Project Dissertation on

Online Shopping Trend &

Fraud Attack – E-commerce

Submitted By:

Rishi Kalia

(2K19/EMBA/544)

Under the Guidance of:

Prof. Mr. Maheshwari

Professor

DELHI SCHOOL OF MANAGEMENT

Delhi Technological University

Bawana Road Delhi 110042

June 2021

CERTIFICATE

This is to certify that the dissertation report titled **"Online Shopping Trend and Fraud Attack - E-commerce"** is a bonafide work carried out by **Mr. Rishi Kalia** of **EMBA 2019-21** and submitted to Delhi School of Management, Delhi Technological University, Bawana Road, Delhi-42 in partial fulfillment of the requirement for the award of the Degree of Masters of Business Administration.

Signature of Guide **Signature of Head (DSM)**

Seal of Head

Place:

Date:

DECLARATION

I, **Rishi Kalia**, student of **EMBA 2019-21** of Delhi School of Management, Delhi Technological University, Bawana Road, Delhi – 42, hereby declare that the dissertation report **"Online Shopping Trend and Fraud attack - E-commerce"** submitted in partial fulfillment of Degree of Masters of Business Administration is the original work conducted by me.

The information and data given in the report is authentic to the best of my knowledge.

This report is not being submitted to any other University, for award of any other Degree, Diploma or Fellowship.

Place: New Delhi **Rishi Kalia**

Date: 04th June 2021

ACKNOWLEDGEMENT

I would like to express my sincere gratitude towards my Guide, Mr. Maheshwari (Professor, Delhi School of Management, DTU) for his support and valuable guidance throughout the duration of the project. I thank him for the constant encouragement and support at every stage.

My sincere gratitude goes out to my colleagues whose participation in the project gave many valuable inputs for its completion.

Rishi Kalia
(2K19/EMBA/544)

ABSTRACT

The volume of electronic transactions has raised significantly in last years, mainly due to the popularization of electronic commerce (e-commerce), such as online retailers (e.g., Amazon.com, eBay, AliExpress.com). It is also observed a significant increase in the number of fraud cases, resulting in billions of dollars losses each year worldwide. Therefore, it is important and necessary to develop and apply techniques that can assist in fraud detection and prevention, which motivates our research. This work aims to apply and evaluate computational intelligence techniques (e.g., data mining and machine learning) to identify fraud in electronic transactions, more specifically in credit card operations performed by Web payment gateways.

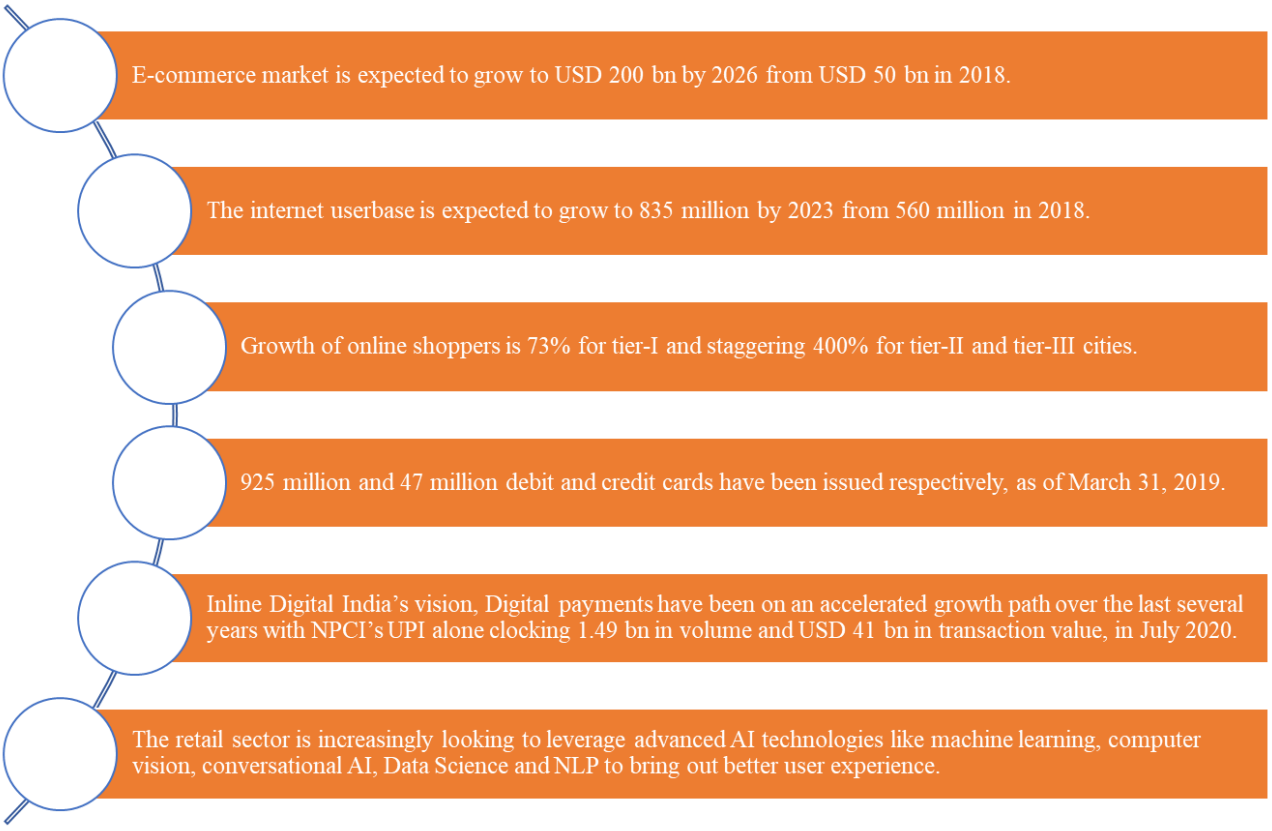
2020-21 has been marked by significant global commerce changes due to the overwhelming impact of the outbreak of Coronavirus (COVID-19). Online consumer volumes have fluctuated considerably, impacting how merchants approach their business practices and effecting how and where fraud and abuse occur. Fraud Attack Index captures in e-commerce transactions and the ability to identify unique users across a robust network. This report tracks and explains these changes amid an unprecedented time of global commerce.

1.INTRODUCTION

Digital payments have made payments and transactions easier in today's connected world. Technological improvements, Internet penetration, mobile phone uptake, online payment use by consumers, SMBs, and banks alike, and new solutions such as UPI, IMPS, wallet integration, and so on have all contributed to India's enormous growth and presence of conducive environment by policy makers and Government to transform India into a less cash economy.

However, as an unforeseen consequence of the progressive momentum, the danger landscape has become more dynamic. This requires all stakeholders in the payment ecosystem to work together to reduce the number of frauds and payment scams. This collaborative study aims to address the growing concerns and underlying causes.

The report attempts to discuss about the online shopping trends, sophisticated online payment frauds, the threats in the payment ecosystem, the importance of incorporating better fraud prevention strategies and recommendations for various stakeholders involved in the payment ecosystem.



2.Objective of the study - Rationale

My research is to identify how customers respond to online shopping, their reaction to the various categories of merchandise, electronics, appliances, etc. Also, to understand the cases of online fraud. For this we will gather and study research papers and through a survey we will consider various attributes that would decide the buying behaviour of the customer and how much do they value the marketing strategy of e-commerce platforms. We will use the exploratory research methodology to investigate the behaviour of the variables and their interactions in this study. Before attempting to quantify mass responses into statistically inferable data, researchers use exploratory research to gain a better understanding of a topic. Data will be analysed both qualitatively and quantitatively. We'll create a statistical model after deciding on dependent and independent variables. The sample size taken was 30 participants.

- Are you
  Male - 20
  Female - 10

- Age group
  Below 30 - 7
  Below 40 - 20
  41 and above – 3

- Status (Marital)
  Married - 21
  Single - 9

- Which e-commerce website do you frequently use?
  Amazon - 20
  Tata Cliq - 2
  Flipkart - 8

- What e-commerce website do you find user friendly?
  Amazon - 25
  Tata Cliq - 4
  Flipkart - 1

- Which category of products do you mostly procure?
  Electronics (TV, cell phones, appliances, etc)- 6
  Computers and accessories - 4

Clothing and accessories - 10
Footwear - 10

- How often do you shop online?
  Daily - 1
  Weekly – 9
  Monthly - 15
  Yearly - 5

- How much do you spend on an average in a month on online shopping?
  Less than INR 5000- 15
  Less than INR 7000 - 7
  Less than INR 9000 - 5
  Less than INR 12000 - 3

- What is your preferred payment mode for online shopping?
  Debit Card- 2
  Credit Card (Visa, Mastercard, Am Ex) - 12
  Cash on delivery (COD)- 10
  Patym, UPI, etc - 6

- What do you think is the most important aspect of an online shopping site?
  Security – 90%
  Privacy – 10%

3.0 Reasons for growth in internet usage

The number of people using the internet is increasing

Access to the internet within the country is growing rapidly, crossing 481 million in 2018 and is predicted to hit five hundred million users by June 2020. “AIMIA” report highlights that urban India’s web penetration was sixty four.84 per cent in Dec 2018, as compared to solely twenty.26 per cent in the rural part of the country. With rural populations accounting for about a third of city populations and goods being affordable, online usage in the interiors of the country is likely to grow at a rate never seen before.

Effect of mobile

It is not a tool used just for human activity it's become a mode that additionally helps the web shopper with various choices. shoppers are becoming comfy shopping for product and other services through numerous mobile applications that ar accessible, therefore creating online shopping a feasible business chance for companies.

Dialectal variety

Use of the countries regional dialects by merchandisers has also lead to regional consumers exploring various ecommerce platforms, thus making shopping an easy activity. More than, ~200 lakh users use languages other than English online, in comparison to ~175 lakh English language users.

The emergence of social commerce

A platform that supports transacting based on social connections and user experiences is known as social commerce. As a multi-cultural society, India is required to embrace the concept of communal buying and selling. With the capacity to provide a wide range of options, as well as shared user experiences and referrals, this industry is projected to have a big impact on customer decision-making.

Union of customers due to technological advancements

With the number of smartphone users projected to rise, ecommerce platforms will benefit from increased internet usage. Ecommerce organisations must now plan for flexible ecosystems that allow customers to transition from entertainment to information and then to online transactions. In addition, a number of businesses can now combine traditional products and services with technology to make them more desirable. Also, with the use of technology, companies are able to make traditional items more tempting and suitable for consumers.

The popularity of digi wallets is expected to continue

In the foreseeable future, significant expenditures in digital media across languages is projected to rise. According to a recent study, more than seventy five percent of Indian language internet users prefer mobile wallets to bank-sponsored websites and applications. Furthermore, the Indian government's push for digital programmes is projected to increase digital adoption and outreach.

4. Types of payment fraud

The multiple methods of payment fraud include:

- **Phishing:**

  The technique of sending emails that appear to be from trustworthy companies in order to get people to divulge personal information like passwords and credit card numbers.

- **Identity theft:**

  Identity theft is the theft of another person's personal or financial information in order to conduct fraud using that person's identity, such as making illegal transactions or purchases.

- **Pagejacking:**

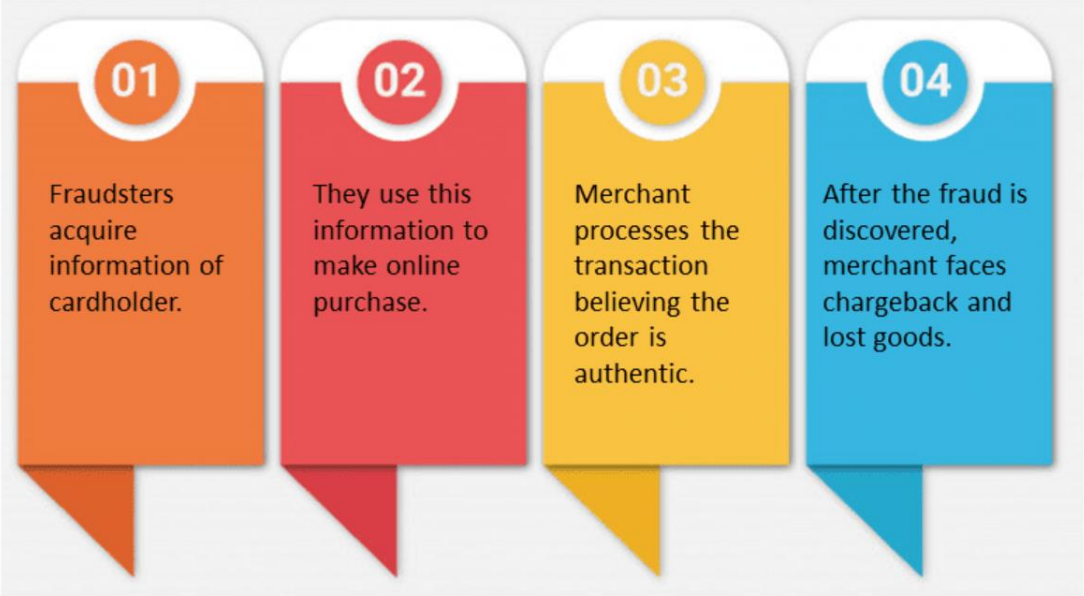
  Pagejacking is the unauthorized copying of valid website material (typically in the form of source code) to a new website intended to look like the original. A fraudulent page-jacker does pagejacking by copying a favorite Web page from a credible site, including the HTML code.

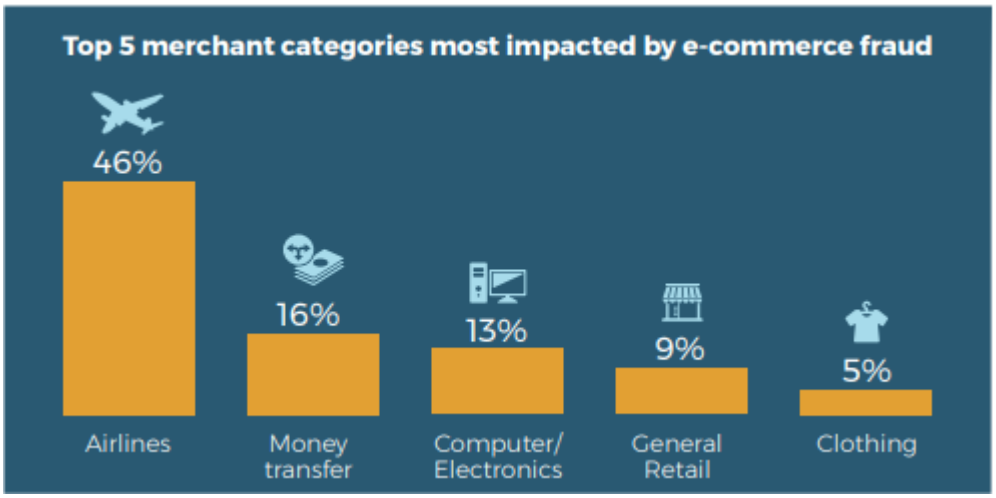
- **Scams involving online payment transfers:**

  Credit card users and ecommerce store owners are targeted by hackers who pose for cash in exchange for a card or cash at a later date.

- **Identity theft by merchants:**

  Criminals set up an account on behalf of a superficially genuine business and charge stolen credit cards using this method. The payment facilitator is liable for the loss as well as any additional credit card chargeback fees if this occurs.


01
Fraudsters acquire information of cardholder.
02
They use this information to make online purchase.
03
Merchant processes the transaction believing the order is authentic.
04
After the fraud is discovered, merchant faces chargeback and lost goods.


Top 5 merchant categories most impacted by e-commerce fraud
46%
16%
13%
9%
5%
Airlines
Money transfer
Computer/ Electronics
General Retail
Clothing

5. Applying technology to prevent online fraud

- **Ensuring login credentials for customers are secured:**

  Accepting payments through client login and eliminating victimization checkout through a guest profile will facilitate scale back fraud incidence. Purchasers should be ready to firmly log in with their own credentials. this may aid in activity analytics to sift out questionable accounts and make sure that dangerous actors area unit stop working before they are doing damage.

- **Use of 3D secure protocol:**

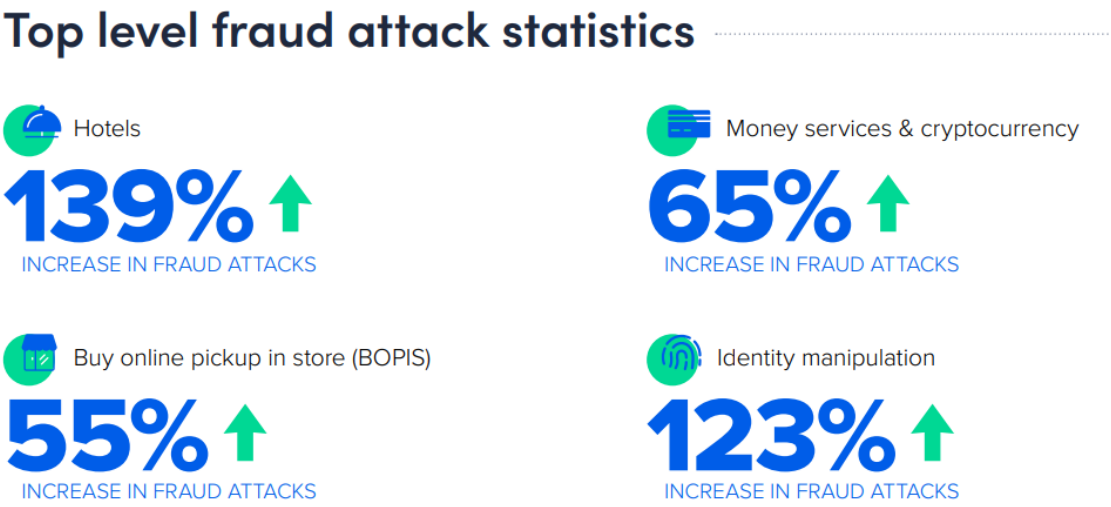
  EMV can without doubt still push fraud to the CNP (Card Not Present) channel wherever there's low hanging fruit for dangerous actors. Combining a comprehensive fraud hindrance strategy with the 3D secure tools offered by the cardboard brands will guarantee retailers or merchants area unit on the correct aspect of the liability shift for such transactions and scale back prices related to manual reviews and interchange rates.

- **Adapting ML with human intervention:**

  As datasets grow larger, advanced machine learning can take the wheel. As a result, it's become incredibly difficult for businesses to efficiently analyse and draw conclusions from this data. While modern machine learning automates these operations to make the process easier and faster, understanding fraud data within the system requires human participation or manual fraud information review capabilities context of however fraud has wedged the online business and client expertise. The e-commerce business and client expertise have been wedged in the backdrop of how fraud has wedged them together. This technology is critical to a variety of critical business problems, but fraud prevention is one of the most significant applications, especially in light of various security and fraud prevention trends into the New Year. Pursue omnichannel customers while keeping an eye on the competition.

- **Useful fraud detection methods:**

  A few security firms have responded to the growing threat of online or e-commerce fraud by inventing new fraud detection technologies and enhanced MFA approaches, such as OOB (Out-of-Band) authentication and exploiting biometric technologies. However, there is a negative side to using technology. As payments technology advances, the Internet of Things (IoT) can help to strengthen security risks.



6. Techniques for Fraud Prevention

Serious competition between players & the trade has seen a general rise in acquisitions. high players ar facing smaller rivals to increase their market share, in many cases influenced by international investors. Speculations supported international trends hint at possible mergers or acquisitions among firms in duopolistic segments of the market. Unrelated variations have in addition started gathering steam as e-retailers unit presently creating a shot to verify a stronger reach and connect with customers. this might probably end in a stronger influence in their future purchase decisions. These companies come from a plethora of industries, like sensible wearable devices, information analytics, game content creators and much of further personal labels promoted by leading platforms area unit on a rise where in there is very important investments by the leading players in categories like fashion, electrnics, home appliances and accessories.

7. How does fraud impact e-commerce businesses?

Consumers are transitioning from brick and mortar stores to online stores as technology advances and the number of internet users grows. Ecommerce is a popular trend among today's merchants. According to Javelin Strategy's analysis, ecommerce transactions accounted for 9.1% of total retail payment volume in 2015, and this figure is predicted to rise to 12.4 percent by 2020.

However, merchants' ability to manage fraud will be harmed as a result of this evolution. Meanwhile, fraudsters are honing their skills and focusing their efforts on online retailers. As a result, all merchants are incurring higher expenses, such as product loss, financial loss, and harm to confidence and reputation.

- **Product Loss**

  This damage is more serious for merchants who sell high value physical products such as Amazon, Microsoft. Etc. Normally, fraudsters get those products and resell in the market to earn money without too much cost involved. Merchants are the one who absorb the cost of goods sold and incur no profit for the goods.

- **Financial Loss**

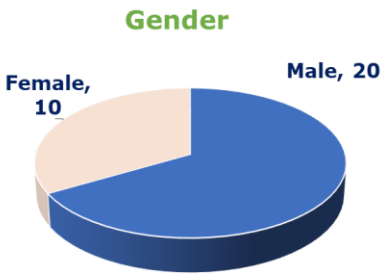
  Depending on each merchant, they have different elements when evaluating the cost of eCommerce fraud losses. Financial loss refers to charge back cost involved after fraudulent event.

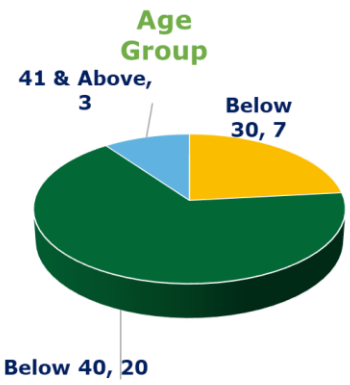
- **Reputation**

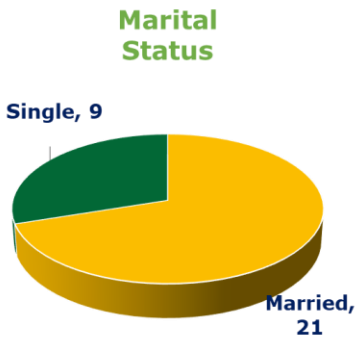
  Customer experience is always priority of merchants especially in Ecommerce platform. When customers do not actually make the purchase and the card is charged by your merchant, they will lose their trust and give up buying or providing their information. This will affect customer loyalty and long-term relationship with merchant.

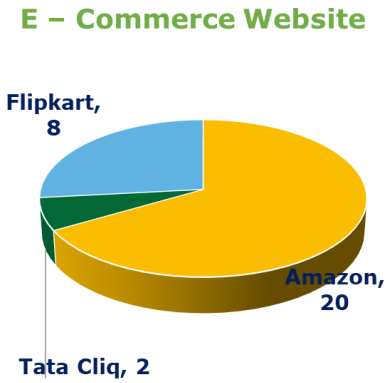
7.0 Conclusion

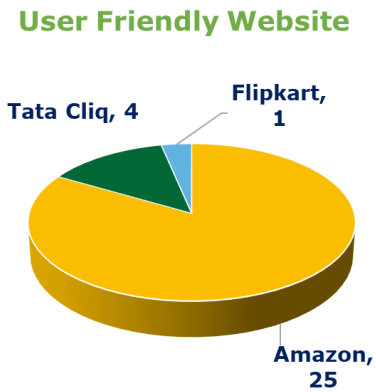
This section highlights the study's goals through critically assessing qualitative data and thoroughly assessing interviewee replies and beliefs. This was accomplished by examining the most important responses provided by the participants. In order to meet the study's analytic purpose, the data was analysed and mentioned by comparing the respondents' comments with the literature review. As a result, the analysis' explanation is based on the respondents' private answers. The primary data for the study was gathered using a well-designed form. The data from 30 respondents was structured uniformly in tables and graphs and then subjected to analysis using appropriate applied statistical methods.



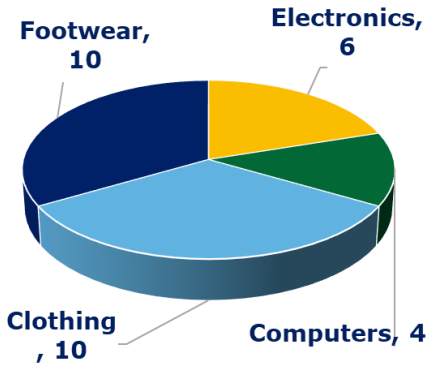




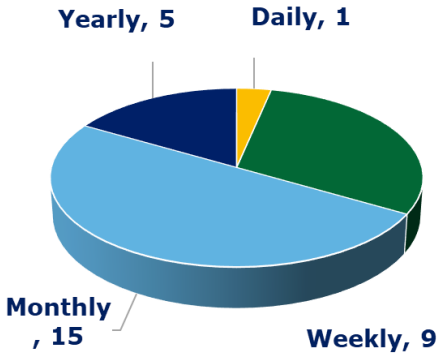




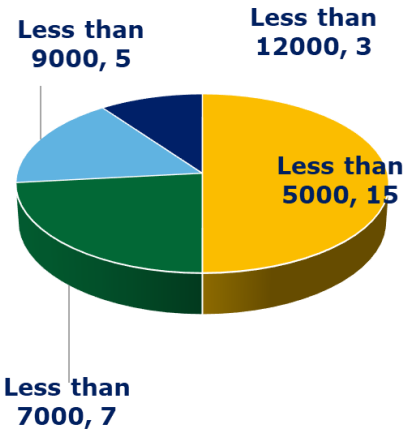
Products Procured



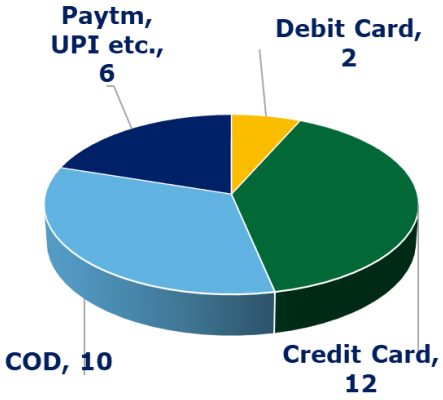
Often do you shop online



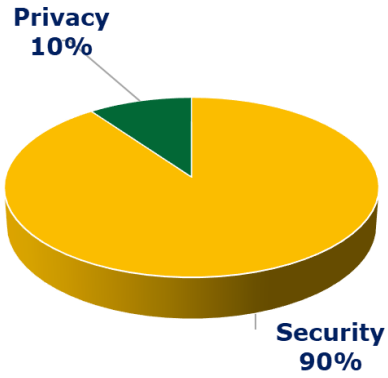
Average Amount Spent



Method of payment



Important Aspect



8.0 References

1.) https://www.researchgate.net/publication/287299598_Fraud_Analysis_and_Prevention_in_e-Commerce_Transactions

2.) https://issuu.com/sanjaykumarguptaa/docs/project-report-on-e-commerce

3.) https://www.enterprisetimes.co.uk/2020/04/22/forter-publishes-report-on-covid-19-impact-on-fraud-and-consumer-behaviour/

4.) https://www.forter.com/blog/ninth-fraud-attack-index/

5.) https://unctad.org/system/files/official-document/ecdr2001_en.pdf

6.) e-commerce-retail-logistics%20(1).pdf