Cyber vs Regular: A Comparison of Consumer Fraud in The United States

***Abstract*—Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.**

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

I. Introduction

the main contributions: Understanding the differences in the nature of cyber and regular frauds in the United States. Exploring if certain demographics are more succeptible to cybercrime Suggesting improvements that might be the right way to create more awareness annd campaings.

Fraud and and deceptive practices have been around since the establishment of

The FTC and the FBI

The categories of the fraud

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Data Field	Field Description
Agency Name	All the complaint collection agencies associated with the FTC. Some of the prominent agencies were the FTC online and phone centers, publisher clearing house and the attorney general in specific states.
Zip code Information	The zip code of the victim and the fraudulent entity. This provided us with low level granularity for analysis, however, the latter was only available for a subset of the complaints
Contact Method	The Primary channel method that was used by the fraudulet entity to contact the victim e.g. Internet, phone, mail.
Fraud Description	A description of nature the fraud, and its type e.g. credit card, fake product, business fraud.
Fraud & Reporting Date	The dates when the fraud initially occurred and the date on which is was reported

TABLE I
THE DESCRIPTION OF THE DATA FIELDS THAT WERE PRIMARILY USED IN THE FOR DATA CALIBRATION AND ANALYSIS

II. Related Work

As our work evaluates both cyber as well as regular frauds, we provide related work that encompasses both of these categories. However, we elaborate more on recent research which focuses on cyber frauds as more individuals are victims of these crimes [13] due to the increased Internet usage trends for sensitive activities. Before the Internet became a primary hub of economic and social activity, researchers measured [9] and developed techniques based on statistical models [10], [11], [12] to detect phone and credit card based frauds. In the past few years, research evaluations have shifted focus towards cyber activity [4], [5], [3], [7] due to its high rate and the potential for harm.

Even though, term *"cyber"* is usually associated with Computer Science, due to its recent socio-economic impact, researchers in Economics, Law, and Finance have also explored for solutions to this problem by incorporating methodologies specific to their areas. Ionescu et. al [3] characterize the types and sources cyber frauds in global digital networks. The authors link the exponential increase of cyber fraud to increased Internet usage for financial management and transactions, especially in financial markets. They suggest the involvement of all stakeholders and employees through awareness and training for containing and mitigating fraud. Similarly, Howard et. al [7] study malicious code attacks against financial networks and suggest technical detection and mitigation techniques for financial infrastructure. [5] studies how the cyber criminals have several potential advantages over their opposing law enforcement agencies. They suggest some practical steps to even out the differential gap.

Due to an increase in the overall concern for online fraudulent activity, there has also been state-sponsored research that measures the impact of fraud. Smyth et. al [8] measure the extent of cyber fraud in Canada in 2011. Their work indicates that a major chunk of frauds does not get recorded and suggest a need for a sentinel record fraud data, similar to the FTC complaint center in the US.

Another significant area of research focuses on understanding the demographics of fraud victims. A recent FTC Report [14] uses complaint data to quantify complaint rates and across different ethnic and education groups in the US. [**?**] also look at how demographics effect the likelyhood of an individual to complain about fraud. Researchers in [4] provide a comprehensive survey report that sums the reactions of the victims of an online data breach. They categorize their results in different income, education, age, and ethnic groups. Such research aims to provide organizations with informed insight to better develop policies for consumer rights protection.

In comparison to previous research which individually look at either cyber of regular fraud, our work provides a unique angle of evaluation. We provide a comparison for both types of frauds and describe certain complaint charectaristics and demographic trends which more prevalent in each specific category.

III. Data and Callibration

In this section we explain the charectarisitcs of our datasets and the sources they were obtained from. We also provide insight into the essential data processing and callibration methodology that we incorporate to classify and filter the data for a fair evaluation of our questions.

A. Data Description

1) FTC Complaint Dataset: The primary dataset that we use for our evlauation is a corpus of the complaint logs filed at different collecitons agencies for the FTC during the months Jan, 13 to June, 14. The Dataset comprises of a total of 865K complaints aggregated for cyber as well as regular fraud instances during the time period. Table I shows the fields of the original dataset along with their description summary. For the purposes of brevity, we only include the fields that were used in our analysis.

2) US Census Datasets: Zip code information in our complaint dataset allows us to perform demographic analysis of the frauds. We obtain the demographic information associated with zip codes available at the US Census Bureau website [15]. The specific information that we collect is stated below:

- Population density per zip code
- Employment and income data
- Age statistics
- Race and ethinic information

As zip codes provide a low level granularity, to aggregate adjacent zip codes we obtain the Zip codes to the Metropolitinan Statistical Area (MSA) mappings from [16]. MSA are essentially groups of geographically connected zip codes that demonstrate strong social andd economic linkage. While there are more than 40,000 zip codes in the United States there are only 382 distinct MSAs [15].

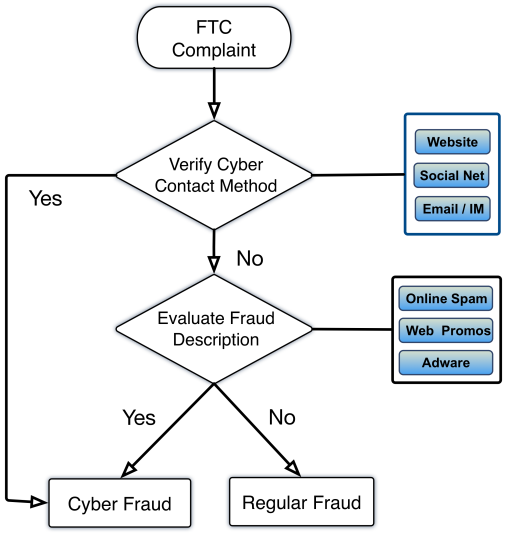

Fig. 1. Classification methodology for cyber and regular frauds

B. Calibration Methodology

While information from the US Bureau was standardized and did not require preprocessing, we cater for inconsitencies in the FTC dataset. We realize the the major source of irregularity as a results of its collection ftom various complaint collection agencies furthered by the lack of sanity checks in complaint forms or as a cause of human error while infromation entry. The two major forms of inconsitencies that we filter our are irregular zip codes that cannot be associated with a geographic region in the US and complaints that were missing essential information that required them to be tagged as a cyber of regular fraud.

As the FTC dataset was aggregated for all fraud channels a major calibration step we perfrom is to tag each crime complaint as either cyber or regular. An associated challenge for this was our limited view of the fraud description. To perform this calibration we use the **Contact Method** and **Fraud Description** fields from Table I. We flag a complaint as cyber if the victims primary contact method was thorugh online media, these are primarily websites, social networks, email and IM. For the remainder of the complaints we look at the description. If the complinat description invovles something associated with Internet, we classify it as a cyber fraud regardless of how the victim was initially approached. Figure 1 provides an depicticon of our classification methodology. This process provides us with two distinct categories and enables a fair comparison of the frauds.

IV. Evaluation

Our evaluation section can be devided into two main components. First we look at the different aspects and trends within the complaint dataset and elaborate on certain prominent charecterisitcs between regular and cyber frauds. The second part of our evaluation focuses on an in-depth analysis of the demographics linked with the types of frauds.

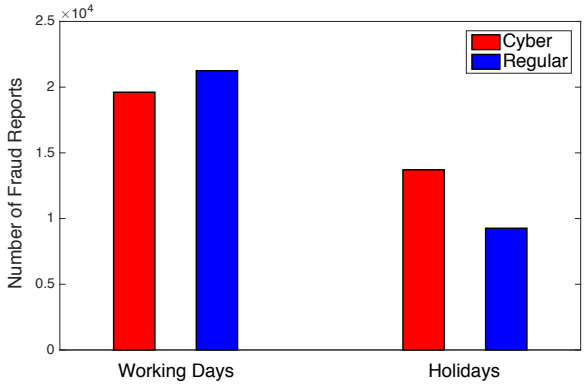

Fig. 2. Cyber and regular fraud variation during regular and holiday season

A. Fraud Reporting over Time

We initially perform a temporal analysis of the 15 month dataset to evaluate how the fraud reporting varies, over time and expore when a certain fraud is more likely to be occur and reported. While the overall rate of reporting remains consistent, we observe significant vairations specifically in the winter holiday season. To investigate this, we select two disciCnt, 20 day periods in the dataset; working days (Aug, 15 to Sept, 5) and holidays (Dec 15, to Jan, 5). Figure 2 shows the variation of cyber and regular frauds within the two specific time periods. We observe that the overall number of fraud reports decrease by a total of 43.7% within the holiday seasion. Another significant insight is the indiviudal number of cyber and frauds in each time period. While cyber reports are approximaltely 8.0% less than regular reports duriing the working days, they are 47.9% more by than regular reports during the holidays.

To further validate our findings from figure 2, we perfrom the t-test to verify the statistical significance of the reporting difference in the two time durations. We find that the *p-value* coefficients to compare cyber and regular frauds in each region. Table II summarizes our results.

Fraud Type	*p-value* Coefficient
Cyber	0.014
Regular	0.003

TABLE II
T-TEST RESULTS FOR CYBER AND REGULAR FRAUDS IN DIFFERENT PERIODS

Our results indicate that cyber fraud reporting trends are statisitcally significant (*p-value* $>$ 0.05) between the two durations. To further invesitigate phenomenon, we look at the reporting methods vitimins use to contact section IV-C.

B. Fraud Reporting Methods

We evaluate the methods that individuals use to report fraud incidencts to the FTC. We aggregate the 26 complaint collecting agencies into online and offline categories. For instance, reports made via the Internet complaint center or the FTC complaint assistant and tagged as online, while the ones

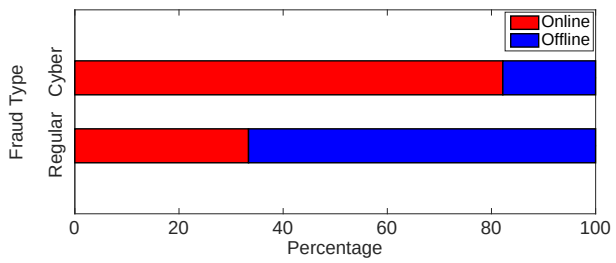

Fig. 3. Distribution of reporting methods in for cyber and regular frauds

made to the FTC call center, publisher clearing house, attoreny generals or other regulatory institutions are categorized and offline reports. Figure 3 provides the distribution of of how individuals opted to report the respective cyber and regular crimes. We see that approximaltey 82% of cyber fraud victims used an online complint facility, and 63% of regular fraud victims reported via offline methods.

As a major chunk of regular frauds are reported via offline methods, and while offline institutions have reduced operation during holidays, this significanlty contributes to the reduction of regular fraud reporting during holidays and biases the value in Figure 2. However, as most cyber frauds are reported via automated online methods which are available aroud the clock, we believe that cyber frauds experience a true reduction in the holiday period. Our understanding is corroborated by the *p-value* statisics in Table II, where the cyber complaints in the working day and holiday time periods belong to different sets whereas the comparions of regular complait sets withtin the periods yeilds insignificant. This insights helps us suggest more meaning suggestions to cater these specifc types of crimes.

C. Top Fraudsters

cyber - use call center and internet

regular -¿ primarily use call, have reduced hours, hence leads to a lower reporting rate..

distinct 20 day periods Holiday 15 jan - 5 Jan

average holiays seasion

Regualr Seasion Aug

Month with Max Reporting Month with minimum reoprting

Even During regular days, cyber reports where ¿ regular reports...

perform p value statisitcal tests... create a p value tabls

are there certain durations where there are a larger number of cyber-crimes than regular crimes. Figure 2 shows t

as online reporting for cyber,

V. Discussion

VI. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.
[2] pete snyder affiliate fraud
[3] cyberfraud in a global digital network
[4] Consumer Attitudes Toward Data Breach Noti cations and Loss of Personal Information
[5] An Uneven Playing Field: The Advantages of the Cyber Criminal vs. Law Enforcement-and Some Practical
[6] Identity Theft as a Teachable Moment
[7] Cyber Fraud Trends and Mitigation
[8] Cyberfraud in Canada
[9] Controlling Cell Phone Fraud in the US: Lessons for the UK Foresight Prevention Initiative
[10] Neural data mining for credit card fraud detection
[11] Detection of mobile phone fraud using supervised neural networks: A first prototype
[12] Statistical Fraud Detection: A Review
[13] http://gotaclassaction.com/wp-content/uploads/2013/05/FTC-Fraud-Survey.pdf
[14] complaints ftc paper
[15] usbureau website
[16] dept of labor website
bibitemconsurmeraffairs Are Consumers Disadvantaged or Vulnerable An Examination of Consumer Complaints to the Better Business Bureau