Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 04 | Issue 02 | October-2021

An Analytical & Statistical Approach for the Identification of Online Payment Fraud

Gopika Baghel[1]

Available online at: www.xournals.com

Received 17th August 2021 | Revised 18th September 2021 | Accepted 30th September 2021

Abstract:

The mechanization of online payments is growing tremendously. As this technology increases, the rate of fraud due to these online payments is also increasing. Nowadays, online payment has started everywhere. Online fraud has flattered a crucial issue in numerous countries & India is either of them who is having a wide diversity of scams related to online payment. The objective of this paper is to explore the category of online money fraud related issues. The paper surveys why victims fall for web scams. What type of procedure online criminals are adopting to trap their prey, also the kind of payment methods they are using for fraud and what methods people are applying to prevent these crimes? Also, how police officers/cyber cells officers are active in solving these online payment crimes.

Keywords: *Payment frauds, Online Banking, Customer trust, Countermeasures, Fraud prevention, trickery.*

Authors:

1. *Dr. Babasaheb Ambedkar Marathwada University Aurangabad, Maharashtra, New Raipur, Chhattisgarh, INDIA*

Introduction

Online money transfer is increasing & growing quickly across geographic & industries. Instantly as an emerging technology or process is deployed to prevent trickery, the impostor finds a weakness to accomplish or alternatively focus their notice elsewhere. Transactions done using online methods are very well liked these days. This thing is also a good profitable medium for financial institutions. This online money transfer system is cheaper when compared with the conventional banking system & it offers customers flexibility & comfortability. It shows a wide number of advantages, including price value and time savings, increased sales and reduced transaction costs. But it is easily accessible to internet fraud and could potentially increase business expenses. Online payment scams is an unlawful operation, which occurs via the World Wide Web. The fraudsters have created different methods to embezzle and steal crucial information. Online parody & phishing are some of the ordinary remittance fraud types. These trikery are responsive to the increasing number of untruthful activities due to greater depth & breadth of facts collected from all e-banking & e-commerce websites, across the world. The detection systems for online banking require a compulsory protocol to prevent & detect fraud, also mitigate threats concerning unusual payment transaction patterns. Fraudulent activities & data breaches are growing revenue losses through millions of monetary transactions per day through several channels, owing to rise in digitalization & internet penetration. On the flip side, growth in the adoption of Artificial Intelligence (AI) & Machine learning (ML) to handle payment gateways is anticipated to fuel the rise of the online money fraud detection market over the forecast period. Consumers are now worried about the safety of their bank accounts, money & their private information to not be leaked. They are anticipating the bank & Cyber security expert to find a solution that can protect them from this payment fraud. The COVID-19 pandemic has begun & grown new avenues for imposters tricky to hood wick unsuspecting customers. Many purchasers have departed online payments for items extending from groceries to account payments due to reduction in movement placed to control the spread of the worm. A repercussion of this has been expanded frauds. There are different modes of payment: Money transfer through the computer machine. Automatic teller machine (ATMs). Various types of cards: Credit & Debit cards, Smart cards, Super Smart Cards, Optical Memory Cards, etc. Internet (Google pay, Paytm, Paypal, UPI (3rd party) & 8 Mobile wallets, Pay Later, e-Wallets. Crime associate with these modes of transfer of money are: Diversion of money from rightful to fraudulent payee · Credit cards are copied & data misused. Credit cards are stolen· Unauthorized person uses lost credit cards · White cards are used in place of originals· Wires are tapped & necessary data stolen to operate ATMs account · Withdrawals & deposits are manipulated to other accounts Tele-marketing money is transferred from the victim accounts without providing the promised goods rate. Governance, risk & compliances is anticipated to drive the online payment detection market. Corporeal systems authorize data analysis & deliver triable insights in order to meet purchaser demands. Web based profession mainly depend on online transactions for their amenity & outcome delivered. Trickery that include trader & triangulation frauds, petty lancery, countermove, page jacking, clean & affiliate sharp practice occur during transaction. The biggest challenges faced by different administrations is the insufficiency of skilled resources to handle trickery activities, which is disturbing their ability to advance Information Technology security needs. Many firms hire security researchers & experts who dearth the appropriate expertise to recognize & analyses developed live through threats while experiencing a cyber-attack.

What Is Online Payment Fraud? Money fraud happens when online purchases are made illegally. The sufferer here is commonly a consumer- fraudsters loot their delicate information, credit card information, their recognition etc., & then utilize it to make snap up. E-Commerce is based on the internet transactions, where customers are paying for products and services. It’s not hard to deduce the growing vogue of online stores. The fraudulent activities are increasing. The thing is that fraudsters also might contact the credit card owners to request crucial information in a ticklish way. They can steal the private facts by sending them an email or SMS (known as phishing), & also redirect them to a fraudulent website, or even give them a call. Cyber-thieves are looking for catches or speckles that weren't refurbished for some time. They use these gaps to get access to sensitive information. Mobile Money Fraud is a budding Problem Mirroring the speedy increase in the demand of cell telephone payments, it is obvious that online trickery is expanding quickly beyond traditional PCs to mobile and other devices, which will likely hasten in the future. Although the combination from cell phone malware has increased day by day over the recent few years, cell phone security is not yet equivalent to traditional device security. For occurrence, security software is slighter common in cell phones, Operating systems are modernized less habitually and cell phone public networking applications occasionally lack detailed privacy buffers. The number of fraudulent practices is growing.

Identity Fraud is the fraudulent acquisition and use of sensitive personal information, such as national identification numbers (e.g., social security numbers), passports and driver's license. This information enables a talented thief to assume a person's identity and conduct numerous crimes. These are the most similar fraudulent scenarios, but you need to get ready for some more absurd situations. When you run an online trade, you must consider how you'll be acting in cases like those above. The thing is that customers are not always right and you must protect your profit. Biometrics is particularly applicable to smartphones, many of which are equipped with iris fingerprint and facial recognition and can also analyse the phone user's voice. Several of the highest FIs have already launched biometric-based identification and authentication solutions in their product. Although crimes via smartphones increase at a faster pace than normal PC or laptops-based crimes, smartphones have the power to become as secure a channel because the web makes use of new strengthened encryption & authentication technologies. This involves leveraging key smartphone sensors as accelerometers, cameras, GPS receiver, microphone and fingerprint/iris sensors to provide advanced biometric security. The biggest contender in monetary services, E-Commerce and purchaser computerized industries, such as Samsung, Microsoft, and MasterCard. They have already started to use biometric verification as a renewal for password, thus following in the footsteps of Apple which has featured biometric identification in its smartphone products since 2013 **(www.experian.com, 2020).** E-Commerce CNP transactions. The main motorist beyond fraud in E-Commerce and web banking are: Growth in E-Commerce has become mainstream and is forecast to expand rapidly during the next few years. Factors driving extension include advanced shopping, payment options and brands pushing into new international markets.

Increased use of online mobile payments - The increasing use of smartphones for payments is a significant factor driving the volume of E-Commerce sales, particularly in emerging markets.

In developing countries with immature payment services and limited fixed line Internet penetration, people are increasingly using mobile phones to erupt the Internet, shop and move money. In a few of these markets, mobile may be the earliest channel for these activities. Increased number of serious data breaches - Scams trends are broadly driven by the vast quantities of identity detail facts available to cyber fraudsters after data breaches. Successive information fact breaches covering many organisations mean scammers can now boost very complete identity information on their sufferers. The web facts are affluent enough for them to appeal for and successfully unlatched a bank account in the sufferer’s name. That's why there is such an efflux in bank account application scams. Fraudsters are more and more focusing their efforts on obtaining personal information and financial details from individual bank account holders rather than obtaining this data by directly attacking the banks **(www.experian.com, 2020).** The contemplate was carried out online. Close to 17% of those occurrences have been within the last month. When asked about web based payment fraud risks, fake apps & websites are the biggest, according to 52% of respondents, followed by compromised password/credentials information (43%) & spyware/malware (39%). Nearly around 75% recognize a one-time password as a key of an anti-fraud mechanism deployed by their bank, according to study **(ciso.economictimes.indiatimes.com, 2020).**

Both the customers and vendors suffer when card not present & fraud occurs. In the recent past years, after the mandate of two-factor verification from the Reserve bank of India, the no. of such 'card-less' or 'card not present' transactions have marginally gone down. However, due to the rise in SIM swaps and skimming, the percentage of such frauds could potentially rocket. Investments in next-level verification methods, communicative biometrics, multi-layered authentication, and real-time observation of frauds are some of the tools that will come to the fore in the future and can be leveraged to reduce frauds and continue to instil in consumers' confidence in digital payments. Although the number of bank trickery detected increased by 45% in FY19 as compared to FY09, the value of money involved adulterated 35 times in the same period. The average allotment of fraud has increased over the previous decade, from 0.4 crore in FY '09 to 10 crore in FY 19. Loan quandary - Loans (advances) constituted the highest number and quantum of frauds in FY '19 among all categories of fraud. Public Sectors Banks accounted for the highest number of frauds & quantum (90.2%). In the chart on the right, each circle represents a set of banking institutions, while the size indicates the average amount per fraudulent transaction in FY'19 **(www.thehindu.com, 2019).**

Law for Cybercrime

The Information Technology Act, 2000 together with Indian penal code (IPC) has sufficient provisions to act towards prevailing cyber-crimes in the country. The act provides for penalizing in the manifestation of incarceration fluctuating from 2 years of life

incarceration & fine/penalty depending on the kind of cybercrime.

Countermeasures

To Analyze & record how the majority of the population get trapped in online payment frauds. I had performed a short survey with the assistance of Google form. Total 350 people responded from different depictions of India where the majority of the population belongs to Chhattisgarh State, they shared their experience & view on web payment services through various mediums like Google pay, PayPal, Paytm etc. Below are some important feedback information collected from their responses.

Out of 350 responses 200 belong to Male respondent & 150 belong to Female respondent of different age groups. Classification of their age group shown below in the bar graph. From the above graph it is perhaps clearly shown that majorities of people belonging to the 18-30 age group that specify youth are more involved in online payment methods as compared to other dotage groups.

As per their Educational qualification is concerned out of 350 respondents majority of respondents are graduated from respective universities with different streams. Many of our respondents use internet banking, in which 72.6% i.e., 254 respondents prefer internet banking over other conventional payment methods. And 27.4% i.e., 96 respondents don't prefer or trust Internet banking.

To get feedback about how they feel about internet banking, I had asked them what are the main reason they don't prefer the use of online web banking over other conventional payment methods in which 253 people responded out of which 2% people never heard about internet banking 19.8% i.e., 50 people are not technically aware about how to use internet banking. Out of 350 responses 57.4% i.e., 201 people use online payments for money transfer, 70% i.e. 245 people use it for shopping, 22.9% i.e.,80 respondents use it for business & rest of them use it for other transactions, data shown below in graph, Out of 350 respondents maximum no. of people use credit/debit card for web payment on monthly basis i.e.,42%, & 38% respondent use electronic bank transfer mode on monthly basis, & rest of my respondents use different modes of payment. It is very interesting to know that 91.1% i.e.,319 respondents are aware about online payment frauds & 34 have lost their money due to digital fraud & also 333 feels that internet banking has made their life easier as compared to earlier modes of transaction.

I asked them to tell how satisfied they are with online payment transactions using (Paytm, BHIM UPI, Google pay, Airtel payment bank, etc.) Also most of our respondents are not limited to a single payment app. Out of 350 respondents few have been sufferers of web payment scams.

Types of Scams No. of respondents affected: Phishing scam 28% Email scam 16.6% Fake website scam 26.3% Credit card scams 12.9% not applied 30.6%. Table showing range of amount in INR people lost while been victimized during online payments, Online payment apps are user friendly & very popular in-spite of that majority of our respondent don't trust them the graph showing height of trust on the extent of 1-5, It was surprising to know that after losing such a valuable amount most of our respondents are not comfortable in filing police complaints.

How they believe on the proportion of 1-5 that their problem gets resolved where 1 being the least & 5 is the high level of trust. As the popularity of online payments are increasing more & more users are getting used to it & proportionally frequencies of fraud are also increasing to measure the prevalence of fraud, I had asked my respondents how often they hear about online web payment crime.

We can clearly measure how alarming the situation is & how much we are prepared for it. To examine the height of awareness of my respondents while doing online payment & cyber-crime related to it, I had asked them a few security checks questions. Above survey of a very small group of people as compared to one hundred thirty-five crore population of India can depict both advantages & drawbacks of using online payments & how necessary it is to tackle this fraud.

Result and Discussion

Cybercrime has become a big issue for the world. Day by day its increasing number of Cyber Crimes take place because of the awareness and less techno friendly people, due to these cyber criminals taking advantage and committing the crime. To prevent all this kind of crime we have to implement several security measures, they are:

1. For the crime which has been committed we need to generate a security architecture for investigation or pre-incident procedure that quickly takes action against the crime. They imperative have the sufficient investigation authority to demand the data for investigation inside the legal boundaries. A specific team must be created that is purely responsible for the invitation against financial fraud.

2. Awareness is a solitary key factor which is missing nowadays, people are adopting new technologies but they are not friendly with them. They themselves don't know about the security structure and how to secure themselves, the companies are less focused on Awareness of security of uses before establishing an emerging technology & to adopt an innovation technology with a proper training under guidance should be conducted. Training sessions for awareness of online crimes should be conducted every week. Updating the laws should be checked to prevent modernistic crimes related to cyberspace as they weigh up to and including the trend of crime. The law system must be modernized to prevent those crimes and take appropriate actions against it. Internet banking transactions come with its share of defects and it is important to be aware of precautions that can assist you avoid landing in any unbidden situation. Never use or share devices when accessing your account. Keep redundant backups - It can also be uncommonly frustrating to go through a data security breach where extra damage is also happening to your digital device. In a few cases, fraudsters may even malevolently damage or wipe data. By keeping redundant backups every day, you definitely reduce the damage associated with a hacker and any subsequent data loss. Once the breach has been addressed, you can restore from your new backup and focus on getting back to business while further improving security. Do not click on channels received through SMS.

3. Rely on official websites or your bank branches to complete the process, if required. Transact payment only through the official Bank, BHIM or UPI applications. Never use links sent by an unknown person, even if they seem genuine. Look for verification by twitter blue ticks while interrelating with National Payments Corporation of India, bank or payment wallet helplines. Don't take help from strangers to complete payment transactions. Never download applications, except official play store ones, endorsed by seemingly obliging people, even if they assert to be bank officials. Use of newer mechanization calls for additional caution.

Since Unified payments interface based applications allow push (send/pay) & pull (collect/receive) payment transactions, new users could get demented. Recognize the procedure thoroughly before hurrying to use them. Never believe your caller ID. Prevent paying ahead of time for a promise: if someone asks you to pay before work for things like debt credit relief & loan proposal, mortgage encouragements, or a job. They possibly even say that you have achieved an award, but initially you have to pay a fee or taxes to get it. If you pay them, they will probably take the amount & disappear. Talk to a trusted person before you give up your money, private information, talk to someone you believe. Swindler wants you to make a commitment in a hurry. Consult an expert. Use a card processor with address and card verification - The more forgery detection systems you have available, the less likely you are to have chargebacks or have customers extract advantage if their personal information is stolen and attempts to purchase are made with your store. Enable an address verification system (AVS), and need the card verification value (CVV) for credit card transactions to reduce fraudulent charges. You can additionally tighten security, here, by requiring a partial or complete address and zip code match during checkout. Regardless of how reputable your eCommerce platform host is, you should perform regular quarterly PCI scans. These scams identify risks and vulnerabilities that could leave your store open to hacks and the injection of malware and viruses. A few extra hours adjusting your code with a developer today could save you twenty of thousands of INR down the road. Never access your bank account using vital passwords at web parlours or any other popular spots to avert the peril of data being mimeographed. Change your passcode frequently. Never reuse the same passcode entirely on your internal systems, especially where there are public-facing logins and, especially, not for administrative accounts. It's best to generate a unique passcode for each & every of your systems, and then set up a schedule for updating passwords. You can also use a passcode manager to originate passwords from an encrypted vault where your sites are only accessed locally and only with a master password. This ensures a unique different password is generated for every site. Communicate to your bank instantaneously if you doubt any substitute in your banking passcode. Set alerts - If your payment device allows you for it, you should configure an alarm using a number of varieties to trigger the alert.

These could include:

a. Orders placed from foreign IP addresses
b. Mismatched billing and customer data on the card.
c. Multiple orders placed on the same card, different orders from the individual using different cards.
d. Conflicting shipping and billing information.
e. Mismatch on customer name vs. cardholder name.

Every Time log-off from your online banking account and finish the web browser after getting the information. With two-factor authentication, even with a compromised password you'll be needed to provide additional information and login confirmation via another channel, such as email, messages, or even phone. Set this up in your E-Commerce platform like Shopify, on your social accounts, and on any other business app you possibly use-especially if it's installed on a mobile device. Help customers be more secure - While customer security is somewhat out of your control in regards to how they protect themselves, you can take extra steps to help them. You should also consider requiring stricter password parameters, like requiring a number, a capital letter, and a symbol within their password. Storing customer and credit card information leads to exposing you and your customer's information, with subsequent great risk. Simply put, never store customer credit card information in any shape. In order of priority to get this accreditation, your site must complete an audit and be found to follow a no. of standards, including:

a. Maintaining an established network with IT professionals,
b. Protecting bank cardholder data at every touch point, ensuring it's not stored.
c. Maintaining a liable management program.
d. Designating superior measures for access control.
e. Performing routine network inspections and tests.
f. Having and maintaining an information security policy.

In the current situation, each & every Indian bank has this prerequisite of web based banking. Nowadays, most of the banks are extending their reach in rural places to enchant more purchasers. This will help our country's entire people to benefit with the advancement in technology. These positive steps of the treasury to educate people about internet banking will contribute in reducing the risk of web based transaction scams.

Conclusion

Online payments are the easiest & most convenient method of the future. Almost all of the businesses now use online methods for selling to provide a better solution. Above open up the considerable activities on online payment frauds, people are now familiar with distinct kinds of fraud/scams, how people's attitude plays a vital role in the increase or lessening of web based banking sector frauds. Criminals can trick customers in many ways to acquire their bank account details. There is a quick increase in growth of online transaction systems. This type of activity has negatively affected customer trust towards online payment services, we can clearly depict that from the above survey. With the growth of these fraudulent activities this online banking sector is working hard to reduce these scams & frauds by implementing unique security protection like Two-factor authentication, as well the introduction of spyware that protects one's network against hacker's network. From the above study, I had concluded that advanced technologies play an important role to reduce the risk factor of validate systems.

References:

Ciso, E. *"Nearly Half of Consumers Worried about Frauds in Digital Transactions: Study."* ETCISO. 14 May 2020, Accessed Date 24th June 2021, Accessed from http://ciso.economictimes.indiatimes.com/news/nearly-half-of-consumers-worried-aboutfrauds-in-digital-transactions-study/75729404

Juniper Research. *"Online Payment Fraud Whitepaper"*, 2020, Accessed Date 24th June 2021, Accessed from https://www.experian.com/assets/decision-analytics/white-papers/juniper-research-onlinepayment-fraud-wp-2016.pdf

Krishnan, V. B. *Bank frauds up by 45% in 10 years, show data.* The Hindu, 9 Oct. 2019, Accessed Date 24th June 2021, Accessed from https://www.thehindu.com/news/national/bank-frauds-up-by-45pc-in-10-years-showdata/article29625654.ece