Big Data Analyses with No Digital Footprints Available

– Evidence from Cyber-Telecom Fraud

Laura Xiaolei Liu[1*]
Yufei Liu[1]
Xinghua Ruan[2]
Qirong Yang[2]
Yu Zhang[1]

This draft: 1/29/2021.

Abstract

Cyber-telecom fraud is an increasingly severe problem globally. We focus on a special type of cyber-telecom financial fraud, where criminals induce innocent people to borrow online. Since there are no digital footprints available for the fraudsters behind the borrowing cases, identifying them is difficult. Using a proprietary dataset of online consumer financing from a large Fintech company in China, we estimate to what extent interventions based on big data and machine learning techniques can identify this type of fraud and prevent customers' financial losses. Female borrowers are more likely to be fraud victims. Young and inexperienced users are more likely to be subject to fraud schemes that target a lack of financial literacy. Experienced and inexperienced users are equally likely to be subject to fraud schemes targeting overconfidence. The intervention is effective on frauds targeting either financial literacy or behavioral biases. However, it takes longer to persuade victims of fraud targeting behavioral biases.

Keywords: Fintech, big data, machine learning, cyber-telecom fraud, Internet finance

[1] Guanghua School of Management, Peking University.

[2] Du Xiaoman Financial.

[*] Corresponding author: Laura Xiaolei Liu (laura.xiaolei.liu@gsm.pku.edu.cn). We thank David Robinson and seminar participants at Fudan University Fanhai School of Finance for suggestions that improve this research. All errors are our own.

I. Introduction

With the development of the Internet, cyber-telecom financial fraud has become a fast-growing field of white-collar crime globally, causing severe financial losses for the telecommunications industry and its customers. Cyber-telecom financial fraud can be understood as “the abuse of telecommunications products or services with the intention of illegally acquiring money from a communication service provider or its customers,” and costs around US$32.7 billion losses annually around the world (Europol 2019).[3]

Cyber-telecom financial fraud has also become an increasingly important threat in China, the world’s second-largest financial market. The Ministry of Public Security registered around 590K cases in 2015, reflecting a year-on-year increase rate of 32.5%, causing RMB 22.2 billion financial losses (US$3.43 billion). According to a survey implemented by Tencent News, among a randomly-selected group of 30 thousand customers, 90% said that they had received cyber-telecom financial fraud messages in different forms.[4] Figure 1 shows the number of cyber-telecom-related criminal lawsuits over the past years.[5] From 2016-2018, cyber-related criminal cases increased by around 40% per year. In 2019, the cases number doubled comparing to the year 2018. It is worth mentioning that this is an incomplete statistic, as only less than 5% of the cyber-telecom financial fraud cases were eventually cracked down on, suggesting that the real number of cases are about 20 times the number reflected by lawsuits.[6]

Among different types of cyber-telecom financial fraud, the most serious one is probably fraudulently induced money borrowing. Unlike bank deposit scams, fraudulently induced borrowing created more severe problems as commonly, victims

[3] See https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/telecommunications-fraud for Europol‘s report.

[4] More details about the survey can be found at https://news.qq.com/cross/20170309/49rpD72V.

[5] The data is based on the China Justice Big Data Research Institute report on cyber-crime (http://data.court.gov.cn/pages/index.html) and Legal Daily (https://www.chinanews.com/gn/2020/04-08/9150640.shtml).

[6] Difficulties in detecting cyber-telecom fraud can be seen at https://m.66law.cn/laws/413213.aspx.

cannot pay back the debt. Sometimes, they have to reborrow from different platforms in order to make the repayment.[7] Since cyber-telecom financial frauds cause severe financial loss to victims, it is important and helpful to understand more about these frauds and the potential mechanism to prevent them. Our study fits the gap

In general, using traditional methods to intervene on financial scams or frauds are unlikely to be effective, as "cooling off laws provide little protection, nudges cannot help, and it is difficult for preventative educational interventions to be timely enough to be salient" (Fernandes, Lynch, and Netemeyer, 2014). In this study, using a large proprietary dataset on online consumer financing from a large Fintech company in China, Du Xiaoman Financial,[8] a subsidiary of a big-tech firm in China, Baidu, we explore two questions: (1) what types of individuals in the financial market are more likely to be victims of cyber-telecom fraudulently-induced borrowing; (2) whether and how Fintech, specifically big data and machine learning, helps to prevent this type of cyber-telecom fraud.

The situation we focus on differs from identifying fraudulent borrowers on online platforms with no intention to pay back. Recently, there is a burgeoning stream of studies on how big data usage can assist a firm's risk control of lending. Agarwal, Qian, Ren, Tsai, and Yeung (2020) and Berg, Burg, Gombović, Karolyi, and Puri (2020) show that digital footprints can be used to model borrower's creditworthiness. Dai, Han, Shi, and Zhang (2020) explore and show that digital footprints can be used as a kind of collateral for debt collection.

Different from these studies, we show how big data analysis and machine learning techniques can help identify cyber-telecom fraud when there is no fraudsters' digital footprint available. The scammers hide in the background, and evades the collection of

[7] Aware of the danger of this particular type of fraud, the Ministry of Public Security launched the "Sword on Cloud 2020-Fighting cyber-telecom fraud on borrowing" campaign in May 2020 (See http://www.gov.cn/xinwen/2020-05/08/content_5509648.htm for more details about the campaign).

[8] Previously named as "Baidu Finance".

their digital footprints. Identifying fraud cases in our scenario is considerably more difficult. It is not just analyzing the borrowers themselves using big data, including digital footprints, to judge their creditworthiness or ability/willingness to pay back the debt. It involves assessing the motivation of the borrowing behaviors and linking the borrowers to someone else in the background who is conducting fraud. To make it more difficult, cyber-telecom fraud criminals are often strangers to the victims, and there is not much data linking the criminals with the victims.

Our data comes from Du Xiaoman Financial. One of their main businesses is online lending. The company has been aware of the fraudulently induced borrowing since May 2019, and accumulated data on transactions that have been shown ex-post to be fraud-related. Commonly, the victims will report the cases to the police. However, in many cases, the criminals cannot be identified, and the loans are subject to legal disputes[9]. Understanding the legal perspective of these fraudulently induced borrowing is beyond the scope of this study; we focus on the occurrence of the fraud itself. The company has developed machine learning algorithms to help identify these fraud-related applications. After implementing the algorithm, the company started to give ex-ante warnings to the loan applicants whose applications were identified to be fraud-related ("the intervention").

In this study, our identification strategy is similar to a field experiment. The treated samples are loan applications (including ex-post performance) after the machine-learning-based intervention was applied. The control samples are similar loan applications when no such technology is used to help prevent fraud. We first show that these two samples are similar in all the dimensions that we can observe. Next, we show that the treated sample indeed has a lower occurrence of fraud ex-post, and financial losses are also much lower than the control sample. Last but not least, we compare the

[9] There are legal debates on whether and under what circumstances victims are still obligated to pay back these loans.

machine learning algorithm adopted in the intervention to traditional logistic regressions, and find that the machine learning algorithm indeed has a better performance. The evidence suggests that big data analyses and machine learning techniques are useful in helping identify cyber-telecom fraud even when the criminals themselves have no data available in the analysis.

A key open question in research on improving the quality of household financial decisions is whether targeting a lack of financial literacy is more effective, or targeting behavioral biases (Fernandes, Lynch, and Netemeyer, 2014). In our study, the fraudulently-induced borrowing cases naturally separates into (1) cases where victims do not know that they are borrowing (representing a lack of financial literacy), and (2) cases where victims know but are overconfident about the high monetary returns the fraudsters promise (representing a type of behavioral bias). We find that inexperienced users are particularly likely to fall for frauds targeting financial literacy, whereas frauds targeting overconfidence take victims more universally. Female users are more likely than male to fall victim regardless of the fraud type. The Platform's intervention, taking the form of a "just-in-time" education (telling victims that this is a loan) as well as persuasion (asking victims to reconsider the risks of the too-good-to-be-true returns), is effective in preventing financial mistakes in both types of frauds, albeit it takes longer time to persuade victims in fraud cases targeting overconfidence.

Our paper makes several contributions. Firstly, it contributes to the rising line of research on big data analyses. According to IBM (2013), "big data is a term applied to datasets whose size or type is beyond the ability of traditional relational databases to capture, manage and process the data with low latency. Big data has one or more of the following characteristics: high volume, high velocity or high variety." "Big data analytics is the use of advanced analytic techniques against very large, diverse data sets that include structured, semi-structured and unstructured data, from different sources, and in different sizes from terabytes to zettabytes." In both accounting and finance literature, scholars have tried to extract information from financial reports by making textual analyses of the reports (e.g., Li, 2010; Loughran and McDonald, 2011; Li, Lundholm, and Minnis, 2013; Lang and Lawrence, 2015; Frankel, Jennings and Lee, 2016; Hoberg and Phillips, 2016). Media is another source of data (e.g., Tetlock, 2007; Tetlock, Saar-Tsechansky, and Macskassy, 2008; Tetlock, 2010; Tetlock, 2015). Recently, with the availability of data from the Internet and mobile devices, more research is carried on using unstructured data from a variety of sources (e.g., Liao, Wang, Xiang, Yan and Yang, 2020).

Secondly, it contributes to the growing strand of literature that applies the new machine learning technology to traditional research questions. For example, Gu, Kelly, and Xiu (2020) use machine learning methods to measure asset risk premium. Giglio, Liao, and Xiu (2019) develop a machine learning method to perform multiple hypothesis testing in order to limit data snooping. Erel, Stern, Tan, and Weisbach (2018) show that machine learning algorithms can help identify better performing corporate directors. Li, Feng, Shen, and Yan (2020) apply machine learning to capture corporate culture. Easley, Lopez de Prado, O'Hara, and Zhang (2020) apply the method to the micro-structure field.

Thirdly, our study contributes to the new line of studies on Fintech. This line of studies explores the economic impacts of the application of Fintech by both traditional financial institutions and the start-up Fintech firms. For example, Agarwal, Qian, Ren, Tsai, and Yeung (2020) and Berg, Burg, Gombović, Karolyi, and Puri (2020) show that digital footprints can be used to model borrower's creditworthiness. Dai, Han, Shi, and Zhang (2020) show that digital footprints are useful for debt collection. Liao, Martin, Wang, Wang, and Yang (2020) show that informing borrowers that their loan performance will be reported to the public credit registry affects their loan take-up and repayment decisions. Our paper differs from these studies as we explore a unique situation when advanced technology has to be used to identify fraud when no information is available on the criminals.

In addition, our paper contributes to the literature on the role of financial literacy and behavioral biases in suboptimal financial actions. There is a growing literature that study the impact of financial literacy on several different financial behaviors and outcomes, such as planning for retirement and wealth accumulation (Ameriks, Caplin and Leahy, 2003; Stango and Zinman, 2009; van Rooij, Lusardi and Alessie, 2012), investment behaviors (van Rooij, Lusardi and Alessie, 2011; Graham, Harvey and Huang, 2009), and credit behaviors (Stango and Zinman, 2009; Brown, Grigsby, van der Klaauw, Wen and Zafar, 2016). Understanding the effect of financial literacy on people's behavior is an important topic in finance as it relates to the usefulness of investor education. However, it is difficult to differentiate financial literacy from behavioral biases. Our dataset and special setting allow us to make this differentiation so as to make an important contribution to the literature.

Last but not least, our paper contributes to the literature on fraud. In the past, studies mainly pay attention to company's fraud such as misreporting (e.g., Dechow, Ge Larson and Sloan, 2011; Yu and Yu, 2011; Khanna, Kim and Lu 2015; Karpoff, Koester, Lee and Martin, 2017; Amiram, Bozanic, Cox, Dupont, Karpoff, and Sloan 2018). Previous research on individual financial fraud or scams in the Western context focuses on older investors (Gamble, Boyle, Yu and Bennett, 2013; DeLiema, Deevy, Lusardi and Mitchell, 2020; Lee, Cummings and Martin, 2019; Kumar, Muckley, Pham and Ryan, 2018). Victims of cyber-telecom financial scams in our dataset are distinguishably younger. Young female users in our dataset are significantly more prone to cyber-telecom financial scams. This natural as the young is the largest user group on the Internet. It is consistent with an operational experience explanation (Modic and Lea, 2014) that young individuals might not have had as much financial experience or experience with financial scams as older individuals.

The rest of the paper is organized as follows. Section II introduces the background information regarding the company's consumer loan business and its AI technology. Section III describes the data and presents empirical evidence. Section IV investigates the impact of financial literacy on potential victims' behavior. Finally, Section V concludes the paper.

II. Institutional Background and AI Technology

a) The Platform

With the development and expansion of the financial market in China, rising credit risks put traditional financial institutions under increasing operating pressures. As banks venture into new pools of customers, the share of borrowers with high-quality hard information in the traditional sense declines, and the cost of customer acquisition rises, forcing banks to slow down growth. Fintech firms, on the other hand, have a greater capacity to process non-traditional types of information, using machine learning algorithms, into signals of risks in credit lending. Fintech firms begin to thrive using this advantage. Specifically, they do so by either providing loan risk management services to traditional banks, or by serving as alternative lenders leveraging advanced risk management capabilities in-house, or both.

We study cyber-telecom financial fraud prevention at the Fintech firm Du Xiaoman Financial, formerly Baidu Finance, and spun off as a standalone company in 2018. Similar to Ant Financial (currently renamed as Ant Group), Du Xiaoman is a multi-business FinTech firm. In 2013, Baidu obtained a third-party payment license, and launched its wealth management platform in the same year, getting a mutual fund sales license shortly in 2014. Baidu's financial services business group is formally established at the end of 2015. In 2017, Baidu and CITIC Bank formed a joint venture Baixin Bank and obtained the license to provide online banking and lending services from the China Banking Regulatory Commission (CBRC). In April 2018, Baidu Finance was officially split from Baidu and renamed to "Du Xiaoman" to achieve independent operation.

As the largest Internet search company in China, Baidu has developed advanced AI algorithms and 14 Internet and mobile applications that each have more than 100 million users. Together, Baidu's user base covers 95% of Chinese Internet users. Its first flagship product, Baidu Search, receives more than 10 billion search requests daily, and hundreds of millions of users send more than 6 billion messages every day using Baidu's applications. Baidu's other flagship product, Baidu Map, is the most frequently used mapping service in China and, in combination with the firm's AI capacity, has led to Baidu's Appolo autonomous driving venture. As a Fintech company, Du Xiaoman inherits Baidu's capabilities in artificial intelligence and provides banks and Internet financial institutions (such as itself) with loan risk management solutions, covering the three stages of loan origination, loan maintenance/servicing, and delinquency management/recovery.

Driven by huge profits, the methods, techniques, and targets of cyber-telecom fraud are always changing. While online loans are becoming more and more efficient and prevalent, providing credit supply to small borrowers not covered by traditional financial institutions. In the meantime, the cyber-telecom swindlers also shift their target to the vast number of potential users of online lending platforms, from whom borrowers are able to get a large amount of money in a short time. We focus on this special type of cyber-telecom fraud, where criminals induce innocent people to borrow through real online finance platforms and transfer money to criminals' own accounts. As one of the leading Fintech platforms in China, Du Xiaoman (hereafter, the Platform) naturally becomes a main target of this kind of attack.

The Platform has noticed cyber-telecom fraudulently-induced borrowing cases since May 2019. In the first few months, there were about 20 cyber-telecom fraud victims on a daily basis, with an average loss of about 25,000 RMB. Some of the victims were induced to borrow from several platforms at the same time, resulting in rather low payback ability. Cyber-telecom fraudulently-induced borrowing causes financial losses for both the users and the Platform, as about half of the victims default on their loans.

However, the existing risk-control rules and models are not applicable to this specific cyber-telecom fraud scenario. The difficulty comes from the fact that the criminals themselves do not show up in the database, so there are no digital footprints available for these scammers. It is not just analyzing the borrowers themselves using big data, including digital footprints, to assess their creditworthiness or ability/willingness to pay back debt, it involves assessing the motivation of the borrowing behaviors and linking the borrowers to someone else who is conducting frauds. To make it more difficult, cyber-telecom fraud criminals are often strangers to the victims, and there is not much data linking the criminals with the victims. Despite all these difficulties, the Platform decided to develop a big-data and machine-learning based anti-fraud system as an intervention.

b) The Gradient Boosting Decision Tree (GBDT) Algorithm

The Platform's intervention is based on the Gradient Boosting Decision Tree (GBDT) machine learning algorithm. GBDT (Friedman, 2001) is a member of the Boosting family of integrated learning.

The GBDT is an iterative algorithm. In each iterative step, the GBDT algorithm fits the best "weak learner," usually a simple nonlinear binary predictor using a constrained and small number of dependent variables, using data from the prediction error from the existing predictive function (the "strong learner"), and then adds the weak learner to the strong learner subject to a learning rate.

The weak learner's functional form in the GBDT algorithm is the Decision Tree model (Lewis, 2000). The Decision Tree model is a simple but nonlinear function of a constrained number of dependent variables for binary outcome prediction. The Decision

Tree model starts from the first layer, where it finds a single variable and a threshold value to partition a dataset into two subgroups, and fit a simple constant for each observation in the subgroup. It then proceeds to the next layer, where each subgroup is further partitioned into two smaller subgroups. The structure of the Decision Tree model resembles its name, where the data set is broken into "tree branches," and the subgroups in the highest layer are the "tree leaves."

Decision trees with a small number of layers is a parsimonious way to allow for interactive effects in predicting binary outcomes. When fit with a large number of layers, decision trees are prone to overfitting. The GBDT algorithm, by iteratively estimating and summing decision trees with a small number of layers, reduces the chance of overfitting while at the same time allow rich interactions of variables in the data to help predict the binary outcome.

The pseudo-code for the GBDT algorithm is as follows:

- Input is the training set sample $D = \{(x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m)\}$, the maximum number of iterations T, a loss function L, a learning rate λ,.and the depth (number of layers) for the weak learner K
- The output is a strong learning of the binary outcome variable given predicting variables: $f(x)$

1) Initialize the weak learner

$$f_0(x) = \arg\min_c \sum_{i=1}^{m} L(y_i, c)$$

2) In each iteration $t = 1,2, \ldots, T$:

    a) For the sample $i = 1,2, \ldots, m$, calculate the negative gradient

$$r_{ti} = -\left[\frac{\partial L(y_i, f(x_i))}{\partial(f(x_i))}\right]_{f(x)=f_{t-1}(x)}$$

b) Use (x_i, r_{ti}) $(i = 1, 2, \ldots., m)$ to fit the t-th decision tree, and its corresponding leaf node area is $R_{tj}, j = 1,2, \ldots, J$. Where J is the number of leaf nodes of the regression tree t with depth K.

c) For each leaf area $j = 1, 2, \ldots., J$ calculate the best fit constant value

$$c_{tj} = \arg\underset{c}{min} \sum_{x_i \in R_{tj}} L(y_i, f_{t-1}(x_i) + c)$$

d) Update the strong learner with the weak learner, subject to the learning rate:

$$f_t(x) = f_{t-1}(x) + \lambda \sum_{j=1}^{J} c_{tj} I(x \in R_{tj})$$

3) Get the strong learner $f(x)$:

$$f(x) = f_T(x) = f_0(x) + \sum_{t=1}^{T} \sum_{j=1}^{J} c_{tj} I(x \in R_{tj})$$

The Platform uses a training sample with a variety of variables about the borrower described in the next section, and an ex-post labeled binary outcome variable of being fraudulently-induced to initiate the GBDT algorithm. The GBDT algorithm specifies (and experimented with) the following parameter settings: a learning rate of 0.1 (0.05, 0.1, 0.5), a maximum number of iteration of 100 (100, 200), and a maximum depth of the decision tree in each iteration of 5 (3, 4, 5, 6). The GBDT algorithm specifies a logistic loss function.

III. Data and Empirical Results

In this section we describe the data and identification strategy for our analysis. Our identification strategy is similar to a field experiment. The treated samples are loan applications (including ex-post performance) after the intervention was applied. The control samples are similar loan applications when the machine-learning-based intervention was not used to help prevent cyber-telecom financial fraud.

[[INSERT Figure 2 about Here]]

Figure 2 illustrates the intervention received by the treatment group in our anti-fraud experiment. An applicant makes a loan usage request if he/she decides to take up the loan after observing the loan terms. In the control group, there is no intervention to prevent cyber-telecom fraudulently-induced borrowing from the Platform at the loan usage stage[10]. For the treatment group, however, the loan usage requests go through the anti-fraud screening as an additional step. The anti-fraud system gives a score for each loan application, with a higher score indicating a higher probability of cyber-telecom fraudulently-induced borrowing. For the low fraud score applicants, the loan usage request gets approved without intervention. For the high fraud score applicants, the Platform sends alerts and gets feedback from them. Most of the cyber-telecom fraudulently-induced applicants would realize the fraud and withdraw the loan usage requests. For those who insist that it is not fraudulently-induced borrowing, their loan usage requests would also get approved. Our sample contains all the loan usage requests of the control group and the treatment group.

The data is at the loan level. We define a loan usage request as Fraud=1 if it is a cyber-telecom fraudulently-induced borrowing case, which is identified based on (a) applicants' feedback to the Platform's warning phone calls, and (b) post-borrowing feedback from borrowers. The loan applications that indeed suffer a loss of cyber-telecom fraudulently-induced borrowing are labeled as Use=1 in our sample, which means a cyber-telecom fraudulently-induced applicant successfully takes up the loan and transfers money to the fraudster's accounts. Loss is the amount of loss caused by cyber-telecom fraud, and is defined as 0 when Use=0. The main purpose of our

[10] In fact, the Platform reviews the loan usage requests and intercepts abnormal deals as a routine procedure before and after the anti-fraud system was applied. However, this routine review procedure has nothing to do with cyber-telecom fraudulently-induced borrowing. So we do not show this step in Figure 3 to make the flow diagram more straightforward.

empirical analysis is to evaluate the treatment effect on the probability of Use and the amount of Loss.

a) Sample Balance of the Treatment and Control Groups

To examine the quality of randomization, we plot applicant characteristics for control and treated groups in Figure 3. The distribution of gender, age, education, income, apply amount and deal approval rate is nearly identical in the control group and the treatment group.

[[INSERT Figure 3 about Here]]

We can also use these summary statistics to characterize loan applicants more generally. The majority of applicants are young males. The applicant base is dominated by individuals younger than 35. Male applicants account for 66% (68%) of the treated and control sample, respectively. As the disclosure of education is voluntary, most of the applicants do not disclose this information. As for income, most applicants earn 4,000-8,000 RMB per month. Over half of the applicants apply for less than 5000 RMB. Only less than 10% loan applications get rejected in both control and treatment groups.

To further show differences in the probability of cyber-telecom fraudulently-induced borrowing across different age and gender groups, we present the presence of Fraud-induced loan usage requests (Fraud) and successful credit use following a fraud-induced loan application (Use) in several sub-samples in Table 1. Panel A shows this information separately for male and female applicants in control and treated groups. Panel B shows Fraud-induced applications and credit use in different age groups of the control sample, and Panel C shows the corresponding information for the treated sample.

[[INSERT Table 1 about Here]]

As shown in Panel A, the probability of Fraud-induced loan applications (Fraud) for female loan applicants is over 12(7) times that of male loan applicants in the control (treatment) group. The probability of Fraud-induced credit use (Use) shows a similar structure. The average loss per capita is furthermore 16% (225%) greater for female versus male applicants induced by fraudsters, and the average loss per potential victim shows a similar pattern.

As shown in Panel B and Panel C, the probability of loan applicants being induced by fraudsters decreases with age. However, the average loss per capita tends to be larger for more mature applicants in the control group. The treated group does not show a similar pattern, possibly as a result of the small number of Fraud-induced credit use incidences post-treatment. All three panels show a large decline in the probability of Fraud-induced credit use (Use) in the treated group. For example, the likelihood of Use conditional on Fraud for applicants between 26 to 30 years old falls from the control group's 95% to the treated group's 2.88%.

We also present in Table 2 the case characteristics of the Fraud-induced loan usage requests, separated into further sub-samples by (1) control versus treated, (2) whether the machine learning algorithm in the treated group successfully detected the fraudster's influence on the applicants, and (3) whether the loan applicant proceeded with credit use even with the fraud alert. Panel A shows the Fraud-induced loan applications in the control group, out of which there is 95.56% probability of Use. Panel B and Panel C show a much smaller number of the Fraud-induced loan applications unidentified (39 applications), versus those identified (346 applications) by the machine learning algorithm. In other words, the machine learning algorithm has a detection rate of 89.87% (346/385).

Panel D shows the Fraud-induced applications alerted by the anti-fraud system, but the applicant failed to see through the fraud, taking up the loan nonetheless, and transferred the money to the fraudsters (4%, 14/346). As shown in Panel D, the Fraud applicants who ignore the Platform's alert are almost young females with relatively high Apply Amount.

[[INSERT Table 2 about Here]]

b) Who are more likely victims of cyber-telecom financial frauds?

In this section, we analyze what type of individuals are more likely victims of fraudulently-induced borrowing. Different from previous research on financial fraud or scams in the Western context focuses on the older population (Gamble et al. 2013, DeLiema et al. 2018, Lee et al. 2018, Kumar et al. 2018), victims of cyber-telecom fraudulently-induced borrowing in our dataset are distinguishably younger.

To make interpretation of the result possible, we carry out logit and probit regressions at the loan level. The dependent variable is Fraud, a dummy variable that equals 1 if the loan usage request is a case of cyber-telecom fraudulently-induced borrowing. Explanatory variables include age, gender, income, apply amount, total credit in the last 12 months (excluding mortgage loans), number of loan account in the last 12 months, historical consumer loan amount (settled and outstanding), days after the last credit report inquiry and the credit card utilization rate. The results are presented in Table 3.

[[INSERT Table 3 about Here]]

The results in Table 3 illustrate that young females are more likely to become potential victims of cyber-telecom fraudulently-induced borrowing. This confirms the patterns presented in Tables 1 and 2. The results in all columns show that female applicants have a much higher likelihood of making loan usage requests induced by fraudsters than male applicants in the same age group, as demonstrated by the coefficient on gender and the interaction terms of gender and age.

Younger applicants have higher probability of Fraud for both female and male. Applicants applying for a higher credit amount are also associated with a higher likelihood of being manipulated by fraudsters, with the Apply Amount>10000 group having the highest logit and probit coefficients. Applicants at the Platform with lower or zero credit experience have a higher risk of being manipulated by fraudsters, indicated by the coefficients of external credit record variables.

Finally, if the applicant has credit report inquiry records on the day of loan usage request, i.e. the applicant tries to borrow from multiple institutions at the same time, there is a higher risk of fraudulently-induced borrowing, as shown by the coefficient of "Days After Last Inquiry=0". This is consistent with an operational experience explanation (Modic and Lea, 2014) that younger account users might not have had as much real world experience with scams as older individuals.

c) The Treatment Effect

In this section, we evaluate the effect of the Platform's big-data and machine-learning based intervention by comparing the probability of successful Fraud-induced credit use (Use) and customer loss (Loss) between the treated and control groups. Table 4 reports the results of the intervention on the treated group. There are 385(315) loan usage requests induced by fraudsters in the treated (control) group.

Conditional on ex-post successful credit use, the average loss is 23,386(29,032) RMB. The probability of fraud-induced borrowing in the treated (control) is 0.18%(0.17%). There is no statistical difference in terms of the probability of being induced by fraudsters or in terms of the average loss conditional on credit use between treated and control groups, as illustrated by t-statistics. This further confirms that the treated and the control groups are similar except for the treatment.

[[INSERT Table 4 about Here]]

Despite the ex-ante similarity of the treated and control groups, the number of ex-post credit use is 301 in the control group, yet only 35 in the treated group. Probability of successful credit use (Use) conditional on being induced by fraudsters (Fraud=1) declines from 95.56% (=301/315) to 9.09% (=35/385), and the average loss conditional on being induced by fraudsters drops from 27741 RMB to 2126 RMB. The machine learning algorithm identifies 13,298 applications as high fraud risk and sends alerts to these applicants, among which 346 are correctly identified. Model Accuracy is 2.60% (=346/13,298), and Detection Rate is 89.87% (346/385). In short, these improvements in the outcome for individuals targeted by financial scams in the treated sample versus the control sample are significant statistically and economically.

The machine learning algorithm significantly improves the efficiency of using calls to intervene on potential victims of financial fraud. To see this, we further calculate the effect of randomly warning calls. As 0.18% of the treatment group are fraudulently-induced money borrowing cases, if we randomly choose 13,298 applicants (the same number as the anti-fraud system) to make warning calls, this alternative randam intervention would on average only catch 24 (=13,298*0.18%) fraud cases, which covers only 6.23% of all the fraud cases in the treated sample, compared to the substantially higher detection rate of 89.87% for the intervention with the help of the machine learning algorithm, even with the same number of calls.

We can estimate the economic benefits created by the anti-fraud system for loan applicants and the Platform using numbers in Table 4. The actual loss of treated group due to applicants being targeted by cyber-telecom fraud is 818.5K RMB. If there were no intervention from the anti-fraud system, the probability of Use conditional on Fraud (~95%) and the average loss per capital (taking the average of treated and control, ~25K RMB) would be similar between the treated and control groups. In that case, the incidences of Use would be 366 (=385*95%) for the treated group, and the counterfactual loss for individual victims of cyber-telecom fraud would reach 9.15 million (=366*25K) RMB.

In other words, according to the simple calculation, the intervention saved over 8 million RMB for applicants during the three-week experiment period, reducing customer loss by over 90%. This is a substantial economic benefit taking the short time length of the experiment into account. The loss prevented at the individual level is also at the order of magnitude of one year's disposable income for the average person in China, suggesting the micro-level impact is also sizable. Moreover, some of the fraud-induced loan applicants in reality apply for loans on several different platforms, so the economic size of the treatment effect could be understated.

Next, we reaffirm that the significant drop in the probability of loss conditional on cyber-telecom fraud and the reduction in the value of customer loss is not driven by fewer customers being targeted by fraudsters, through regression evidence on the similarity of the probability of being targeted by fraudsters across the treated and control sample. Table 5 compares the probability of fraud for control and treatment groups using the logit model and the probit model, respectively, at the loan usage request level. The dependent variable is Fraud, a dummy variable equals to 1 if the loan usage request is a case of cyber-telecom fraudulently-induced borrowing. Treatment=1 for the treatment group and 0 for the control group. The coefficients on Treatment indicate the differences in Fraud probability between treated and control groups. In all the four specifications, the coefficients of Treatment are not significant, which shows that the likelihood of being manipulated by fraudsters ex-ante (before the anti-fraud alert) is similar between the treated and control groups.

[[INSERT Table 5 about Here]]

Finally, we show regression evidence for effects of the intervention on the probability of actual fraud-induced credit use due to cyber-telecom fraud (Use) and value of customer loss (Loss) in Table 6. We use the logit model and the probit model, respectively, for the incidences of fraud-induced credit use, and OLS for the value of customer loss, at the loan usage level. The coefficients on Treatment indicate the differences in probability of fraud-induced credit use and in customer financial losses between the treated and the control groups. In all four specifications, the coefficients of Treatment are significant negative at 1% significance level, which means the probability of fraud-induced credit use and customer loss are statistically lower for the treated group, which confirms the finding in Table 4.

The corresponding average marginal effect of Treatment for the logit model in column (1) is -0.17%, i.e. that the probability of fraud-induced credit use drops by 0.17% after treatment. This effect is significant economically as the probability of fraud-induced credit application is 0.18% (=385/213,584) in the treatment sample, meaning that the treatment successfully identified intervened on the great majority of fraud cases in the treatment sample.

The OLS results presented in column (3)-(4) indicate that all else equal, average loss per customer is 67.75RMB lower, and average loss conditional on being targeted by a fraudster is 20534.22RMB lower for the treatment group, indicating that the intervention based on the machine learning algorithm prevented considerable financial loss for individuals on the online borrowing platform.

[[INSERT Table 6 about Here]]

d) Back Test

In this section, we show the results of a back test, i.e. applying the algorithm on data for the control group, and evaluate the performance on fraud identification. If the decline of the probability of Use and Loss in the treatment group is indeed the effect of the intervention, the algorithm should also be able to detect the fraud cases in other samples. We report the result of the back test in Figure 4. The fraud score distribution of the normal loan usage requests concentrates on the left side, while the fraud score distribution of the normal loan usage requests is more uniform. With a cut-off point of 0.3, the anti-fraud system identifies 17,622 loan usage requests as high fraud risk, among them 281 are correctly identified (over total 315 fraud cases). The detection rate is very similar to the treatment group (89.21% vs 89.87%). Model accuracy is slightly lower than the treatment group (1.59% vs 2.60%), maybe because of additional variables collected for the treatment group included in the anti-fraud prediction system that were retrospectively not collected for the control group.

[[INSERT Figure 4 about Here]]

e) Does the GBDT Algorithm Perform Better than Logistic Regressions?

In this section, we compare the predictive power of conventional binary outcome regressions with the Platform's anti-fraud system based on machine learning, specifically the GBDT algorithm for binary outcome prediction. We compare the logit model (2) of Table 3, the conventional binary outcome regression model with the highest pseudo R-sq. among models in Table 4 in predicting Fraud, with the Platform's anti-fraud system based on the GBDT machine-learning algorithm. We present in Figure 5 the receiver operating characteristics curves (ROC curve) and the area under the curve (AUC) for the logit model and the anti-fraud system.

An important consideration in evaluating binary outcome prediction algorithms is the tradeoff between the model accuracy (the ratio of cases correctly identified over total cases identified) and the detection rate (the ratio of cases correctly identified over all correct cases). Put differently, this is the tradeoff between false positives and false negatives. For example, one can set a high threshold for the logit model, which improves the model accuracy by reducing false positives, but it will simultaneously worsen the detection rate, by increasing false negatives. Vice versa, one can set a low threshold for the logit model, which achieves a better detection rate at the sacrifice of model accuracy.

The ROC curve shows the performance of a classification model at all classification thresholds by plotting sensitivity (true positive) against 1- sensitivity (false positive). The closer the curve comes to the 45-degree diagonal of the ROC space (ROC curve for random classification model), the less accurate the test. The closer the curve comes to the upper left corner of the ROC space (ideal classification model), the more accurate the test. To compare different classifiers, it can be useful to summarize the performance of each classifier into a single measure. One common approach is to calculate the area under the ROC curve (AUC). A classifier with high AUC can occasionally score worse in a specific region than another classifier with lower AUC. But in practice, the AUC performs well as a general measure of predictive accuracy.

[[INSERT Figure 5 about Here]]

As shown in Figure 5, the ROC curve for the anti-fraud system are closer to the upper left corner compared to the ROC curve for the logit model. The AUC for the anti-fraud system and the logit model are 97.64% and 94.74%, respectively, which means a 3% increase in predicting power (97.64%/94.74%-1). The result of Chi2 test indicates that we can reject the H0 hypothesis that the two models have the same predicting accuracy at 1% significance level. We do not present the ROC curve for the probit model (4) of Table 3, as it almost coincides with the ROC curve for the logit model. In sum, the results presented in Figure 5 provide suggestive evidence that the GBDT machine learning algorithm performs significantly better than logistic regressions in detecting cyber-telecom fraudulently-induced borrowing.

IV. Frauds that Targets Financial Literacy or Behavioral Bias

In this section, we investigate the impact of financial literacy and behavioral biases on the likelihood of victimization and the effectiveness of treatment. The potential victims of cyber-telecom fraudulently-induced borrowing in our sample can be classified naturally into two groups: those who did not know they were applying for a loan and those who did know they were going through a loan application process.

The first group of potential victims fall into traps such as refund scams, false account cancellations, etc., follow the fraudsters' instructions, and they have no idea about they were applying for a loan, even if they are filling out a loan application form. This group of potential victims generally lack financial literacy. In contrast, the latter group of potential victims fall into traps like promising investment opportunity that were in hindsight to good to be believed, and unlicensed online-gambling, mistakenly believing they could make a fortune. This group of potential victims exhibits behavioral biases and more specifically, overconfidence.

The Platform keeps a record about the fraudulently-induced borrowing cases, including the tricks used by the fraudster, the number of warning calls made, and the length of each communication, making it possible for us to distinguish the two kinds of potential victims and measure the difficulty of persuading a potential victim from fraud. In our sample, potential victims who lack financial literacy accounts for about 4/5 of fraud cases.

We explore applicant characteristics associated with two types of potential victims. Table 7 shows the results of logit models and the differences of coefficients between Columns (1) and (2). The outcome variable of Column (1), Fraud_FL, equals to one if it is a fraud case that targets lack of financial literacy. Similarly, the outcome variable of Column (2), Fraud_OC, equals one if it is a fraud that targets overconfidence. Similar to Table 3, the results of Column (1) indicate that young and inexperienced females are more likely to be victims of fraud that targets lack of financial literacy.

However, there are some differences when it comes to fraud that targets overconfidence. Fraud that targets overconfidence draw victims more universally across young and old, as the coefficients of Age18-25 of Column (2) are significantly smaller than that of Column (1). Historical credit experience does not affect the likelihood of fraud that targets overconfidence, as the coefficients of Total Loan in Previous 12 Month, Number of Loan Account in Previous 12 Month and No Previous Credit Inquiry[11] are not significant. In addition, compared with potential victims who lack financial literacy, those who are overconfident apply for a relatively larger amount, as the coefficient of Apply Amount>10k in Column (2) is significantly higher than that of Column (1).

Young and inexperienced users are more likely to be victims of fraud that targets lack of financial literacy, whereas fraud that targets behavioral biases draw victims more universally across young and old, experienced and inexperienced users. Female users are more likely to be victims of both types of frauds.

[[INSERT Table 7 about Here]]

A key open question in the literature on improving quality of individual financial decisions: Are interventions targeting financial literacy more effective (e.g. financial education), or those targeting behavioral biases (e.g. nudging)? Our setting allows us to distinguish victimization due to a lack of financial literacy or due to over-confidence. Specifically, the intervention takes the form of a call (often a robocall), where the user is first asked whether she knows she is applying for a loan (and educated if not knowing), and then asked whether she is promised returns that are too-good-to-be-true (and tries to persuade if indeed the case). Hence, the intervention in our setting combines "just-in-time" financial education with persuasion.

Aiming to provide information that may help answer this open question, we analyze behavioral responses that are collected on the cyber-telecom financial fraud victims

[11] As the central bank keep the loan inquiry records for 2 years, No Previous Credit Inquiry =1 means the applicant does not have credit experience in the past 2 years.

when the treatment intervention is applied. That is, whether they are able to be persuaded (and thus preventing the suboptimal action), and how difficult they are to be persuaded (and thus resources it takes to effectively correct the suboptimal action), i.e., who are not receptive to listening to the warnings from the platform. We take particular attention on whether the intervention is effective on victims of frauds targeting a lack of financial literacy, or of frauds targeting overconfidence, or both, and the time and resources it takes in order to successfully intervene in either cases.

We report the findings on the treatment effectiveness on behavioral biases versus lack of financial literacy in Figure 6. We present the difficulty of persuading two different types of potential victims from fraudulently-induced borrowing, measured by the number of warning calls made and the total length of warning calls. As shown in Panel A, a larger proportion of potential victims lacking financial literacy could be persuaded by only 1 warning call, while a larger proportion of overconfident potential victims need more than 3 warning calls to see through the deception. As shown in Panel B, over a half of overconfident potential victims falls into the group that takes the longest time on the call in order to be persuaded, almost twice the proportion of potential victims lacking financial literacy that takes a long time to persuade. The results of Figure 6 indicate that potential victims lacking financial literacy are more willing to listen to the Platform's warnings than overconfident potential victims. It is relatively more difficult to persuade potential victims with behavioral biases, with more warning calls and longer communication time.

In sum, we find evidence that it takes significantly longer to persuade users that fall victim to this type of fraud due to over-confidence, compared to users that fall victim due to a lack of financial literacy, even though both types of victims are eventually able to be persuaded.

V. Conclusion

Cyber-telecom fraud has become a more and more serious problem globally and also in China. In this study, we focus on a special type of cyber-telecom fraud, where criminals induce innocent people to borrow through real online finance platform. Since there is no digital footprints available for the fraud criminals behind the borrowing cases, identifying them becomes much more difficult. Using a proprietary dataset of online consumer financing from a large Internet company in China, we find that big data analyses and machine learning technic can help identify this type of fraud and reduce customers' financial losses.

The effects are economically and statistically significant. According to our estimation, the big-data and machine-learning based intervention prevents millions of RMB loss for customers and the Platform annually. In other words, the anti-fraud system prevents thousands of applicants from cyber-telecom fraud a year, saving tens of thousands RMB for each of them. Our results also find that young females with little or no credit experience are more likely to be cyber-telecom fraudulently-induced borrowing victims. Potential victims lacking financial literacy are more willing to listen to the Platform's warning, indicating that consumer education could play an important role in preventing cyber-telecom fraudulently-induced borrowing. The findings of this paper could be useful for individuals, Fintech companies, as well as government departments in terms of preventing cyber-telecom financial fraud.

Reference

Agarwal, Sumit, Wenlan Qian, Yuan Ren, Hsin-Tien Tsai and Bernard Yin Yeung. 2020. The Real Impact of FinTech: Evidence from Mobile Payment Technology. Available at SSRN: https://ssrn.com/abstract=3556340 or http://dx.doi.org/10.2139/ssrn.3556340.

Ameriks J, Caplin A, and Leahy J. 2003. Wealth Accumulation and the Propensity to Plan. Quarterly Journal of Economics, 118(3): 1007-1047.

Amiram, D., Z. Bozanic, J. Cox, Q. Dupont, J. Karpoff, and R. Sloan. 2018. Financial Reporting Fraud and Other Forms of Misconduct: A Multidisciplinary Review of the Literature. *Review of Accounting Studies* 23(2): 732-783.

Berg, Tobias, Valentin Burg, Ana Gombović, Andrew Karolyi, and Manju Puri. 2020. On the Rise of FinTechs: Credit Scoring Using Digital Footprints. *The Review of Financial Studies* 33:2845-2897.

Brown, Meta, John Grigsby, Wilbert van der Klaauw, Jaya Wen, and Basit Zafar. 2016. Financial Education and the Debt Behavior of the Young. The Review of Financial Studies, 29(9): 2490-2522.

China Justice Big Data Research Institute, China Justice Big Data Report – Cyber-Telecom Criminal Cases 2019.

Dai, Lili, Jianlei Han, Jing Shi, and Bohui Zhang. 2020. Digital Footprints as Collateral for Debt Collection. Working Paper.

Dechow, Patricia M., Weili Ge, Chad R. Larson, and Richard G. Sloan. 2011. Predicting Material Accounting Misstatements. Contemporary Accounting Research 28:17-82.

DeLiema M, Deevy M, Lusardi A, Mitchell OS. 2020. Financial Fraud Among Older Americans: Evidence and Implications. The Journals of Gerontology: Series B 75(4):861-868.

Easley, D., M. Lopez de Prado, M. O'Hara, and Z. Zhang. 2020. Microstructure in the Machine Age, The Review of Financial Studies, forthcoming.

Erel, I., Stern, L. H., Tan, C., & Weisbach, M. S. 2018. Selecting directors using machine learning (No. w24435). National Bureau of Economic Research.

Europol. 2019. Cyber-Telecom Crime Report 2019.

Frankel, Richard, Jared Jennings, and Joshua Lee. 2016. Using Unstructured and

Qualitative Disclosures to Explain Accruals. *Journal of Accounting and Economics* 62:209-227.

Fernandes, Daniel, John G. Lynch, and Richard G. Netemeyer. 2014. Financial Literacy, Financial Education, and Downstream Financial Behaviors. Management Science, 60 (8): 1861-1883.

Gamble, Keith Jacks and Boyle, Patricia and Yu, Lei and Bennett, David. 2013. Aging, Financial Literacy, and Fraud. Netspar Discussion Paper No. 11/2013-066, Available at SSRN: https://ssrn.com/abstract=2361151 or http://dx.doi.org/10.2139/ssrn.2361151

Giglio, S., Liao, Y., & Xiu, D. (2019). Thousands of alpha tests. Chicago Booth Research Paper, (18-09), 2018-16.

Graham, John R., Campbell R. Harvey, and Hai Huang. 2009. Investor Competence, Trading Frequency, and Home Bias. Management Science, 55(7): 1094-1106.

Gu, Shihao, Kelly Bryan, and Dacheng Xiu. 2020. Empirical Asset Pricing via Machine Learning. *Review of Financial Studies* 33:2223-2273.

Hoberg, Gerard, and Gordon Phillips. 2016. Text-based Network Industries and Endogenous Product Differentiation. *Journal of Political Economy* 124:1423-1465.

IBM. 2013. What is Big Data? – Bringing Big Data to the Enterprise, ibm.com.

Karpoff, Jonathan M, Allison Koester, D. Scott Lee, and Gerald S. Martin. 2017. Proxies and Databases in Financial Misconduct Research. *The Accounting Review.* 92(6):129-163.

Khanna, Vikramaditya, E. Kim, and Yao Lu. 2015. CEO Connectedness and Corporate Fraud. *Journal of Finance*, 70 (3):1203~1252.

Kumar, Gaurav and Muckley, Cal B. and Pham, Linh and Ryan, Darragh, 2018. Can Alert Models for Fraud Protect the Elderly Clients of a Financial Institution? Michael J. Brennan Irish Finance Working Paper Series Research Paper No. 18-16. Available at SSRN: https://ssrn.com/abstract=3230188 or http://dx.doi.org/10.2139/ssrn.3230188

Lang, Mark, and LorienStice-Lawrence. 2015. Textual Analysis and International Financial Reporting: Large Sample Evidence. *Journal of Accounting and Economics* 60:110-135.

Lee, Steven, Cummings, Benjamin F. and Martin, Jason, Victim Characteristics of Investment Fraud. 2019. Academic Research Colloquium for Financial Planning and Related Disciplines. Available at SSRN: https://ssrn.com/abstract=3258084 or http://dx.doi.org/10.2139/ssrn.3258084.

Li, Feng. 2010. The Information Content of Forward-looking Statements in Corporate Filings-A Naive Bayesian Machine Learning Approach. *Journal of Accounting Research* 48:1049-1102.

Li, Feng, Russell Lundholm, and Michaael Minnis. 2013. A Measure of Competition Based on 10-K Filings. *Journal of Accounting Research* 51:399-436.

Li, K., M. Feng, R. Shen, and X. Yan. 2020. Measuring Corporate Culture Using Machine Learning. *The Review of Financial Studies*, forthcoming.

Liao, Li, Xiumin Martin, Ni Wang, and Zhengwei Wang. 2020. The Carrot Effect of Informing Borrowers about Credit Reporting: Two Randomized Field Experiments. Working paper.

Liao, Li, Zhengwei Wang, Jia Xiang, Hongjun Yan, and Jun Yang. 2020. User Interface and First-hand Experience in Retail Investing; *Review of Financial Studies*, Forthcoming.

Loughran , Tim, and Bill Mcdonald. 2011. When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks. Journal of Finance 66(1):35-65.

Modic, David and Lea, Stephen E. G. 2013. Scam Compliance and the Psychology of Persuasion. Available at SSRN: https://ssrn.com/abstract=2364464 or http://dx.doi.org/10.2139/ssrn.2364464.

Stango V, Zinman J. 2009. Exponential Growth Bias and Household Finance. *The Journal of Finance*, 64(6): 2807-2849.

Tetlock, Paul C. 2007. Giving Content to Investor Sentiment: The Role of Media in the Stock Market," *Journal of Finance* 62:1139-1168.

Tetlock, Paul C., Maytal Saar-Tsechansky, and Sofus Macskassy. 2008. More Than Words: Quantifying Language to Measure Firms' Fundamentals. *Journal of Finance* 63:1437-1467.

Tetlock, Paul C. 2010. Does Public Financial News Resolve Asymmetric Information? *Review of Financial Studies* 23:3520-3557.

Tetlock, Paul C. 2015. The Role of Media in Finance. In S.P. Anderson, D. Stromberg, and J. Waldfogel (Eds.), Handbook of Media Economics, Vol 1B, Chapter 18, pp. 701-721. Oxford: Elsevier.

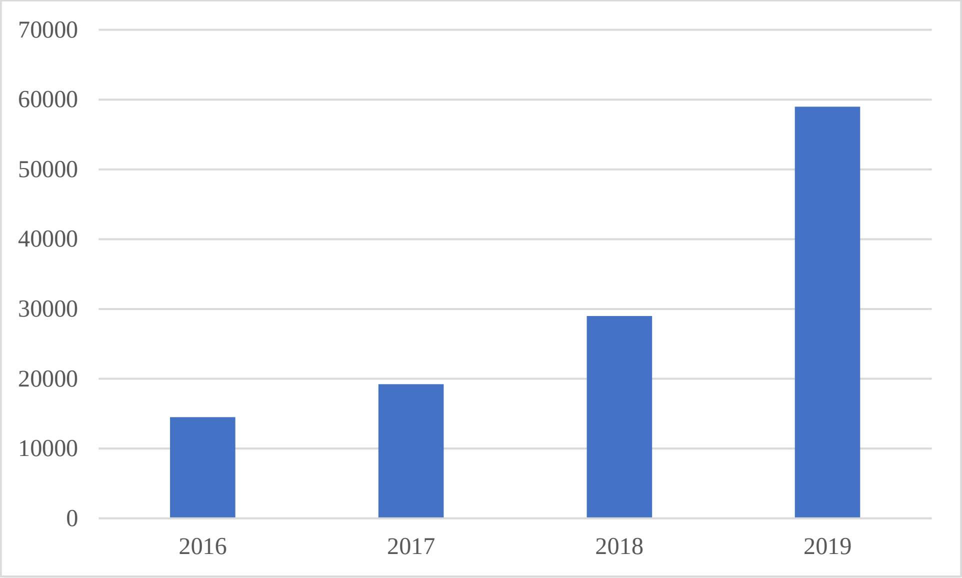
van Rooij, Maarten C. J., Annamaria Lusardi, and Rob J. M. Alessie. 2012. Financial Literacy, Retirement Planning and Household Wealth. *The Economic Journal*, 122(560): 449-478.

van Rooij, Maarten, Annamaria Lusardi, and Rob Alessie. 2011. Financial Literacy and Stock Market Participation. *Journal of Financial Economics*, 101(2): 449-472.

Yu, Frank, and X. Yu. 2011. Corporate Lobbying and Fraud Detection. *Journal of Financial and Quantitative Analysis* 46(6):1865-1891.

360 Group. 2020. Report on Trend of Cyber-Telecom Fraud.

Panel A: Number of cyber-telecom criminal cases



Panel B: Per capita losses due to cyber-telecom fraud

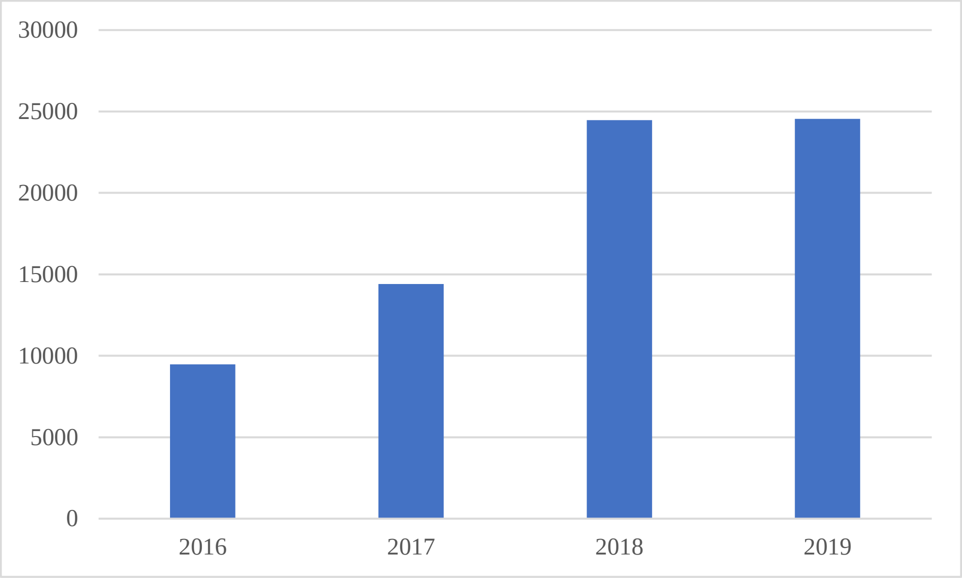
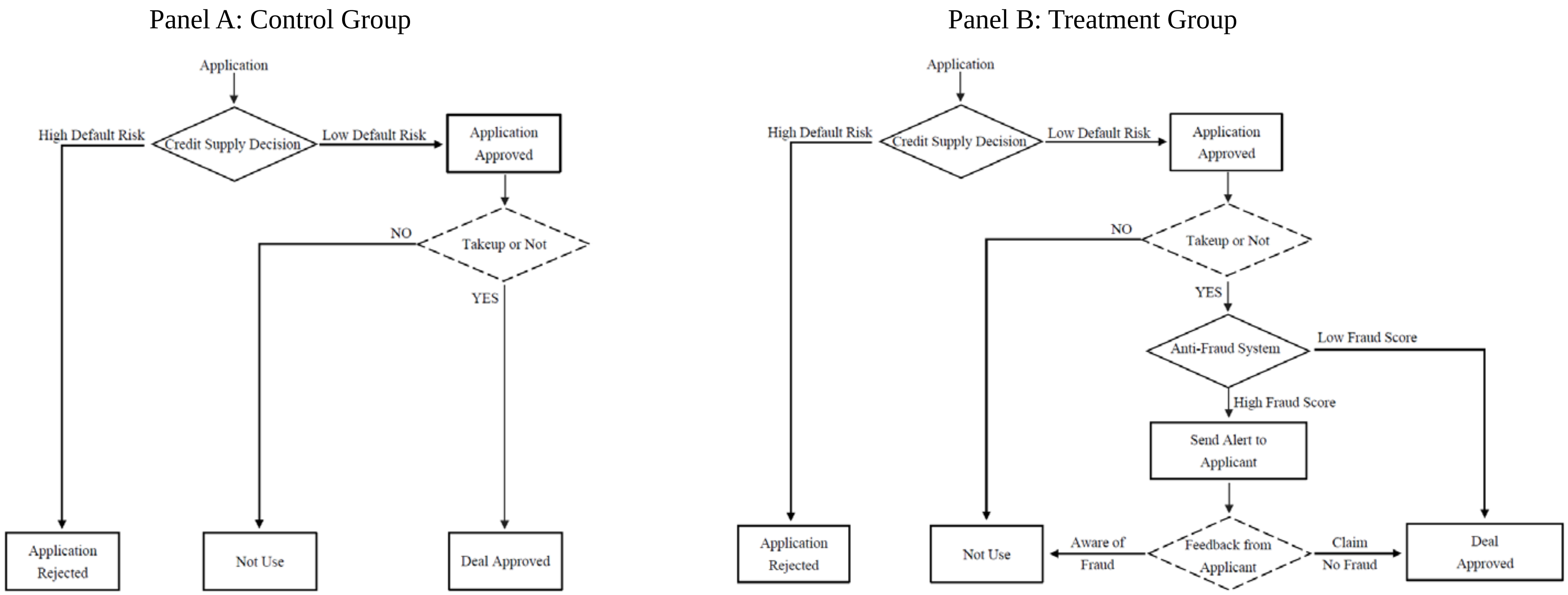


Figure 1: Number of Cyber-Telecom Criminal Cases over the Year

Notes: Panel A reports the number of cyber-telecom related criminal cases over the year. Data is from China Justice Big Data Research Institute report and Legal Daily. Panel B reports average per capita losses due to cyber-telecom fraud. Data is from 360 Internet Safety Center.



Panel A: Control Group

Panel B: Treatment Group

Figure 2: The Anti-Fraud Experiment

Notes: This figure illustrates the intervention received by the treatment group in the anti-fraud experiment. For the control group, there is no intervention to prevent cyber-telecom fraudulently-induced borrowing from the Platform at the loan usage stage. For the treatment group, however, the loan usage requests go through the anti-fraud screening as the first step. The anti-fraud system gives a score for each loan application, with a higher score indicating a higher probability of cyber-telecom fraudulently-induced borrowing. For the low fraud score applicants, the loan usage request gets approved without intervention. For the high fraud score applicants, the Platform sends alerts and gets feedback from them. Most of the cyber-telecom fraudulently-induced applicants would realize the fraud and withdraw the loan usage requests. For those who insist that it is not fraudulently-induced borrowing, their loan usage requests would also get approved. Our sample contains all the loan usage requests of the control and the treatment group.

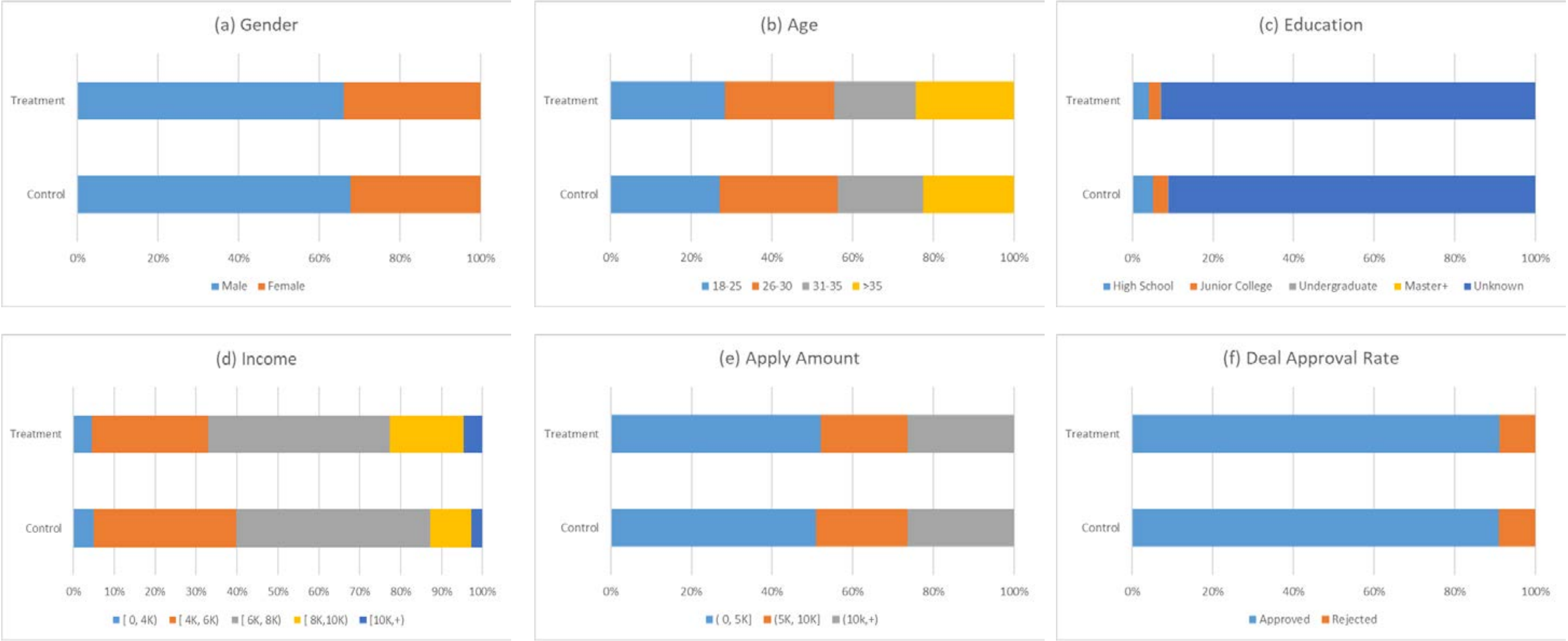


Figure 3: Characteristics of Treatment and Control Group

Notes: This figure presents the distribution of gender, age, education, income, apply amount and deal approve rate for the treatment group and control group. The y-axis signifies the percentage of applicants in each sub-category. Panel (a) plots the percentage share of male and female; Panel (b) plots the percentage share of the four age groups. Panel (c) plots the share of applicants with different education levels. Panel (d) plots the percentage share of the five income groups. Panel (e) plots the percentage share of the three apply amount groups. Panel (f) plots the share of approved and rejected loan usage requests.

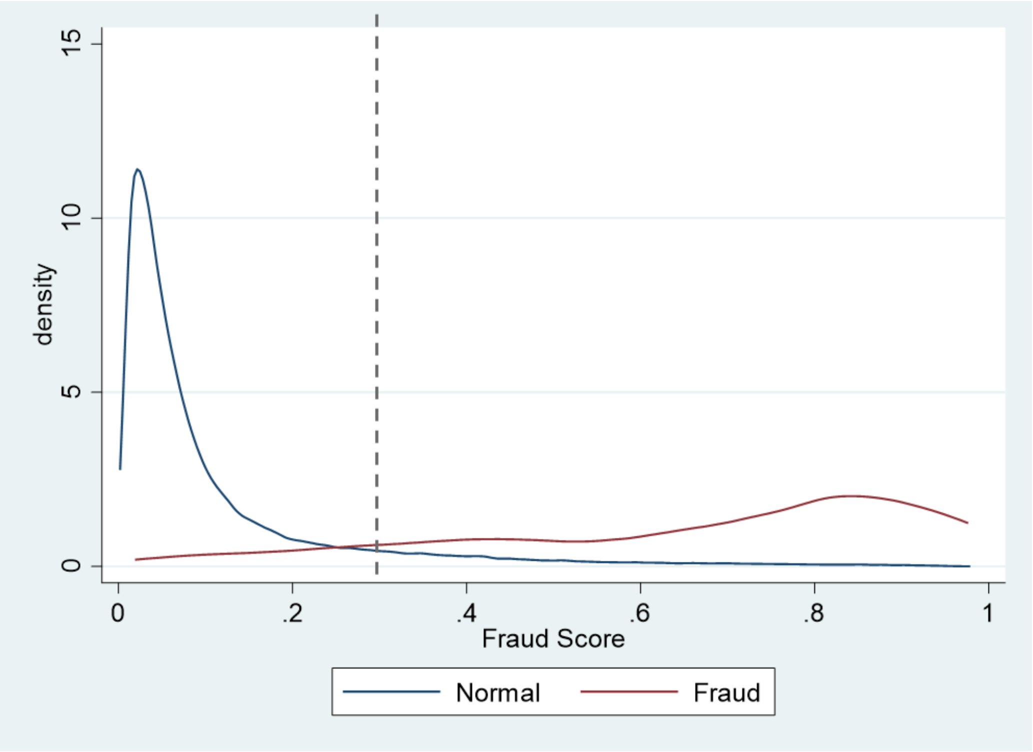
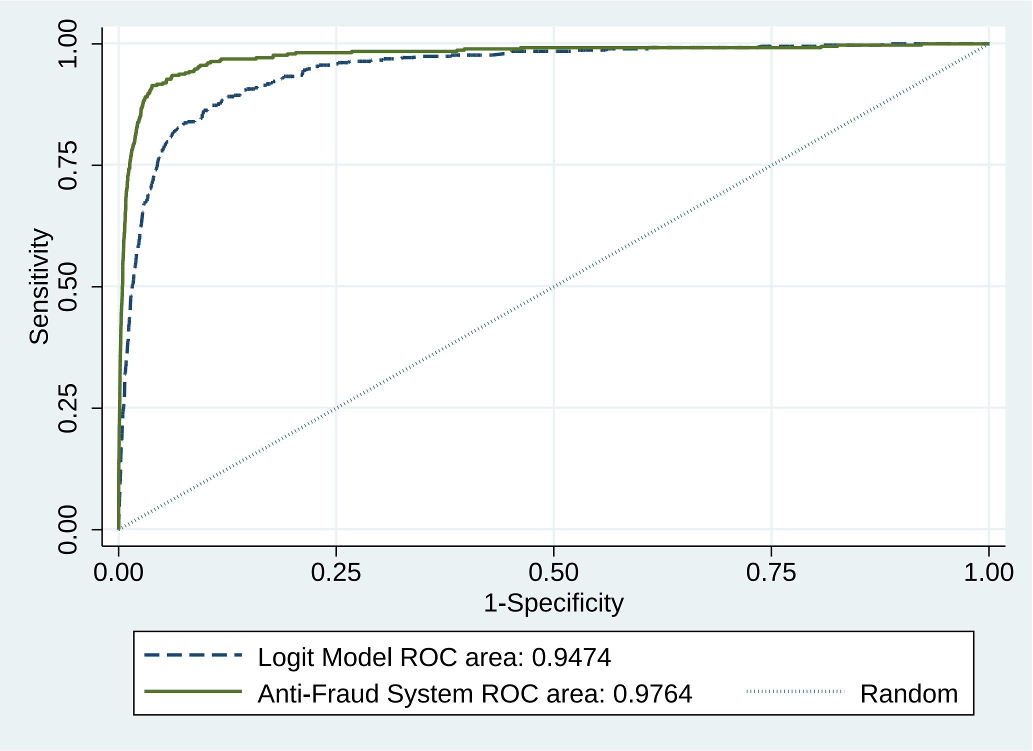


Figure 4: Back Test the Anti-Fraud System in Control Group

Notes: This figure presents the distributions of the fraud score of the control group, given by the anti-fraud system in the back test procedure. The fraud score of normal applicants is shown with the blue line, while the fraud score of cyber-telecom fraudulently-induced applicants is shown with the red line. The vertical dotted line is the cut-off point, with a fraud score higher than 0.3 defined as a high probability of cyber-telecom fraudulently-induced borrowing.

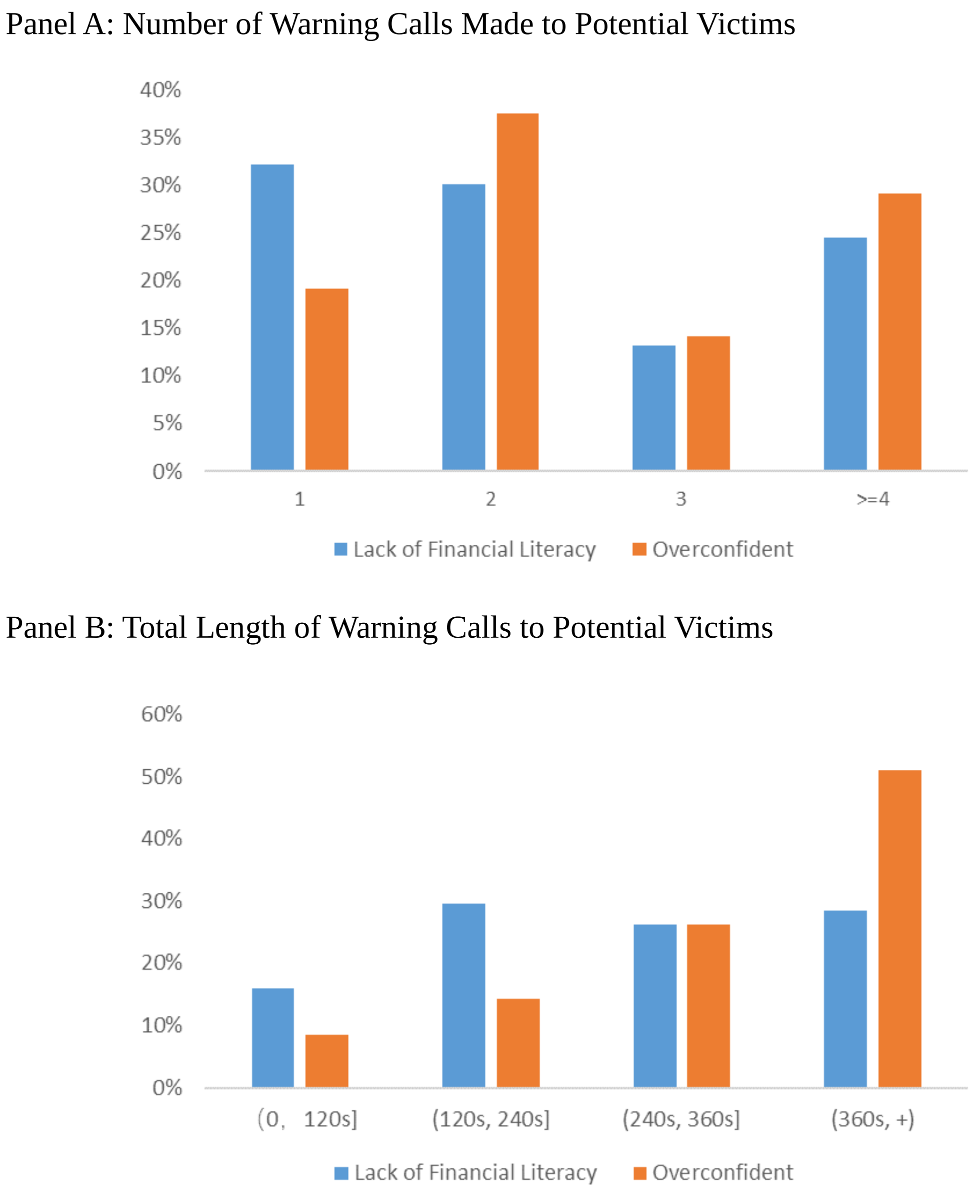


Ho: Area(Logit Model) =Area(Anti-Fraud System)

Chi2(2)=55.47 Prob>chi2=0.0000

Figure 5: ROC Curves for Logit Model and Anti-Fraud System

Notes: This figure illustrates the discriminatory power of different models by providing the receiver operating characteristics curve (ROC curve) and the area under the curve (AUC). The ROC curves of the anti-fraud system (green) and the logit model (blue) are shown in the figure. The sample only includes the treatment group, and logit model specification used is the same as Column (2) Table3. The result of the Chi2 test for AUC difference between the logit model and the anti-fraud system is also presented in this figure.



Panel A: Number of Warning Calls Made to Potential Victims

Panel B: Total Length of Warning Calls to Potential Victims

Figure 6: The Effect of Financial Literacy on the Difficulty of Persuading a Potential Victim from Fraudulently-induced Borrowing

Notes: This figure presents the difficulty of persuading two different types of potential victims from fraudulently-induced borrowing, measured by the number of warning calls made and the total length of warning calls. We divide the potential victims into two groups: those who didn't know they were applying for a loan and those who definitely know it was a loan application. The first group generally lacks financial literacy, while the latter exhibit overconfidence (mistakenly believe they could earn a very high return through investment or lottery).

Table 1: Cyber-Telecom Fraudulently-Induced Borrowing in Sub-Samples of Interest

Panel A: Male VS Female

	Male, Control	Male, Treated	Female, Control	Female, Treated
N	126,847	141,112	60,332	72,467
No. of Fraud	46	80	269	305
No. of Use	44	7	257	28
Prob. of Fraud	0.0363%	0.0567%	0.4459%	0.4209%
Prob. of Use conditional on Fraud	95.65%	8.75%	95.54%	9.18%
Average Loss per capita	25545.45	8357.14	29628.40	27142.86
Average Loss per potential victim	24434.78	731.25	28306.69	2491.80

Panel B: Different Age Groups in Control Sample

	Age<26, Control	Age[26,30], Control	Age[31,35], Control	Age>35, Control
N	50,469	54,905	39,812	41,993
No. of Fraud	138	100	43	34
No. of Use	131	95	43	32
Prob. of Fraud	0.2734%	0.1821%	0.1080%	0.0810%
Prob. of Use conditional on Fraud	94.93%	95.00%	100.00%	94.12%
Average Loss per capita	5,577.10	27,766.32	35,713.95	37,950.00
Average Loss per potential victim	24,279.71	26,378.00	35,713.95	35,717.65

Panel C: Different Age Groups in Treated Sample

	Age<26, Treated	Age[26,30], Treated	Age[31,35], Treated	Age>35, Treated
N	607,076	57,838	42,900	52,135
No. of Fraud	201	104	48	32
No. of Use	17	3	11	4
Prob. of Fraud	0.0331%	0.1798%	0.1119%	0.0614%
Prob. of Use conditional on Fraud	8.46%	2.88%	22.92%	12.50%
Average Loss per capita	16,029.41	45,666.67	12,636.36	67,500.00
Average Loss per potential victim	1,355.72	1,317.31	2,895.83	8,437.50

Notes: This table shows the cyber-telecom fraudulently-induced borrowing in different gender and age sub-samples for both control and treated groups. The Platform labels a loan usage request as fraud or not based on (a) applicants' feedback to the alert phone calls, and (b) post-borrowing feedback from borrowers. Fraud=1 if the applicant realizes the fraud and withdraws his or her loan application after receiving the alert message, or the applicant who was indeed swindled report the fraud case to the Platform afterwards. Use (credit use following a fraud-induced loan application) is defined as 1 if the cyber-telecom fraudulently-induced applicant takes up the loan successfully, and 0 otherwise. The probability of fraud-induced loan usage requests (Fraud) is the number of fraud-induced loan usage requests divided by the sample size, while the probability of successful credit use following a fraud-induced loan application (Use) is the number of Use incidences divided by the sample size. Average loss per capita is calculated as the total loss amount due to cyber-telecom fraud divided by the sample size, and average loss conditional on Fraud is total loss divided by the number of Fraud incidences.

Table 2: Case Characteristics of Fraud Sub-Samples

Panel A: Control, Fraud

	N	mean	p50	sd	min	max
Use	315	95.56%	1	0.21	0	1
Female	315	0.85	1	0.35	0	1
Age	315	27.81	26	5.81	20	50
Apply Amount	315	29,070.79	20,000	25,426.10	1,000	100,000
Loss conditional on Use	301	29,031.56	20,000	25,207.56	1,000	100,000

Panel B: Treated, Fraud & Unidentified

	N	mean	p50	sd	min	max
Use	39	53.85%	1	0.51	0	1
Female	39	0.67	1	0.48	0	1
Age	39	28.44	28	5.99	21	52
Apply Amount	39	13,069.23	6,700	16,244.48	500	75,000
Loss conditional on Use	21	14,666.67	10,000	17,736.38	500	75,000

Panel C: Treated, Fraud & Identified

	N	mean	p50	sd	min	max
Use	346	4%	0	0.20	0	1
Female	346	0.81	1	0.40	0	1
Age	346	26.98	25	5.25	20	50
Apply Amount	346	13,404.62	10,000	16,059.02	500	100,000
Loss conditional on Use	14	36,464.29	17,250	34,743.82	3000	100,000

Panel D: Treated, Fraud, Identified & Use

	N	mean	p50	sd	min	max
Use	14	100%	1	0	1	1
Female	14	0.93	1	0.27	0	1
Age	14	28.79	25.5	6.39	22	40
Apply Amount	14	33,607.14	17,250	33,392.29	3,000	100,000
Loss conditional on Use	14	36,464.29	17,250	34,743.82	3,000	100,000

Notes: This table presents the applicant characteristics of fraud sub-samples. Panel A shows the fraud applications in the control group. Panel B, C, D show the fraud applications in the treatment group, while Panel B shows the fraud applications missed by the Platform’s anti-fraud system, Panel C shows the fraud applications captured by the anti-fraud system, and Panel D shows the fraud applications captured by the anti-fraud system, but the applicant fails to see through the fraud, take up the loan successfully and transfer money to the fraudsters. Use is defined as 1 if the cyber-telecom fraudulently-induced applicant takes up the loan successfully, and 0 otherwise. Loss conditional on Use is set to missing for Use=0 applications.

Table 3: Who are more likely to become cyber-telecom fraudulently-induced borrowing victims?

	Logit Model		Probit Model	
	(1)	(2)	(3)	(4)
	Fraud	Fraud	Fraud	Fraud
Female	1.6358^{***}		0.5995^{***}	
	(0.1019)		(0.0353)	
Age (>35 ref.)				
18-25	1.5854^{***}		0.5780^{***}	
	(0.1515)		(0.0554)	
25-35	0.8335^{***}		0.2934^{***}	
	(0.1388)		(0.0494)	
Age&Gender Group (>35 Male ref.)				
18-25 Female		3.4907^{***}		1.1895^{***}
		(0.3320)		(0.1007)
25-35 Female		2.9093^{***}		0.9744^{***}
		(0.3242)		(0.0962)
>35 Female		2.0816^{***}		0.6656^{***}
		(0.3446)		(0.1046)
18-25 Male		2.2737^{***}		0.7203^{***}
		(0.3426)		(0.1040)
25-35 Female		0.7656^{**}		0.2266^{**}
		(0.3621)		(0.1075)
Income (0-4k ref.)				
4k-6k	0.4227^{***}	0.3366^{**}	0.1647^{***}	0.1312^{**}
	(0.1384)	(0.1402)	(0.0552)	(0.0560)
6k-8k	0.7088^{***}	0.6405^{***}	0.2610^{***}	0.2352^{***}
	(0.1578)	(0.1585)	(0.0625)	(0.0629)
8k-10k	0.7499^{***}	0.6780^{***}	0.2787^{***}	0.2541^{***}
	(0.2004)	(0.2011)	(0.0783)	(0.0787)
>10k	0.4778	0.4377	0.1619	0.1390
	(0.3598)	(0.3602)	(0.1339)	(0.1352)
Apply Amount (0-5k ref.)				
5k-10k	0.5227^{***}	0.5349^{***}	0.2081^{***}	0.2112^{***}
	(0.1174)	(0.1176)	(0.0437)	(0.0438)
>10k	1.2154^{***}	1.2294^{***}	0.4842^{***}	0.4882^{***}
	(0.0987)	(0.0991)	(0.0374)	(0.0376)
Total Loan in Previous 12 Month (>20k ref.)				
0	1.8891^{***}	1.8790^{***}	0.6406^{***}	0.6416^{***}
	(0.2513)	(0.2511)	(0.0799)	(0.0802)
<=20k	0.2505	0.2404	0.0851	0.0841
	(0.1756)	(0.1753)	(0.0583)	(0.0584)
Number of Loan Account in Previous 12 Month (>1 ref.)				

0	1.1660***	1.1649***	0.3775***	0.3795***
	(0.2379)	(0.2377)	(0.0765)	(0.0767)
1	0.3823	0.3728	0.1531*	0.1540*
	(0.2625)	(0.2624)	(0.0823)	(0.0826)
Historical Consumer Loan (>10k ref.)				
0	0.9271***	0.9271***	0.3562***	0.3573***
	(0.1392)	(0.1393)	(0.0493)	(0.0495)
<=10k	0.4059***	0.4036***	0.1497***	0.1502***
	(0.1542)	(0.1542)	(0.0537)	(0.0537)
Days after Last Credit Inquiry (>0 ref.)				
0	2.2499***	2.2469***	0.8165***	0.8168***
	(0.0978)	(0.0977)	(0.0329)	(0.0330)
No Previous Credit Inquiry	1.1600***	1.1575***	0.3636***	0.3646***
	(0.1896)	(0.1897)	(0.0710)	(0.0712)
Credit Card Usage (>20% ref.)				
<=20%	1.3426***	1.3353***	0.4768***	0.4775***
	(0.1200)	(0.1201)	(0.0421)	(0.0423)
Without Credit Card	1.1229***	1.1160***	0.3788***	0.3787***
	(0.1268)	(0.1269)	(0.0448)	(0.0449)
Constant	-12.9331***	-13.2197***	-5.2695***	-5.2990***
	(0.3316)	(0.4329)	(0.1187)	(0.1410)
pseudo R-sq	0.306	0.308	0.306	0.308
N	400758	400758	400758	400758

Notes: This table illustrates what type of persons are more likely to become cyber-telecom fraudulently-induced borrowing victims using the logit model and the probit model, respectively, at the loan usage request level. The dependent variable is Fraud, a dummy variable equals to 1 if the loan usage request is a case of cyber-telecom fraudulently-induced borrowing, according to (a) applicants' feedback to the alert phone calls, and (b) post-borrowing feedback from borrowers. Explanatory variables include age, gender, income, apply amount, total credit in the last 12 months (excluding mortgage loans), number of loan account in the last 12 months, historical consumer loan amount (settled and outstanding), days after last credit report inquiry and the credit card utilization rate. The last five variables are from external credit records. The baseline groups for age, income and apply amount are above 35, under 4000 RMB and under 5000 RMB, respectively. For the other five variables, the baseline groups are total credit in the last 12 months exceeding 20000 RMB, more than one loan account in the last 12 months, historical consumer loan amount exceeding 10000 RMB, at least one day after last credit report inquiry, and credit utilization rate over 20%.

Table 4: The Treatment Effects of the Intervention

		Treated	Control	Diff.	t-stat
(i)	Sample Size	213,584	187,179		
(ii)	No. of Fraud-induced applications (Fraud)	385	315		
(iii)	No. of Identified	13,298	0		
(iv)	No. of Correctly Identified	346	0		
(v)	No. of Use	35	301		
(vi)	Average Loss per capita	23,385.71	29,031.56	-5,645.85	1.2414
(vii)	Prob. of Fraud (ii)/(i)	0.18%	0.17%	0.01%	0.9053
(viii)	Model Accuracy（iv)/(iii）	**2.60%**	-	-	-
(ix)	Detection Rate (iv)/(ii)	**89.87%**	0	89.87%	52.7885
(x)	Prob. of Use Conditional on Fraud (v)/(ii)	9.09%	95.56%	-86.46%	44.7253
(xi)	Average Loss per potential victim (vi)*(v)/(ii)	2,125.97	27,741.27	-25,615.29	17.9860

Notes: This table presents the treatment effects of the anti-fraud system on the probability of successful credit use as well as customer loss following fraud-induced credit applications, showing differences between the two groups and the t-statistics. The Platform labels an application as fraud-induced or not based on (a) applicants' feedback to the alert phone calls, and (b) post-borrowing feedback from borrowers. Fraud=1 if the applicant realizes the fraud and withdraws his or her loan usage application after receiving the alert message, or the applicant who was indeed manipulated by fraudsters report the fraud case to the Platform afterwards. Identified is defined as 1 if the application gets a fraud score higher than the cut-off point from the anti-fraud system. Correctly identified is defined as 1 if Fraud=1 and Identified=1. Use is defined as 1 if the cyber-telecom fraudulently-induced applicant takes up the loan successfully, and 0 otherwise. The average loss per capita is calculated as total loss/number of Use=1 cases. The probability of fraud is the number of Fraud-induced loan usage requests divided by the sample size. Model accuracy is defined as the number of Fraud-induced loan usage requests correctly identified, divided by the number of all applications identified. The detection rate is the percentage of fraud-induced loan usage requests identified by the anti-fraud system, i.e. the number of correctly identified/number of all fraud-induced loan usage requests. Probability of Use conditional on Fraud is the number of Use/number of Fraud-induced loan usage requests. Average loss per potential victim is calculated as the total loss amount/number of Fraud.

Table 5: Probability of Fraud: Treated vs Control

	Logit Model		Probit Model	
	(1)	(2)	(3)	(4)
	Fraud	Fraud	Fraud	Fraud
Treatment	0.0412	0.1352	0.0135	0.0362
	(0.0778)	(0.0834)	(0.0256)	(0.0326)
Female	2.2383***	1.6371***	0.7001***	0.5996***
	(0.0992)	(0.1020)	(0.0295)	(0.0354)
Age (>35 ref.)				
18-25	1.5066***	1.5760***	0.4939***	0.5752***
	(0.1493)	(0.1511)	(0.0469)	(0.0554)
25-35	0.7238***	0.8370***	0.2236***	0.2938***
	(0.1374)	(0.1388)	(0.0422)	(0.0494)
Income (0-4k ref.)				
4k-6k	0.2907**	0.4306***	0.0927**	0.1660***
	(0.1359)	(0.1386)	(0.0465)	(0.0552)
6k-8k	0.3710**	0.6881***	0.1258**	0.2554***
	(0.1498)	(0.1583)	(0.0510)	(0.0627)
8k-10k	0.2551	0.7028***	0.0890	0.2663***
	(0.1901)	(0.2025)	(0.0630)	(0.0791)
>10k	-0.0664	0.4376	-0.0115	0.1506
	(0.3497)	(0.3607)	(0.1092)	(0.1343)
Apply Amount (0-5k ref.)				
5k-10k		0.5258***		0.2093***
		(0.1174)		(0.0438)
>10k		1.2287***		0.4883***
		(0.0991)		(0.0377)
Total Loan in Previous 12 Month (>20k ref.)				
0		1.8237***		0.6238***
		(0.2543)		(0.0813)
<=20k		0.2467		0.0841
		(0.1755)		(0.0583)
Number of Loan Account in Previous 12 Month (>1 ref.)				
0		1.0793***		0.3551***
		(0.2442)		(0.0792)
1		0.2897		0.1292
		(0.2688)		(0.0852)
Historical Consumer Loan (>10k ref.)				
0		0.9311***		0.3571***
		(0.1390)		(0.0493)
<=10k		0.4021***		0.1491***
		(0.1542)		(0.0537)
Days after Last Credit Inquiry (>0 ref.)				

0		2.2538***		0.8172***
		(0.0978)		(0.0329)
No Previous Credit Inquiry		1.1656***		0.3659***
		(0.1897)		(0.0710)
Credit Card Usage (>20% ref.)				
<=20%		1.3454***		0.4771***
		(0.1200)		(0.0421)
Without Credit Card		1.1180***		0.3767***
		(0.1268)		(0.0448)
Constant	-8.8924***	-12.9370***	-3.7132***	-5.2699***
	(0.2170)	(0.3317)	(0.0697)	(0.1188)
pseudo R-sq	0.086	0.306	0.086	0.307
N	400758	400758	400758	400758

Notes: This table compares the probability of fraud-induced loan applications for control and treatment groups using the logit model and the probit model respectively, at the loan usage request level. The dependent variable is Fraud, a dummy variable equals to 1 if the loan application is a case of cyber-telecom according to (a) applicants' feedback to the alert phone calls, and (b) post-borrowing feedback from borrowers. Treatment equals 1 for the treatment group and 0 for the control group. Control variables include age, gender, income, apply amount, total credit in the last 12 months (excluding mortgage loans), number of loan account in the last 12 months, historical consumer loan amount (settled and outstanding), days after last credit report inquiry and the credit card utilization rate. Apply amount ranges from 500-100,000 RMB. The other five variables are from external credit records The baseline groups for age, income and apply amount are above 35, under 4000 RMB and under 5000 RMB, respectively. For the other five variables, the baseline groups are total credit in the last 12 months exceeding 20000 RMB, more than one loan account in the last 12 months, historical consumer loan amount exceeding 10000 RMB, at least one day after last credit report inquiry, and credit utilization rate over 20%.

Table 6: Probability of Use & Loss: Treated vs Control

	Logit Model	Probit Model	OLS	
	(1)	(2)	(3)	(4)
	Fraud&Use	Fraud&Use	Loss	Loss in Fraud Subsample
Treatment	-2.2519***	-0.7392***	-67.7454***	-20534.2195***
	(0.1851)	(0.0572)	(4.5530)	(1503.4666)
Female	1.7000***	0.5889***	46.4968***	2349.4556
	(0.1569)	(0.0508)	(3.7936)	(1769.7576)
Age (>35 ref.)				
18-25	1.1173***	0.4139***	28.0312***	-1739.7427
	(0.2265)	(0.0801)	(5.9396)	(2645.8520)
25-35	0.6394***	0.2317***	12.3312***	-3511.8943
	(0.1925)	(0.0668)	(4.4744)	(2412.5695)
Income (0-4k ref.)				
4k-6k	-0.0199	-0.0086	7.9893	2221.5675
	(0.1845)	(0.0722)	(8.9074)	(2322.7280)
6k-8k	-0.1604	-0.0596	0.2506	3965.6339
	(0.2261)	(0.0859)	(9.6259)	(2602.2605)
8k-10k	-0.0132	0.0197	2.0386	7054.0262**
	(0.3048)	(0.1112)	(10.7915)	(3321.5702)
>10k	-0.1452	-0.0689	6.8006	29237.1216***
	(0.5060)	(0.1813)	(13.4785)	(6034.7430)
Apply Amount (0-5k ref.)				
5k-10k	0.6580***	0.2440***	2.5177	-1340.8638
	(0.2130)	(0.0706)	(4.5214)	(2006.8266)
>10k	1.9897***	0.7054***	78.6832***	12906.9618***
	(0.1632)	(0.0560)	(4.4387)	(1740.7156)
Total Loan in Previous 12 Month (>20k ref.)				
0	1.6636***	0.5736***	71.8578***	-7316.1111*
	(0.2930)	(0.0914)	(7.4399)	(3912.8004)
<=20k	-0.1254	-0.0210	2.7296	-2748.1109
	(0.2562)	(0.0811)	(4.7243)	(2990.0214)
Number of Loan Account in Previous 12 Month (>1 ref.)				
0	1.3678***	0.4621***	38.4626***	-5641.1233
	(0.2807)	(0.0885)	(6.4259)	(4291.9842)
1	0.8418**	0.3183***	51.1999***	-5243.9883
	(0.3274)	(0.0994)	(5.6857)	(4846.7489)
Historical Consumer Loan (>10k ref.)				
0	1.1246***	0.3883***	60.2081***	365.1158
	(0.2097)	(0.0690)	(6.6423)	(2387.5527)
<=10k	0.8912***	0.2958***	12.3341**	190.7980
	(0.2291)	(0.0750)	(5.4280)	(2618.6180)

Days after Last Credit Inquiry (>0 ref.)				
0	1.6925***	0.6020***	77.7822***	-2568.7877
	(0.1317)	(0.0446)	(5.2460)	(1699.0023)
No Previous Credit Inquiry	1.1118***	0.3554***	78.3702***	-2.9870
	(0.2353)	(0.0891)	(14.2573)	(3226.8287)
Credit Card Usage (>20% ref.)				
<=20%	1.1401***	0.3952***	44.4846***	815.5284
	(0.1599)	(0.0550)	(4.8520)	(2080.8229)
Without Credit Card	0.7529***	0.2500***	-2.1100	-958.2578
	(0.1768)	(0.0611)	(4.6032)	(2219.1958)
Constant	-12.1552***	-4.9121***	-64.7304***	24042.6425***
	(0.4233)	(0.1481)	(11.2289)	(5723.2069)
R-sq			0.004	0.450
pseudo R-sq	0.336	0.331		
N	400758	400758	400758	700

Notes: This table compares the probability of actual credit use following fraud-induced credit applications and customer loss for control and treatment groups. We use the logit model and the probit model, respectively, for the incidences of credit use, and OLS for customer loss, at the loan usage level. The outcome variables are Use and Loss. Use is a dummy variable defined as 1 if the cyber-telecom fraudulently-induced applicant takes up the loan successfully, and 0 otherwise. Loss is the loss amount caused by cyber-telecom fraud, which is defined as 0 for those Use=0 applicants. Treatment equals 1 for the treatment group and 0 for the control group. Control variables include age, gender, income, apply amount, total credit in the last 12 months (excluding mortgage loans), number of loan account in the last 12 months, historical consumer loan amount (settled and outstanding), days after last credit report inquiry and the credit card utilization rate. Apply amount ranges from 500-100,000 RMB. The other five variables are from external credit records. The baseline groups for age, income and apply amount are above 35, under 4000 RMB and under 5000 RMB, respectively. For the other five variables, the baseline groups are total credit in the last 12 months exceeding 20000 RMB, more than one loan account in the last 12 months, historical consumer loan amount exceeding 10000 RMB, at least one day after last credit report inquiry, and credit utilization rate over 20%.

Table 7: Probability of Fraud: Lack of Financial Literacy VS Overconfidence

	(1)	(2)	
	Fraud_FL	Fraud_OC	Coefficient Diff.
Treatment	1.6518***	1.8672***	0.2300
	(0.1672)	(0.3524)	(0.3900)
Age (>35 ref.)			
18-25	2.2651***	0.7317*	-1.4978***
	(0.3131)	(0.4147)	(0.5198)
25-35	1.2708***	0.5558	-0.7090
	(0.3104)	(0.3646)	(0.4789)
Income (0-4k ref.)			
4k-6k	0.8858***	0.9326	0.0707
	(0.2461)	(0.6458)	(0.6911)
6k-8k	1.5096***	1.4675**	-0.0082
	(0.2670)	(0.6743)	(0.7262)
8k-10k	1.6704***	1.2289	-0.3940
	(0.3330)	(0.7644)	(0.8355)
>10k	1.2982**	0.8328	-0.4310
	(0.6490)	(1.2160)	(1.3788)
Apply Amount (0-5k ref.)			
5k-10k	0.3594**	0.5840	0.2334
	(0.1679)	(0.3936)	(0.4278)
>10k	0.0809	1.3611***	1.2645***
	(0.1786)	(0.3349)	(0.3797)
Days after Last Credit Inquiry (>0 ref.)			
0	3.5943***	2.0698***	-1.5039***
	(0.2484)	(0.2960)	(0.3861)
No Previous Credit Inquiry	1.4302***	-0.5105	-1.9401*
	(0.5108)	(1.0366)	(1.1556)
Total Loan in Previous 12 Month (>20k ref.)			
0	1.0850	4.9728	3.8967
	(0.7252)	(5.8619)	(5.8864)
<=20k	0.5628*	0.6667	0.1035
	(0.3007)	(0.7304)	(0.7897)
Number of Loan Account in Previous 12 Month (>1 ref.)			
0	1.5337**	-1.3542	2.8853
	(0.7599)	(5.8950)	(5.9237)
1	0.4274	-2.6704	3.0985
	(0.7451)	(5.8536)	(5.8806)
Credit Card Usage (>20% ref.)			
<=20%	1.8622***	1.7021***	-0.1471
	(0.2426)	(0.4287)	(0.4925)
Without Credit Card	1.7737***	1.9154***	0.1572

	(0.2471)	(0.4450)	(0.5089)
Constant	-14.0791***	-17.5055***	-3.4970
	(0.8871)	(5.9406)	(5.9876)
pseudo R-sq	0.347	0.280	
N	213477	213477	

Notes: This table presents the characteristics of two types of potential victims, i.e. potential victims who lack financial literacy and potential victims who are overconfident. We use the treated sample in this table as the Platform did not keep records on fraud type for the control sample. Columns (1)-(2) both use the logit model. The outcome variable of Column (1), Fraud_FL, equals to one if it is a fraud case due to lacking financial literacy. Similarly, the outcome variable of Column (2), Fraud_OC, equals to one if it is a fraud case due to overconfidence. Explanatory variables include age, gender, income, apply amount, total credit in the last 12 months (excluding mortgage loans), days after last credit report inquiry, the credit card utilization rate, and the number of loan account in the last 12 months. Apply amount ranges from 500-100,000 RMB. The other five variables are from external credit records, which are missing for some of the applicants. The baseline groups for age, income and apply amount are above 35, under 4000 RMB and under 5000 RMB, respectively. For the other five variables, the baseline groups are total credit in the last 12 months exceeding 20000 RMB, at least one loan account in the last 12 months, historical consumer loan amount exceeding 10000 RMB, at least one day after last credit report inquiry, and credit utilization rate over 20%.