

**Researchers**

Jonathan Fu  
University of Zurich

Mrinal Mishra  
University of Zurich

**Timeline**

2021-2022

**Study Status**

Results

**Study Type**

Other

**Research Implemented by IPA**

Yes

**Combatting fraudulent and predatory fintech apps with  
machine learning**

Jonathan Fu<sup>1</sup> and Mrinal Mishra<sup>2</sup>

<sup>1</sup>*Department of Banking & Finance, University of Zurich and the Centre for Sustainability & Private Wealth*

<sup>2</sup>*Department of Banking & Finance, University of Zurich and the Swiss Finance Institute*

February 10, 2022

**Policy Brief**

**Combating fraudulent and predatory fintech apps with  
machine learning**

Jonathan Fu<sup>1</sup> and Meinal Mishra<sup>2</sup>

<sup>1</sup>*Department of Banking & Finance, University of Zurich and the Centre for Sustainability & Private Wealth*  
<sup>2</sup>*Department of Banking & Finance, University of Zurich and the Swiss Finance Institute*

February 10, 2022

**Working Paper**

# Combating Fraudulent Financial Technologies with Machine Learning

Over the past decade, predatory and fraudulent practices in digital finance and financial technology have increased. With the increasing share of the global population using mobile devices for financial services, there are ongoing concerns about problematic providers targeting users with limited digital financial service literacy to exploit vulnerable households and businesses. The scale of this problem has been heightened by the COVID-19 pandemic. This not only harms consumers but can lead to mistrust of digital finance and delay financial inclusion efforts.

Machine learning — a type of artificial intelligence (AI) that allows software applications to become more accurate at predicting outcomes without being explicitly programmed to do so — shows promise in mitigating fraudulent financial technologies by analyzing available data collected regularly on the app stores to create a system for flagging and reporting highly suspicious apps. To demonstrate this, researchers drew on available data on Google finance apps for 63 countries covering from 2020 to mid-2021 to document the prevalence of such

problematic apps and test the efficacy of such methods. Focusing on personal loan apps, they tested two approaches for labeling problematic apps in a training dataset as falling into several suspect and legitimate classes using: 1) manual classification and 2) classification based on market-specific guidance. They then set up models to predict the propensity of apps in a separate test dataset to be predatory or fraudulent, drawing on both static and real-time signals from the apps' metadata as well as those provided in the user review data. For both approaches, they benchmarked their models' general accuracy against actual app removals.

Overall, machine learning techniques demonstrated an ability to create a system for efficiently and accurately flagging and reporting apps with suspicious behaviors, particularly in separating between "likely legitimate" and "likely suspect" apps. However, model accuracy was somewhat lower when differentiating more granular categories –e.g., between "pure fraud" and "predatory" cases. Different machine learning model set-ups were found to have some influence on predictive accuracy. While these results indicate further fine-tuning is necessary, they also suggest that using an ensemble of approaches may be useful in successfully identifying suspect apps of interest. Altogether, results show that machine learning — even when requiring manual review to protect against false positives or fine tuning — can considerably reduce the burden of regulators manual verification of new finance apps. This can also speed up the rate at which suspicious apps can be flagged and removed from app stores.