

# Shortchanged: Uncovering and Analyzing Intimate Partner Financial Abuse in Consumer Complaints

Arkaprabha Bhattacharya<sup>1,2</sup>, Kevin Lee<sup>1</sup>, Vineeth Ravi<sup>1</sup>, Jessica Staddon<sup>1,3</sup>, Rosanna Bellini<sup>2</sup>

<sup>1</sup>J.P. Morgan AI Research, JPMorgan Chase, New York, New York, USA; <sup>2</sup>Cornell University, New York, New York, USA; <sup>3</sup>Northeastern University, Oakland, California, USA

## BACKGROUND

- **Intimate partner violence (IPV)** is a pattern of abusive behavior through physical, emotional, sexual, and financial means to achieve control or assert power over a partner
- **Intimate Partner Financial Abuse (IPFA)** involves controlling access to financial resources, significantly affecting the well-being of survivors.
- Digital financial products and services, such as banking applications, can be used by abusers to monitor and control the financial activities of survivors
- Attacks are often reported retroactively, requiring survivors to infer how the attacks occurred and the vulnerabilities involved.
- Survivors' marginalized status makes it difficult to reach them and necessitates careful attention in research

Abuse "He **financially abused** me and did not let me have access to see the debt on the credit cards he was accumulating..."

Abuse ? "My ex husband submitted an insurance claim under my policy for an accident he had in a rental..."

## RESEARCH QUESTIONS

1. How might computational text analysis help to identify financial abuse between intimate partners in online consumer complaints?
2. Which digital consumer-facing financial products and technology-enabled financial attacks are prominently represented in such complaints?
3. What barriers to service do consumers report encountering when attempting to resolve concerns around technology-enabled financial abuse?

## CONTRIBUTIONS

1. Constructed the first dataset of positive IPFA-indicative complaints
2. Identified key financial products and attacks reported by survivors
3. Uncovered barriers to service faced by survivors during resolution of complaint

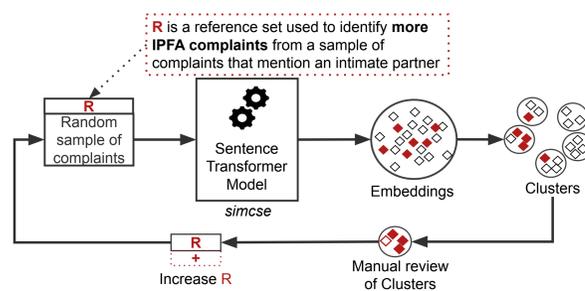
## METHOD

We developed a workflow for collecting consumer-authored complaints on technology-enabled intimate partner financial abuse

We collected complaints for our study from the CFPB, a government organization that collects, monitors, and resolves consumer complaints



After creating an initial reference set  $R$  of known IPFA complaints, which were vetted by five experts in IPV research, we developed a workflow combining pre-trained language models, similarity clustering, and human review to identify instances of financial abuse in consumer complaints



As research experts in financial abuse, we then performed an in-depth qualitative analysis of the 513 complaints in  $R$

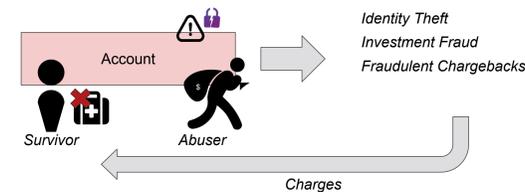


Deductive Coding for eight categories of interest  
Attack type, consequences, resolution ...

Critical Discourse Analysis  
What does "unable to access finances" mean ...

## SELECTED FINDINGS

Common attack: asset/account takeover for criminal activity



Common attack: abuser's negligence over digital asset/debt management



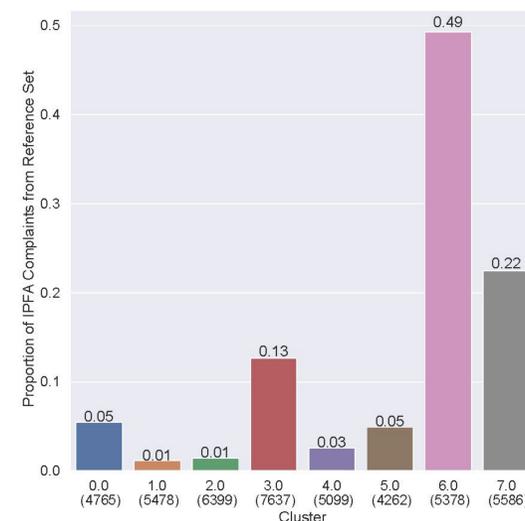
Evidence of policies that overlook the dynamic of IPFA

"... there was a fraudulent transaction of \$10,000.00 from my account ... This was an ex-partner who had stolen my phone and sent the money to themselves ... I contacted <company> to inform them but they then informed me that it was a non fraudulent transaction because said my ex-partner and I had previous legitimate transactions"

Evidence of survivor challenges with providing proof

"... My ex-wife has continued to obtain new credit in my name. I have disputed many accounts that appear on all 3 credit bureaus only to have them respond with "we need proof". ... nothing changes or helps ... I'm really just stuck ... This is insane."

Clustering aided us to better identify IPFA narratives



The distribution of ref across clusters; where Clusters -3, -6, and -7 would be selected for review.

## PRACTICAL TAKEAWAYS

- **Improved Security Tooling.** Enhance the safety of digital financial products through regular security audits and checkups
- **Evidence Gathering and Reporting.** Improve digital systems for evidence collection and reporting, making it easier for survivors to gather and present necessary information
- **Support Systems for Financial Services.** Strengthen support systems to better assist clients, particularly those vulnerable to financial abuse

## MORE IN THE PAPER

Our peer-reviewed study was presented at the 2024 ACM CHI Conference on Human Factors in Computing Systems



## ACKNOWLEDGEMENTS

We thank Fannie Liu and Francesca Mosca for their feedback on this work. We are also grateful to our associate chairs and reviewers, whose comments helped to improve the manuscript.

Rosanna Bellini's contributions are supported in part by NSF Award CNS-1916096 and a research award from JPMorgan Chase.

This presentation was prepared for informational purposes in part by the Artificial Intelligence Research group of JPMorgan Chase & Co. and its affiliates ("JP Morgan"), and is not a product of the Research Department of JP Morgan. JP Morgan makes no representation and warranty whatsoever and disclaims all liability, for the completeness, accuracy or reliability of the information contained herein. This document is not intended as investment research or investment advice, or a recommendation, offer or solicitation for the purchase or sale of any security, financial instrument, financial product or service, or to be used in any way for evaluating the merits of participating in any transaction, and shall not constitute a solicitation under any jurisdiction or to any person, if such solicitation under such jurisdiction or to such person would be unlawful. This document is intended to raise awareness about modelling techniques. This document is not intended to provide policy recommendations regarding any substantive issue or to convey JP Morgan's position on, or policies regarding, consumer complaint tracking or review.