing the most important global electronic markets, which contribute significantly to global trade.

4. The Major Important Global Markets in e-Commerce.

At the end of the twentieth century, economic globalization dominated the global economy and created new concepts and ideas designed to control that system while explaining the new conditions to investors and that the new global market today is the main driving force behind finance and international trade, as it deals with concepts on the scale of the macro and micro economy. A single geographic area often provides better value for certain products or industries and continued equivalence at a higher rate of return for the same amount of capital inflow. (Cecile, 2019)

Fig.1. shows an infographic of some of the world's leading companies in the field of e-commerce.


History of e-commerce
1969
1979
1982
1990
1995
1997
1998
2012
2014
2015
2017
2018
The first major U.S. e-commerce company. CompuServ. is founded
Electronic shopping is invented
Boston Computer Exchange launches one of the first e-commerce platforms
The first web browser, WorldWideWeb. launches
Amazon & eBay launch
Netflix launches subscription video on demand service
PayPal launches online payment system
Instacart launches online food ordering and delivery
Apple Pay launches mobile app payment system
Pinterest adds buyable Pins
Amazon acquires Whole Foods
Walmart acquires Flipkart

Source: https://www.the-future-of-commerce.com/2020/01/30/

In 1969, CompuServe was the first major e-commerce company to be established in the United States of America. It has grown from an e-mail service provider to a remote facility in the seventies of the last century. Also, do not forget that the entry of cable television into the service in the United States of America also contributed. In the development and crystallization of the field of electronic commerce. Some tech-savvy users also formed The Boston Computer Exchange, which was a billboard-based marketplace created to facilitate the sale of used computers. This company pioneered the formulation of a fully automated online auction and marketplace for global trade, such as; Alibaba, Amazon, and Walmart. eBay, Way-Fair, and PayPal. (Mady, 2020)

It can be said, for many years, electronic commerce existed quietly, but in 1993 and with the launch of the first web browser for the World Wide Web, e-commerce took off at an increasing speed.

In this research paper, after we have dealt with a brief historical overview of electronic commerce and the most important electronic commercial markets, and according to what we have raised in the problem and objectives of the subject of crimes or fraud in electronic commerce, we try to highlight the most important methods of fraud in electronic commerce. But before that, e-commerce must be defined, with a mention of the nature of e-commerce.

5. Meaning of e-commerce

It is trading in products, services, or services using computer networks such as the Internet, and e-commerce relies on technologies such as mobile commerce, electronic money transfer, supply chain management, marketing, and online transaction processing as well as electronic data exchange, inventory management systems, and automated data collection systems. E-commerce typically uses the World Wide Web as at least one part of the transaction lifecycle, although it also uses other technologies such as email. Some e-commerce companies may use some or part of the following: (Martin 2016)

- Internet marketing sites for direct retail sales to consumers
- Providing or participating in online marketplaces that process sales to many parties
- Buying and selling between companies
- Collect and use demographic data through web and social media communications
- Electronic data exchange between companies
- Marketing to potential clients via (e-mail or fax)
- Engaging in pre-sales to launch new products and services as retail, (also referred to as pre-retail or pre-trade).
- Before we talk about the techniques or techniques of e-commerce, it must be mentioned

6. Nature of e-commerce

The mother of electronic commerce is the Internet, and the transaction on the Web took many technical technologies such as the email protocol. e-commerce businesses contain buying goods or things such as Alibaba or Amazon…many Academics and researchers categorized three areas of e-commerce; online retailing, electrics Markets, and online auctions. (Indraprastha 2019) However, the key reasons that have been behind the raise of e-commerce, one can mention;

1. The accessibility to the internet
2. Access to the global market is much easier
3. The cost of the goods in e-commerce is likely less than in traditional commerce
4. Rapid response to needs

5. Global choice for e-commerce
6. Saving cost

Computerization and communication are two roads on which the internet has been soul to them, and that is behind the genesis of e-commerce which has been a global power in business since the flourishing of the internet in society by the end of twenty century. over the years techniques of fraud and theft raised in e-commerce and taken many methods via the internet. Hence this paper will light this technique by highlighting them to the readers to avoid those scammers.

7.E-commerce Fraud

Many definitions have been given to e-commerce fraud, one's can find that the term refers to electronic business, or activity over the internet by buying or selling products by using online services. Now-day fraud in e-commerce is increasing dramatically and dangerously, while the increase in fraud in itself is not new. Fraud existed since 1993 which means it started when the internet went vast throughout all the countries and is increasing annually in a way that draws attention. (Witke, 2019) Card-not-present Fraud (CNP) is expected to increase. Hence, fraud is the unauthorized use of a payment card when the cardholder does not actually present it at the time of the transaction. (Bacan, 2015) Over time e-commerce fraud is not exclusive to credit card payments, criminals are becoming more sophisticated in using malware to command logins to online banking, phone, tablets, and computers, using stolen bank account details to make fraudulent payments. According to a field procedure conducted by Karsten Witfe, on a group of merchants from six industrialized countries, he came up with facts that the crime used by criminals is embodied in six important and effective ways in cybercrime. (K. Witke 2019)

So, the technique in e-commerce has taken many faces or ways not just one expression that criminals used.

This paper shed light on the most common methods in e-commerce fraud and also will answer the problem question of which, criminality in e-commence takes many faces, not just one as this article mentions in the problem question. Six methods which are most known in the world of e-commerce lawbreaking or criminality going to be highlighted;

7.1 Identity Theft:

Identity theft and, identity fraud are two terms that refer to the same meaning, which is all sorts of crime that can be used by one person, group, or by company, wrongfully gets and uses another person’s information data in an unauthorized manner that involved fraud for e-commerce gain. Identity theft is the most common method and, the most common type of fraud in e-commerce that confuses merchants is embodied in identity theft 71%, phishing 66%, and account theft 63%. Hence, credit card theft is the most common target, as the fraudster does not need much to perform a “non-card” transaction. exist” (CNP). Identity theft occurs when someone steals their personal information such as their Social Security number, bank account number, and credit card information. Identity theft can occur in several ways, as some identity thieves search through garbage cans to try to find bank or credit card statements, and also include more high-tech methods of accessing a company's database to steal lists of customer information, and once identity thieves have the information The ones, they search for can destroy a person's credit application and other information standing. (Kagan, 2021)

Identity thieves are also increasingly using computer technology to obtain other people's personal information for the purpose of identity fraud. They can search the hard drives of stolen or discarded computers, hack into computers or computer networks to access computer-based public records, and use software. Malware to gather information to infect computers, also browse social networking sites or use misleading emails or text messages. (Kagan 2021) Identity theft may occur in several types or methods. So, this paper highlighted seven types or ways that the researcher found throughout his examined data, that deal with identity theft;

1. **Financial identity theft:** Someone uses another person's identity or information to obtain credit, goods, services, or benefits. This is the most common form of financial identity theft, either by obtaining a credit card number, bank account number, social security number, driver's license number, or any other information. (Siciliano, 2020)
2. **Social Security Identity Theft:** If identity thieves get hold of your Social Security number, they can use it to apply for credit cards and loans and then not pay outstanding balances. (Hussain 2022)
3. **Medical identity theft:** In the case of medical identity theft, a person poses as another person to obtain free medical care, and medical identity theft includes the fraudulent use of a person's health to receive compensation for health care services provided to an individual that is not meaningful in the document. (Frankenfield, 2021)
4. **Synthetic identity theft:** A type of fraud in which a criminal combines real (usually stolen) information with a fake one to create a new identity

which is used to open fraudulent accounts and make fraudulent purchases. Synthetic identity theft allows a criminal to steal money from any credit card companies or lenders who offer credit. Based on the fake identity (O'Shea, 2020)

5. **Child identity theft:** Someone uses a child's identity for various forms of personal gain, and this is common because the child usually does not have information associated with him that could pose obstacles for the perpetrator. The fraudster may use the child's name and social security number to obtain residency, work, obtain loans, or avoid arrest on outstanding warrants. Often the victim is a family member, the son of a friend, or another stranger of the perpetrator. (Kagan 2021)
6. **Tax identity theft:** Tax identity theft occurs when someone uses your personal information including your Social Security number to file a fake tax return or a federal tax return in your name and collect a refund. (Kagan 2021)
7. **Criminal identity theft:** In criminal identity theft, the offender poses as another person during arrest to try to avoid a subpoena, prevent discovery of a warrant issued in his real name, or avoid an arrest or conviction record. Criminal identity theft is often used to refer to a specific type of proceeding that involves criminal charges. (Bellemare, 2020)

Here, I have to mention that according to the federal Commission 2021 was the worst year of all time for identity theft in the United State of America in which 5.7 million Americans were victims of identity theft and fraud, and billions of Dollars were gone.

7.2 Fraud by mistake

The second method that a fraudster uses is fraud by mistake which happens when a person or a group intentionally and willfully gives false information to deceive another person or party. Karsten Witke also finds that some of the merchants surveyed refer to “individual fraud.” This seems friendlier than it is in reality: customers order and pay for goods or services, preferring to use a “withdrawal” payment method such as a credit card or credit card or Direct debit. They then proceed to intentionally return the amounts paid claiming that their credit card or account details have been stolen, they are compensated but they keep the goods or services. (K. Witke 2019)This method of fraud is particularly prevalent with services such as those in adult or gambling circles. It's the preferred place for criminals who use stolen payment data to pay for their purchases and don't send their data to their home addresses. Instead, they use brokers who use their data to make purchases and prices for sending merchandise. (K. Witke 2019)

7.3 Clean fraud

The term “Clean fraud” also known as sleeper fraud (Cox, 2022) that refers to any fraud attack appears to be legitimate most of the time a fraudster uses a credit card to make a purchase. This fraudulent operation doesn’t get easily spotted because they seem real. this method regularly uses real information that has been stolen, that why it seems genuine and, is not that easy to spot. The term clean fraud is misleading because there is nothing clear about it, the basic principle of clean fraud is to use a stolen credit card to make the purchase but then the transaction is manipulated in such a way that fraud detection functions are circumvented. The transaction looks very clean and will not be caught by fraud filters or blacklists. (Chargebacks911 2022)

Much more technical knowledge is required here than friendly fraud, where the only fraud is to cancel the payment once the purchase has been made. In Clean Fraud, criminals use sound analytics on widespread fraud detection systems, as well as a great deal of knowledge of the rightful owners of stolen credit cards. A large amount of correct information is then entered during the payment process in order to deceive if fraud is detected. Before committing a clean scam, cheap online trials are often conducted to verify that the stolen credit card details work. And successful clean fraud relies on one key component: legitimate cardholder data. The more data they can capture, the better. (Chargebacks911 2022)

7.4 Affiliate fraud

Affiliate fraud is a type of advertising fraud that involves any false or corrupt activity carried out by fraudulently offering to collect coins from an affiliate marketing program. Affiliate marketing fraud has always been an unfortunate occurrence in currency marketing, but it has become more complex since the advent of digital marketing. (Chen, 2020) marketers in 2020 are lost about $ 1.4 billion due to affiliated marketing fraud according to a study by CHEQ and the University of Baltimore, (Marciano, 2022) in the United States of America. Phishing scams are associated with early affiliate programs that paid for traffic, clicks, automatic page refresh, and the use of programs to click or send spam from a referral link.

Types of affiliate fraud:

Affiliate fraud remains a problem, and it evolves with the development of technology. This is the latest type of fraud.

1. Using stolen data to generate more leads or stolen credit cards to increase sales
2. Uniform Resource Locater (URL) hijacking domains close to the company name or its products, in order to capture referrals from redirects
3. Get people to download adware or spyware that automatically inserts affiliate code
4. Reproduction of the content of another affiliate site to steal the traffic center
5. The cookie embeds all visitors to the website for profit if the visitor later purchases something for reasons other than the basket
6. Traffic spoofing and software autofill are still effective fraudulent activities depending on the compensation numbers of a particular affiliate program. Chen (2020)

Traffic spoofing and software autofill are still effective fraudulent activities depending on the compensation numbers of a particular affiliate program. Here, one can say that affiliate fraud can take various forms, but the most common or known are cookie, fake lead fraud, and chargeback fraud.

7.5 Triangulation fraud

Triangulation fraud happens when a person makes a purchase on a third-party marketplace (such as Ali Baba, Amazon) but the product they received was fraudulently purchased from a different retailer's website. The third-party market palace seller, who is actually a fraudster makes an order with a legitimate retailer for the same product the valid customer order. This practice harms businesses of all kinds and customers are usually not aware of it. This name comes from the three-way relationship: the unsuspecting customer, the legitimate trader, and the fraudulent broker. (Triangulation Fraud, 2020)

1. A reassuring customer submits an order in an auction or market using some form of credit or debit or a bid from PayPal, for example
2. A fraudulent seller receives this order and then places an order for the actual product through a legitimate e-commerce website using a stolen credit card
3. A legitimate e-commerce site that then processes the criminal matter

Frequently, the person with the credit card details stolen gets hit with these charges, causing the original retailer to refund the purchase price. This type of fraud often occurs when cybercriminals create a fake or duplicate website and lure buyers with cheap goods. Sometimes these fake websites may appear in advertisements or be sent to users' emails directing them to the website through a phishing attempt. (Basul, 2017) Hence, triangulation fraud involves three parties, the fraudster, a buyer, and an e-commerce store.

7.6 Merchant Fraud

Commercial fraud can be very difficult to detect due to the complexity of the digital payments system (Teicher 2017). However, the work involved in detecting and preventing merchant-based fraud is nothing of value compared to the costs involved in dealing with chargebacks, fees, and Fines. Commercial fraud leads acquirers to liability for facilitating criminal activity, which puts them at risk of chargebacks, fines, brand or reputational damage, and prosecution even in legal proceedings. (Teicher 2017)

There are three types of commercial fraud:

7.6.1 Bust out fraud:

A bust-out fraud also known as hit and run, can happen on many types of financial services such as credit card scam.it is one's an individual wants a credit card, then starts a normal usage pattern and solid repayment history, after that racks up many charges, and maxes out the card with no intention of paying the bill. (Chen, Bust-Out Credit Card Fraud: Definition and Impact 2022) bust-out fraud starts with the criminals opening up credit card accounts with many different financial organizations. the danger for that organization that uses digital channels growing especially when they extend credit. Here, one has to mention that fraudsters most of the time use stolen identity data, and used it fast before the scheme is revealed, by the victim weeks after the fact. studies in the United States of America that were held in 2021 showed that 1.25 million US children were known to be victims of identity fraud. (Najarian, 2022)

7.6.2 Identity Swap:

Certain individuals who have been behind this sort of fraud are very much dangerous in their activities, they are using various methods, techniques, schemes, and instruments criminals use to hide launder or move illegal fund, for example individuals on anti-money laundering watch lists, traders from economically sanctioned countries, or individuals belonging to certain extremist groups are prohibited from opening trading accounts with large buyers. To circumvent these prohibitions, the Merchants often use a fake or stolen identity or create a fake online storefront to secure a merchant account. (Teicher, Three Types of Merchant Fraud: A Guide For Merchant Acquirers 2017)

7.6.3 Transaction laundering (also known as commission)

Transaction laundering, also earlier known as “undisclosed aggregation” or “factoring”, happens when a business method an unknown transaction on behalf of another business. (Role 2018) another meaning of transaction laundering lets criminals produce or build legitimate transactions as a means of cleaning illegal funds. The best definition that can one stated is that of Master Card as “the action whereby a merchant processes payment card transaction on behalf of another merchant.”

Although many industries’ initiatives emphasize scams and identity theft, in reality, a large percentage of financial losses are connected to operation laundering. An urgent and growing problem in the payments industry, where transaction laundering occurs when an unknown company uses the payment credentials of an authorized merchant to process Payments for products and services that the buyer is not aware of. The proliferation of small merchants and instant registration, as well as the proliferation of different payment methods, contribute to the increase in data load and the difficulty of monitoring the merchant's file. According to some estimates, $352 billion is laundered annually in this way in the United States of America. (Teicher, Three Types of Merchant Fraud: A Guide For Merchant Acquirers 2017) detecting and preventing transaction laundering presents important challenges, to individuals, groups, and companies.

8. Conclusion

This paper identified the most important fraudulent methods used by cybercriminals, and the most important factors that were and still are behind the spread of this criminal activity. The Internet is the mother of e-commerce fraud and, is a way to get a mass population without spending that much money within a short time. As the problem question of this paper stated above, fraud in e-commerce is electronic activity and is a multi-faceted and thorny phenomenon in order to follow up the activities of users and the activities of electronic fraud. The activity of electronic criminals, as we saw in the analysis, is linked to the emergence of the Internet in 1991, and after only two years it began to become increasingly active and flourishing according to the activity of commercial transactions, which also began to pursue the activity of electronic commerce. As we have noticed, fraud methods differ, depending on the sales channel, and most users, led by merchants, seek to achieve sales in multi-channel ways. We also concluded that electronic fraud in electronic commerce is not only in credit card payments, but electronic fraud has become more sophisticated in the use of malware to issue orders to log in to online banking services, phones, tablets, and computers, and this using stolen bank account details to conduct fraudulent payments. Electronic fraud has taken several methods and very complex aspects, which is why it is sometimes difficult to track electronic crime. The world of e-commerce fraud is in the hand of very intelligent fraudsters, they can strike individuals, groups, and companies, at any given time. However, it is not easy to protect ourselves from them, because we are unaware of the techniques and methods to discover them. Fraudulent action happens daily, sometimes unintentionally but most of the time intentionally.

9. Bibliography List :

Bacan, M. (2015, 4). *Card-not-Fraud (card not present transaction)*. Retrieved 03 19, 2021, from https://searchsecurity.techtarget.com/definition/card-not-present-fraud-card-not-present-transaction.

Basul, A. (2017). *5 types of fraud that is used to target 2-commerce retailers* . Retrieved from https://www.ravelin.com/blog/5-types-of-fraud-that-is-used-to-target-e-commerce-retailers.

Bellemare, J. (2020, 10 06). *Criminal Identity theft-are you at risk*. Retrieved from https://www.identityforce.com/blog/criminal-identity-theft-risk.

Cecile, F. E. (2019, 03). Evolution of E-commerce and Global Marketing . *International Journal of Technology for Business , 1*(1), 33-38. Retrieved 3 19, 2021

Chargebacks911. (2022, 10 05). *Clean Fraud*. Retrieved 01 27, 2023, from https://chargebacks911.com/clean-fraud/

Chen, J. (2020, 09 14). *Affliate Fraud*. Retrieved from https://www.investopedia.com/terms/a/affiliate-fraud.asp.

Chen, J. (2022, 06 20). *Bust-Out Credit Card Fraud: Definition and Impact*. Retrieved 01 1, 2023, from https://www.investopedia.com/terms/b/bustout.asp-0

Cox, M. (2022, 7 25). *What is FIrst-Party Fraud*. Retrieved from https://www.fico.com: https://www.fico.com/blogs/what-first -party-fraud

Frankenfield, J. (2021, 2 18). *Medical Identity Theft*. Retrieved from https://www.investopedia.com/terms/m/medical-identity-theft.asp.

Hussain, A. (2022, 09 21). *What Is Identity Theft? Definition, Types, and Examples*. Retrieved 1 27, 2023, from https://www.investopedia.com/terms/i/identitytheft.asp

Indraprastha, G. G. (2019, 02 10). *E-commerce; Meaning, Nature and Concept*. Retrieved 02 7, 2023, from https://theintactone.com/2019/02/10/ec-u1-topic-1-e-commerce-meaning-nature-and-concept/

J.Ohene-Djan, E. c. (2008). *Electronic Commerce.* London: University of London.

Kagan, J. (2021, 2 13). *what is Identity theft*. Retrieved from https://www.investopedia.com/terms/i/identitytheft.asp.

Kutz, M. (2016). *introduction to E-commerce. combining Business and information technology* . Hochschule Anhalt, Germany . Retrieved 03 17, 2021

Mady, J. (2020, 1 30). *the history of E-commerce: A long and a winding road* . Retrieved from https://www.the-future-of-commerce.com/2020/01/30/history-of-e-commerce/.

Marciano, J. (2022, 0 08). *The 8 Biggest Affiliate Marketing Fraud Case* . Retrieved from https://cheq.ai: https://cheq.ai/blog/8-biggest -affiliate-marketing-fraud-legal-case/

Martin, K. (2016). *introduction to E-commerce combing Business and Information Technology.* Hochschule Anhalt: Martin Kutz ans eBook Company.

Najarian, A. (2022, 08 17). *Bust-out Fraud, How it works, How to Prevent it*. Retrieved from https://www.outseer.com: https://www.outseer.com/payment-security/bust-out-fraud/

O'Shea, B. (2020, 7 28). *what is Synthetic Identity thedt?* . Retrieved from https://www.nerdwallet.com/blog/finance/synthetic-identity-theft/.

Role, A. (2018, 08 15). *What is transaction laundering and what is the Industry doing about it?* Retrieved 01 27, 2023, from https://www.paymentscardsandmobile.com/what-is-transaction-laundering-and-what-is-the-industry-doing-about-it/

Siciliano, R. (2020, 11 1). *what is financial Identity theft?* Retrieved from https://www.thebalance.com/identity-theft-and-affinity-fraud-4117147#:~:text=Financial%20identity%20theft%20is%20a,financial%20fraud%20or%20other%20crimes.

Teicher, R. (2017, 11 21). *Three Types of Merchant Fraud: A Guide For Merchant Acquirers*. Retrieved 01 27, 2023, from https://www.finextra.com/blogposting/14769/three-types-of-merchant-fraud-a-guide-for-merchant-acquirers

Teicher, R. (2017, 11 21). *Three Types of Merchant Fraud: A Guide For Merchant Acquirers*. Retrieved 01 27, 2023, from https://www.finextra.com/blogposting/14769/three-types-of-merchant-fraud-a-guide-for-merchant-acquirers

Teicher, R. (2017, 11 21). *Three Types of Merchant Fraud: Aguide for Merchant Acquirers* . Retrieved from https://www.finextra.com/blogposting/14769/three-types-of-merchant-fraud-a-guide-for-merchant-acquirers.

Triangulation Fraud. (2020, 11 25). Retrieved from https://chargebacks911.com/triangulation-fraud/.

Witke, K. (2019, 11 25). *The seven types of e-commerce fraud explained*. Retrieved 1 26, 2023, from https://www.information-age.com/seven-types-e-commerce-fraud-explained-1396/

Witke, k. (2019, 11 25). *The seven types of e-commerce fraud explained* . Retrieved from https://www.information-age.com/seven-types-e-commerce-fraud-explained-123461276/.

Zwass, V. (2016, Feb 10). *https://www.britannica.com/technology/e-commerce*. Retrieved 03 17, 2021