# Old is Still Gold: A Comparison of Cyber and Traditional Consumer Fraud in The United States

Mohammad Taha Khan and Chris Kanich
Department of Computer Science, University of Illinois at Chicago
taha@cs.uic.edu, ckanich@uic.edu

***Abstract*—While cybercrime is a relatively recent human invention, fraudulent activity has a much longer history. Understanding the extent to which cybercrime is fundamentally different from, or similar to, traditional fraudulent activity is the first step toward being able to effectively combat it. This paper investigates the differences in fraud targeting among United States based consumers by comparing reports of fraudulent activity mediated by the Internet with traditional forms of fraud. By partitioning the FTC Consumer Sentinel complaint dataset into cyber and traditional categories, we summarize the difference in fraud trends across time, distance and location metrics. We also evaluate fraud variations across different ethnic and socioeconomic factors. Our findings suggest that reports of both categories of frauds decrease during the holiday season. Individuals who are victimized via traditional methods are more likely to complain using traditional methods, while a majority of cyber victims submit fraud complaints online. By evaluating the top frauds in each category, we demonstrate how traditional fraudsters have evolved in their methodologies to execute scams on the Internet that were initially perpetrated through traditional means.**

## I. Introduction

In the United States, a total of more than 25 million people are victims of frauds per year [1]. These deceptive scams are a major cause of economic damages to users, as well as added stress and wasted time. Such illicit practices have been a part of the underground economy for quite a while. Initially, individuals were contacted via scam calls, snail mail, or in person communication. The rise of the Internet has provided fraudulent entities with a more effective method of communicating with the overall population. According to a Javelin study in 2017, identity frauds hit a record high, targeting 15.4 million victims in the United States [2]. The findings indicated that individuals with an online presence were more susceptible to possibility of theft. Another recent study released by the Federal Trade Commission (FTC) reported that debt collection, identity theft, and impostor scams contributed towards 56% of the total frauds complaints in 2015 [3] . With the number of Internet users on the rise, the number of cyber frauds is likely to increase over the next couple of years [4]. To deal with this rising situation, the Federal Bureau of Investigation (FBI), has also been actively involved in addressing this issue. Their complaint portal, known as the IC3 is specifically designed to record complaints on Internet-based fraudulent practices [5]. This emerging trend of deceptive practices necessitates their study in order to evaluate and mitigate the harm caused to victims.

This paper evaluates the nature of consumer fraud in the United States. Our work provides a comparison between cyber and traditional frauds. We categorize cyber frauds as all those deceptive practices that victimize users online, while regular (or traditional) frauds target individuals over the phone, via mail, or in-person. While we understand that online scams [6] are a major focus of today's research, our comparison based approach allows us to better understand how they differ from traditional fraud methods. It also enables us to independently evaluate trends in traditional frauds and to determine whether fraudsters are adopting online mechanisms to target more individuals. This combined analysis enables us to provide strategic suggestions in means to develop better fraud prevention techniques.

To evaluate fraud trends, we use the FTC's Consumer Sentinel database, a dataset of complaints from the year 2013 and 2014. We also collect demographic information from the US Census Bureau [7]. In addition to data collection, we devise a calibration methodology to identify and separate cyber frauds from regular ones in the complaint dataset.

Our work provides three main contributions. First, we evaluate the distinctive trends prevalent in cyber and regular frauds in the dataset. This encompasses their reporting numbers and methods, the nature of frauds which are more common in each specific category as well as the insights on the fraudsters who carry out these specific deceptive activities. Secondly, we look at ethnic, age, education, and employment demographics in each specific category and evaluate if certain individuals are more likely to report. Finally, based on our findings we suggest measures that can be taken into account by regulatory agencies to reduce overall fraud in the United States.

The rest of the paper is structured as follows, section II provides a comprehensive overview of the relevant work. In section III, we elaborate on features of the datasets used in our analysis along with a description of our calibration methodology. Section IV summarizes our findings from the data, followed by our suggestions to regulatory agencies in V. We conclude our work in section VI and discuss avenues of future research.

## II. Related Work

As our work evaluates both cyber as well as regular frauds, we provide related work that encompasses both categories. Before the Internet became a primary hub of economic and

| Data Field | Field Description |
|---|---|
| Agency Name | The complaint collection agencies associated with the FTC. |
| Zip code Information | The zip code of the victim and the fraudulent entity. |
| Contact Method | The primary channel used by the fraudulent entity to contact the victim e.g. Internet, phone, mail. |
| Fraud Description | Nature of the fraud, and its type e.g. credit card, fake product, debt collection. |
| Occurrence & Reporting Date | The dates when the fraud initially occurred and the date on which is was reported. |

TABLE I
DATA FIELD PRIMARILY USED FOR DATA CALIBRATION AND ANALYSIS

social activity, researchers measured [8] and developed techniques based on statistical models [9], [10], [11] to detect phone and credit card based frauds. In the past few years, research evaluations have shifted focus towards cyber activity [12], [13], [14], [15], [16] due to the increased Internet usage trends for sensitive activities and its increased potential for harm.

Even though term *"cyber fraud"* is usually associated with Computer Science, its recent socio-economic impact has motivated researchers in Economics, Law, and Finance to explore solutions by incorporating methodologies specific to their areas. Ionescu et al. characterize the types and sources of cyber financial frauds in global digital networks [14]. The authors suggest the involvement of all stakeholders and employees through awareness and training to contain and reduce fraud. Similarly, Howard et al. study malicious code attacks against financial networks and suggest technical detection and mitigation techniques for financial infrastructure [15] . Studies also show how the cyber criminals have several potential advantages over their opposing law enforcement agencies and suggest some practical steps to even out the differential gap [13].

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. measure the extent of cyber fraud in Canada in 2011 [17]. Their work indicates that a major chunk of frauds does not get recorded and hence the suggest a need for a sentinel to 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 [18]. A recent FTC Report [19] quantifies complaint rates across different ethnic and education groups in the US. Garrett et al also look at how demographics affect the likelihood of an individual to complain about fraud [20]. Researchers have also focused on studying the reactions of the victims of an online data breach [12]. 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.

Contrary to previous research, which individually studies cyber or regular fraud, our work provides a unique angle of evaluation, by comparison of both fraud types. We evaluate characteristics for both types of cyber and regular frauds and their demographic trends.

## III. Data and Calibration

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

### A. Data Description

| Description | Value |
|---|---|
| % Cyber Complaints | 52.1 |
| % Regular Complaints | 47.9 |
| Month with Most Complaints | July 2013 |
| Month with Least Complaints | Feb 2013 |

TABLE II
SUMMARY STATISTICS OF THE FTC DATASET

*1) FTC Complaint Dataset:* The primary dataset we use for our evaluation is a corpus of the complaint logs collected between the months of Jan 2013 to June 2014 at agencies within the US and reported to the FTC[1]. The Dataset is comprised of 865K complaints aggregated for cyber as well as regular fraud. Agencies responsible for collecting these logs provide online portals, phone or in-person reporting services. Inconsistent reporting semantics is an associated challenge with multiple data collection sources. While the FTC data is calibrated to a fair extent, to ensure the accuracy of our results, we perform an initial data consistency parse to exclude irrelevant outliers from the aggregated dataset. Table I shows the fields of the used dataset along with their description. While the original dataset has several fields, for reader convenience and brevity, we only include the relevant ones form the basis our analysis. we also provide summary statistics of the data in table II.

*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 [7]. The specific information that we collect is stated below:

- Population density per zip code
- Education and income data [2]
- Age statistics
- Race and ethnic information

As zip codes provide a low-level granularity, to aggregate adjacent zip codes we obtain the Zip codes to the metropolitan Statistical Area (MSA) mappings from [22]. MSA are essentially groups of geographically connected zip codes that

[1]This data was obtained from the directly from the FTC under the Freedom of Information Act (FOIA).

[2]We obtained education data from an aggregator of US demographics [21].

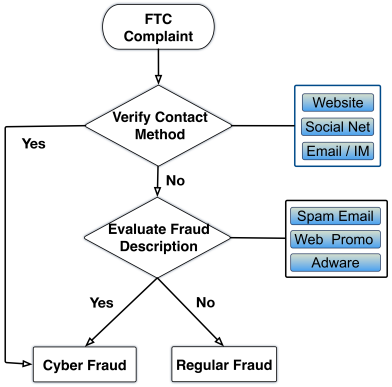


Fig. 1. Methodology for classifying cyber and regular frauds.

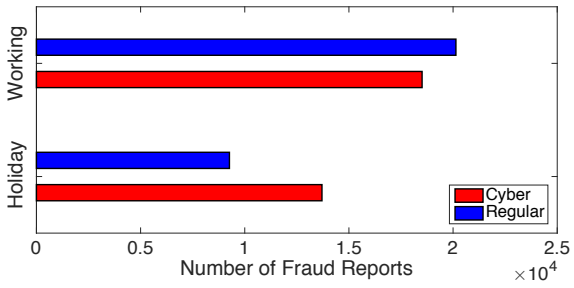


Fig. 2. Fraud reporting incidence during regular and holiday season

demonstrate strong social and economic linkage. While there are more than 40,000 zip codes in the United States there are only 382 distinct MSAs [7]. While our analysis in section IV-G aggregates different demographics based on zip codes, we incorporate the use of MSAs while performing location based evaluations in section IV-F. This essentially allows us to cluster the zip codes and associate a named location with them. This aggregation also helps mitigate any bias caused by an anomalous outlier zip code.

### B. Calibration Methodology

One of the major fundamentals of our comparison is accurate tagging of each complaint as either cyber or regular fraud. While having a limited view of the fraud description, this paper takes a *best effort* calibration approach to differentiate between the two types of frauds. To perform this calibration we use the **Contact Method** and **Fraud Description** fields from Table I. Initially, we manually classify all contact methods and descriptions as either cyber or regular. We then flag a complaint as cyber if the victim's primary contact method was through online media; these are primarily websites, social networks, email, and IM. For the remainder of the complaints, we look at the description. If the complaint description involves something associated with the Internet, we classify it as a cyber fraud regardless of how the victim was initially approached. For instance, frauds, in which an individual is contacted via phone and requested to perform certain actions on their computer e.g. visiting a certain website, will be categorized as cyber. While this is a sophisticated technique that involves phone communication, the actual fraud hinges on the victim performing specific actions online, making it cyber nature. Figure 1 provides a visualization of our keyword classification methodology. This process provides us with two distinct categories and enables a fair comparison of the frauds.

## IV. Evaluation

Having the categorized dataset, we aim to answer the primary question of how cyber and regular fraud compare to each other Based on the auxiliary information in the FTC dataset, combined with the informative fields from secondary sources, we are able to explore various data dimensions for our cpmparison. First, we look at how cyber and regular crimes vary across the different times of the year. We then aim to understand the distribution of cyber and regular frauds across victims. We also compare the reaction of the targeted individuals by evaluating their respective reporting methods and reaction time. Similarly, we explore if fraudsters of cyber and regular frauds have certain distinguishable characteristics. Finally, we provide an in-depth comparison of various demographics for the two fraud types.

### A. Fraud Variation over Time

We initially perform a temporal analysis of the 15-month dataset to evaluate how the fraud reporting varies over time and explore when a certain type of frauds is more likely to be reported. We use the reporting date as an estimate of fraud count on that specific date. While the overall rate of fraud remains consistent, we observe a significant reduction in reporting in the winter holiday season. To investigate this, we select two distinct, 20 day periods in the dataset; we label them as **Working** (Aug, 15 to Sept, 5) and **Holiday** (Dec 15, to Jan, 5). Figure 2 shows the variation of cyber and regular frauds within the two specific time periods. We observe a significant drop in the frauds during the holiday time period. Individually, cyber fraud decreases by 26% while regular fraud decreases by a much larger value of 56%. Our analysis is based on the conservative assumption that, reporting count on a date positively correlates with the number of frauds and there is not a significant reporting delay between the crime and reporting dates. We validate this in figure 4 (a), which shows that approximately 70% of reporting dates are within a week of the date when the incident occurred, we also suggest some associated limitations to this approach in section IV-C. We also believe that the larger decrease in regular frauds is an overestimate as result of a bias that we explain using additional statistical findings from the next section.

### B. Fraud Reporting Methods

Consumers have the ability to report complaints to the FTC via several methods and agencies. We aggregate the 26 complaint collecting entities into online and offline categories. For instance, reports made via the Internet complaint center or the FTC complaint assistant are tagged as online, while the

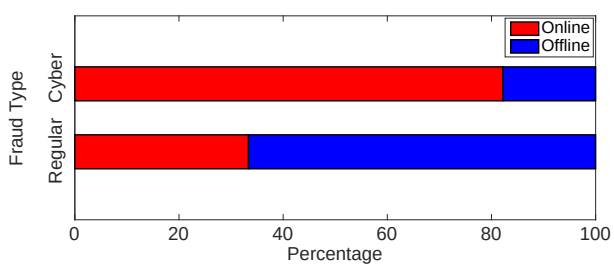


Fig. 3. Distribution of reporting methods for frauds

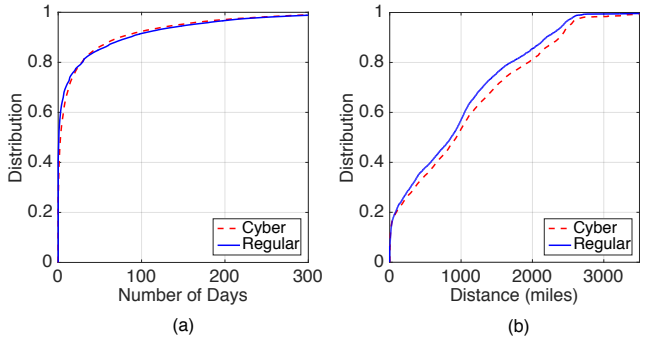


Fig. 4. The cumulative distribution for (a) The difference between fraud and reporting dates. (b) The distance between consumers and fraudsters.

ones issued to the FTC call center, publisher clearing house, attorneys general, or other regulatory institutions are categorized as offline. Figure 3 provides the distribution of how individuals opt to report cyber and regular crimes. Approximately 82% of cyber fraud victims used an online complaint facility, and 63% of regular fraud victims reported via offline methods.

We observe that a major chunk of regular frauds is reported to offline institutions, which have reduced operation during holidays. We believe this significantly contributes to the reduction bias of the value of regular frauds in figure 2.

To further validate this, we perform a two-sample t-test over the distribution of fraud reports for both cyber and regular frauds. The compared distributions belong to the working and holiday period explained in section IV-A. Our null hypothesis assumes that both time periods belong to the same reporting pool. The statistically significant *p-value* for regular frauds in table III suggests in favor of the alternative hypothesis, hence validating our assumed bias for a decrease in regular frauds. Additionally, we also calculate the percent increase in reporting between the last 10 holidays and 10 working days right after. While cyber reports only increase by 37% the increase in regular fraud reports is a staggering 104%. The ratio of increases is in line with the proportions (17:66) for offline reporting methods used by cyber and regular fraud victims. We believe that while both types of frauds experience a decrease, the decrease in cyber frauds represents a more accurate trend. These derived insights enable us to suggest more meaningful measures in section V to deal with consumer fraud.

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

TABLE III
T-TEST RESULTS FOR FRAUDS ACROSS DIFFERENT TIME PERIODS

### C. Consumer Reaction Time

Here we evaluate on how quickly do victims of a fraud react and report the incident. Figure 4 (a) shows the CDF of the number of days between the date when the fraud occurred and when in was first reported to the FTC. We do not observe any difference between the reaction time trends of cyber and regular fraud victims. The graph shows that for both fraud categories, almost 30% of the individuals take more than a week to respond. We believe that this provides ample time window for fraudsters to maliciously act on the assets acquired from individuals. This increased delay can also be a result of individuals discovering they were victimized by a fraud at a later date than the actual incident. One example would be a credit card theft when the victims only recognize the breach after they see an unauthorized transaction. Unfortunately, we do have enough information in the dataset to normalize in against such a situation in practice.

| **Cyber** | **%** | **Regular** | **%** |
|---|---|---|---|
| Online Shopping & Sales | 14.1 | Impostor Fraud | 29.8 |
| Impostor Fraud | 10.8 | Telemarketing | 20.1 |
| Unsolicited Email | 7.71 | Debt Collection | 16.1 |
| Counterfeit Check Scams | 7.40 | Prizes & Sweepstakes | 15.5 |
| Prizes & Sweepstakes | 7.40 | Grants & Credit Loans | 4.14 |

TABLE IV
TOP FRAUD DESCRIPTIONS

### D. Most Common Frauds

By using the fraud description fields we summarize the the top frauds in table

IV provides a summary of the top frauds in each category.

We see a significant cyber presence of impostor scams and sweepstakes. While these frauds have long existed in the regular domain, this provides us anecdotal evidence that fraudsters are adopting new technology to execute the same types of scams online, which were previously perpetrated offline. We incorporate this specific insight in our discussion. Our results greatly align with the top sources of frauds stated in an FTC news release in 2016 [3].

### E. Fraudster Coverage

In order to understand the operational regions of fraudulent entities, we calculate the distances between consumer and fraudster zip codes. Figure 4 (b) provides a cumulative distribution of the operational radii for cyber and regular fraudsters. This analysis provides insight on whether cyber fraudsters leverage the Internet for more visibility and access to target more distant individuals. With a median distance of 993 and 861 for cyber and regular frauds, we believe that both types of fraudsters follow similar trends. This indicates that Internet-based communication does not provide cyber fraudsters with

a significant advantage over regular ones, as they are able to achieve similar operational spans by using phone and mail based communication methods.

| Metropolitan Area (MSA) | % Cyber | % Regular |
|---|---|---|
| New York, New Jersey, Long Island | 8.41 | 7.67 |
| Los Angeles, Long Beach, Santa Ana | 6.50 | 7.09 |
| Washington, Arlington, Alexandria | 4.10 | 5.78 |
| Miami-Fort Lauderdale, Pompano Beach | 4.16 | 5.40 |
| Dallas, Fort Worth, Arlington | 2.89 | 3.36 |
| Chicago, Naperville Joliet | 3.17 | 3.27 |

TABLE V
TOP FRAUDSTERS LOCATIONS

### *F. Top Fraudster Locations*

Next, we identify the primary locations of the fraudsters within the United States and present our findings in V. While fraudulent entities are spread throughout, most of the heavy hitters belong to the metropolitan areas. We believe this provides an efficient disguise to the fraudulent entities. We also observe certain areas that having a high cyber to regular fraud ratio and vice versa. The San Franciso, Oakland and San Jose, Santa Clara MSAs have a cyber to regular fraud ratio of 2.21 and 5.13. The popular fraud types in these regions are Internet services, unsolicited email, and online shopping. These areas serve as a good medium for cyber fraudsters as it allows them to gel into the surrounding cyber industry. Meanwhile, The Buffalo, Niagara Falls MSA has a regular to cyber fraud ratio of 8.76 with debt collection being the significant outlier. Further investigation reveals that Buffalo has a network of debt collectors which have been responsible for multi-million frauds [23], [24].

### *G. Demographic Analysis*

By normalizing over cyber and regular frauds in each zip code, we evaluate how they vary with certain demographic features, which are obtained from the complementary datasets that we discuss in section III.

To realize the effect of these features, we perform a logistic regression and summarize our coefficients and their significances in table VI. Among different ethnicities, only Hispanic communities show statistically significant change for cyber and regular fraud per capita. While the regression coefficients suggest that frauds decrease for heavier concentrations of Hispanics, a survey study [1] showed that Hispanics and Black communities are more likely to be victims of crimes. The decreasing trend is likely a result of fraud under-reporting due to cultural reasons, distrust in institutions, and lack of awareness or education [25].

Other socio-economic variables that we take into account are age, income, education, and unemployment rate. In addition to the regression analysis, we investigate their variation by observing complaint rates across their distributions in figure 5.

**Age:** While the differences in cyber and regular complaints remain fairly consistent, from figure 5 (a) we observe that individuals greater that 50 years complain significantly more than other age groups. Our significant regression values also corroborate to this trend.

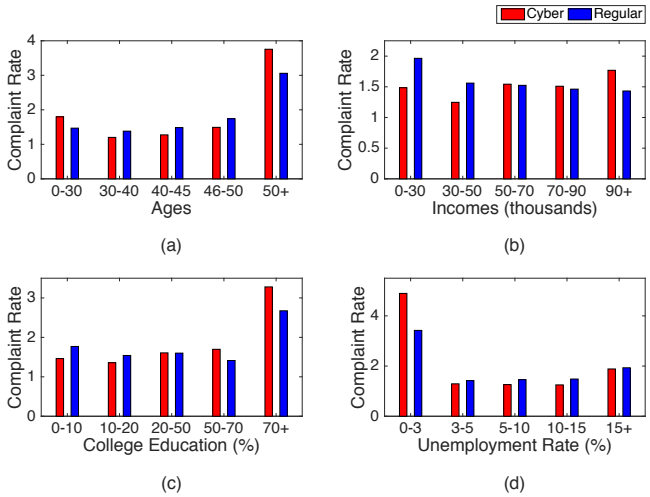


Fig. 5. Cyber and regular fraud trends over age, income, education and unemployment.

**Education:** Both cyber and regular complaints increase along with an increase in percentage education. We associate this trend with greater increased educational awareness among individuals [25]. Another subtle trend, in the increase in cyber to regular complaint ratio from 0.82 to 1.23. We associate this diverging trend to more educated individuals being active on the Internet, and hence being more prone to online fraud [26].

We do not include income and unemployment in our analysis due to their insignificant correlation values in table VI.

## V. DISCUSSION

Based on our findings from section IV, we elaborate some discussion points to provide context for this analysis in hopes that it will assist in the development of better policies and help reduce consumer fraud in the U.S.

Our results indicate that while cyber frauds are on the rise, regular fraud methods still hold an equally significant share in the economy, and while policy developments are trending towards mitigating online fraud, there should be continuous awareness campaigns for phone, mail and other regular fraud types. As a result of reduced operational hours in the winter holidays, offline collection agencies experience an uneven decrease followed by a great influx of reports on resuming operation. To streamline the process, online reporting methods should be promoted.

We also learn that fraudulent entities tend to work in groups and establish networks [24]. The fraudulent cyber establishments of San Jose and San Francisco discussed in Section IV-D, help us understand that fraudulent entities likely reflect the makeup of nearby legitimate industries.

By observing the overlap between top cyber and regular frauds (Table IV) we realize that with the rise of Internet, fraudsters have their choice of vectors to execute scams that were traditionally only perpetrated through traditional means.

| | Cyber Complaints Per Capita | | | Regular Complaints Per Capita | | |
|---|---|---|---|---|---|---|
| **Observed Variable** | **Coefficient** | ***p-value*** | **95% Confidence Interval** | **Coefficient** | ***p-value*** | **95% Confidence Interval** |
| % White (Non-Hispanic) | -0.0042 | 0.074 | [-0.009, 0] | -0.0013 | 0.128 | [0.003, 0] |
| % Black | -0.0058 | 0.017 | [-0.011, -0.001] | 0.0017 | 0.054 | [$-2.77^{-5}$, -0.003] |
| % Asian | -0.0025 | 0.468 | [-0.009, 0.004] | -0.0051 | 0.00 | [-0.008, -0.003] |
| % Hispanic | -0.0026 | 0.014 | [-0.05, -0.001] | -0.0054 | 0.00 | [-0.006, -0.005] |
| Age | 0.0064 | 0.023 | [ 0.001, 0.012] | 0.0281 | 0.00 | [0.026, 0.030] |
| Income | $-2.226^{-6}$ | $8.85^{-7}$ | [$-3.96^{-6}$ , $-4.92^{-7}$] | $-3.695^{-6}$ | 0.000 | [$-4.31^{-6}$, $-3.08^{-6}$] |
| Education | 0.0155 | 0.000 | [0.013, 0.018] | 0.0044 | 0.00 | [0.003, -0.005] |
| Unemployment | 0.0084 | 0.111 | [-0.002, 0.019] | -0.0028 | 0.138 | [-0.006, 0.001] |

TABLE VI
REGRESSION RESULTS FOR PER CAPITA FRAUDS EVALUATED FOR ETHNIC AND SOCIO-ECONOMIC FACTORS

Better understanding these advanced communication modalities requires a technologists' touch; policy makers should consider working closely with technologists to devise detection mechanisms similar to [9], [10] which enable better filtering and control of the fraudulent activity.

## VI. CONCLUSION & FUTURE WORK

The goal of this paper is to investigate the dynamics of cyber and traditional methods for committing fraud in the United States. By partitioning the FTC Consumer Sentinel complaint dataset, we are able to explore trends among cyber and regular fraud, and analyze trends along time, distance and location metrics as well as their variation across consumer demographics. The Internet has greatly expanded the potential reach and scale of fraudsters, enabling them to contact millions of users very quickly, whether through fraudulent websites, Craigslist posts, or spam emails. Even so, the difference between the cyber and non-cyber methodologies is not overwhelming: this effect suggests that non-cyber activities, like purchasing goods or posting money orders, may still serve as a limiting factor on the extent or targeting of these fraudulent activities.

As a future effort in this space, we plan to extend our analysis over multiple years through analysis of different, higher fidelity datasets that span a longer duration. We also look forward to evaluating our current findings with data collected by other regulatory agencies such as the FBI. This will eventually also allow us to overcome certain nuances and limitations of the current evaluation and help us develop stronger insights. Another interesting future direction is to evaluate how international fraud compares to fraud within the US, and identify any prominent international fraudsters who target US victims. This can possibly be achieved by using data from the European Commission and the eCrime project.

## VII. ACKNOWLEDGMENTS

We would like to thank the reviewers for their helpful feedback. This material is based upon work supported by the National Science Foundation under Grant No. 1351058. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

## REFERENCES

[1] K. B. Anderson, "Consumer fraud in the united states, 2011: The third ftc survey," *Federal Trade Commission*, 2013.

[2] A. Pascual, K. Marchin, and S. Miller, "2017 identity fraud: Securing the connected life — javelin," https://www.javelinstrategy.com/coverage-area/2017-identity-fraud, (Accessed on 03/07/2017).

[3] "Ftc releases annual summary of consumer complaints — federal trade commission," https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer-complaints, March 2016, (Accessed on 01/17/2017).

[4] M. Duggan, "Online harassment — pew research center," October 2014.

[5] "Internet crime complaint center (ic3)," https://www.ic3.gov/, (Accessed on 01/17/2017).

[6] N. Miramirkhani, O. Starov, and N. Nikiforakis, "Dial one for scam: Analyzing and detecting technical support scams," *arXiv preprint arXiv:1607.06891*, 2016.

[7] "United states census bureau," https://www.census.gov/, (Accessed on 01/17/2017).

[8] R. V. Clarke, R. Kemper, and L. Wyckoff, "Controlling cell phone fraud in the us: Lessons for the uk foresightprevention initiative," *Security Journal*, vol. 14, no. 1, pp. 7–22, 2001.

[9] R. Brause, T. Langsdorf, and M. Hepp, "Neural data mining for credit card fraud detection," in *Tools with Artificial Intelligence, 1999. Proceedings. 11th IEEE International Conference on*. IEEE, 1999, pp. 103–106.

[10] Y. Moreau, H. Verrelst, and J. Vandewalle, "Detection of mobile phone fraud using supervised neural networks: A first prototype," in *International Conference on Artificial Neural Networks*. Springer, 1997, pp. 1065–1070.

[11] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Statistical science*, pp. 235–249, 2002.

[12] L. Ablon, P. Heaton, S. Romanosky, and D. C. Lavery, "Consumer attitudes toward data breach notifications and loss of personal information," 2016.

[13] T. Piper, "An uneven playing field: The advantages of the cyber criminal vs. law enforcement and some practical suggestions," 2002.

[14] L. Ionescu, V. Mirea, and A. Blajan, "Fraud, corruption and cyber crime in a global digital network," *Economics, Management and Financial Markets*, vol. 6, no. 2, p. 373, 2011.

[15] R. Howard, R. Thomas, J. Burstein, and R. Bradescu, "Cyber fraud trends and mitigation," in *The International Conference on Forensic Computer Science (ICoFCS)*, 2007.

[16] P. Snyder and C. Kanich, "No please, after you: Detecting fraud in affiliate marketing networks," in *Proceedings of the Workshop on the Economics of Information Security (WEIS)*, 2015.

[17] S. M. Smyth and R. Carleton, "Measuring the extent of cyber-fraud: A discussion paper on potential methods and data sources," 2011.

[18] B. Cornwell, D. Bligh, and E. Babkus, "Complaint behavior of mexican-american consumers to a third-party agency," *Journal of Consumer Affairs*, vol. 25, no. 1, pp. 1–18, 1991. [Online]. Available: http://dx.doi.org/10.1111/j.1745-6606.1991.tb00278.x

[19] D. Raval, "What determines consumer complaining behavior?" *Federal Trade Commission*, 2016.

[20] D. E. Garrett and P. G. Toumanoff, "Are consumers disadvantaged or vulnerable? an examination of consumer complaints to the better business bureau," *Journal of Consumer Affairs*, vol. 44, no. 1, pp. 3–23, 2010.

[21] "Zip code, area code, city & state profiles — zipatlas," http://zipatlas.com/, (Accessed on 01/17/2017).

[22] "U.s. bureau of labor statistics," https://www.bls.gov/, (Accessed on 01/17/2017).

[23] G. Warner and J. Zremski, "Buffalo debt collector pleads guilty in massive fraud - the buffalo news," https://buffalonews.com/2016/11/

02/head-buffalo-debt-collection-agency-pleads-guilty-fraud/, Nov 2016, (Accessed on 01/17/2017).
[24] P. Faribanks, "Buffalo debt collectors accused of taking in 'tens of millions' by harassing consumers - the buffalo news," http://buffalonews.com/2016/11/02/buffalo-debt-collector-accused-harassing-consumers/, Nov 2016, (Accessed on 01/17/2017).
[25] T. Dahdouh, "L.a. lessons — consumer information," https://www.consumer.ftc.gov/blog/la-lessons, Feb 2015, (Accessed on 01/17/2017).
[26] A. Smith, L. Rainie, and K. Zickuhr, "College students and technology — pew research center," http://www.pewinternet.org/2011/07/19/college-students-and-technology/, July 2011, (Accessed on 01/17/2017).