The Digital Economy and Consumer Fraud *

Kenny Phua Chishen Wei Gloria Yang Yu

Abstract

We investigate whether the transition to the digital economy has unintended social consequences. We exploit bank branch closures, driven by the shift to digital banking, as shocks that push consumers to increase digital activity and exposure to consumer fraud. Following branch closures, consumers shop less in physical stores, increase online spending, and spend more time on finance and retail mobile apps. Using two quasi-natural experiments, we find that branch closures increase identity theft in the local area, especially among vulnerable communities such as military veterans. Adversaries actively target areas with more branch closures, exposing potential victims to more unwanted calls and phishing attacks. An analysis of local crime patterns suggests that our mechanism arises from a shift towards non-cash, digital transactions. Overall, bank branches can remain a vital social good in the digital age, providing security and consumer protection.

*Yu (corresponding author): gloriayu@smu.edu.sg, Singapore Management University. Phua: kenny.phua@uts.edu.au, University of Technology Sydney and Digital Finance Cooperative Research Center. Wei: chishen.wei@polyu.edu.hk, Hong Kong Polytechnic University. We are grateful for comments from William Cong, Marcin Kacperczyk, and Robert Marquez and seminar participants at the Hong Kong Polytechnic University and the University of Technology Sydney.

1 Introduction

The digital economy is reshaping economic activities, consumer behavior, and business practices, with data playing a central role in this transformation. As transactions and services move online, firms increasingly rely on vast amounts of consumer data to enhance efficiency, lower costs, and improve personalization. However, there are also significant tradeoffs. Tirole (2021) examines how the data-driven economy can create negative externalities in reduction of pro-social behavior. Our study explores whether the transition to the digital economy has unintended social consequences in the form of consumer fraud. Consumer fraud is an emerging risk alongside the rise of the digital economy. The U.S. Federal Trade Commission (FTC) reports that consumer losses to fraud in 2023 alone exceeded U.S. $10.3 billion. Despite these staggering losses, there is limited evidence on how the digital economy may contribute to this growing socioeconomic problem.

We formulate and test the hypothesis that the risk of consumer fraud rises as consumers increase their digital activity. Digitalization creates data privacy issues, and data collection fundamentally generates externalities. Consumer concerns include data harvesting, behavioral manipulation, and personal safety (Armantier, Doerr, Frost, Fuster, and Shue, 2024). Users may bear privacy costs from interactions with digital businesses that over-collect data and under-invest in information security (Fainmesser, Galeotti, and Momot, 2023; Ramadorai, Uettwiller, and Walther, 2025). Data leakage from data breaches and privacy scandals (Cong, Xie, and Zhang, 2021) may result in unauthorized third parties acquiring unsecured data for economic gain.

Our identification strategy exploits branch closures, driven by the shift to digital banking, as shocks that push bank consumers to engage more with the digital economy. Banks facilitate many economic activities that involve payments and transfers, so they are uniquely positioned to influence consumer behavior. Over time, as consumers demand more digital financial products, banks increase investments in digital offerings, leading to a richer service ecosystem. The complementarity between consumer adoption and digital service investments naturally leads to branch closures in equilibrium. Many consumers can seamlessly transition to digital banking, but those who lack digital literacy may be forced to do so at great risk of falling prey to consumer fraud.

The closure of bank branches can increase the risk of consumer fraud through

several channels. First, greater engagement with the digital economy involves the transfer of personal identifying data. Digital banking in itself is unlikely to cause consumer fraud, but in processing other types of digital transactions, data can leak and become vulnerable to exploitation by adversaries. Second, stolen personal identifying data can be leveraged to refine fraud techniques. Adversaries increasingly exploit compromised data to further target victims using tactics such as emails, texts, phone calls, and even SIM card swaps. Third, branch closures eliminate a crucial alternative for consumers who prefer in-person services. Bank branches serve as a frontline defense against fraud, enabling face-to-face authentication and providing additional security checks. For example, bank personnel can verify identity, flag suspicious activity, and provide personalized security advice.

Among the various types of consumer fraud, we focus on identity theft because it has serious and long-lasting consequences. Victims may suffer severe emotional distress (Harrell and Langton, 2013) and face significant financial repercussions including reduced credit access and greater bankruptcy risk (Hamdi, Kalda, and Sovich, 2024). In a recent data privacy survey conducted by the Federal Reserve Bank of New York (FRBNY), identity theft was overwhelmingly (92%) the most common concern (Armantier et al., 2024). In response to these harms, the U.S. government has enacted laws to fight identity theft. Under 18 U.S.C. §1028(a)(7), identity theft is any crime that misuses personal information for financial gain, including credit card fraud, fraudulent loan applications, and unauthorized access to bank accounts.[1] Insurance companies now offer policies to insure against related losses. Identity thieves often exploit the feature that digital transactions do not require face-to-face verification, utilizing stolen credentials such as passwords, Social Security numbers, and/or private account details. Identity theft has become an omnipresent threat in the digital economy, resulting from digital activities and exposure to weak data privacy protection (Bian, Pagel, Raval, and Tang, 2024).

We start our analysis by showing how consumer behavior changes after local branch closures. First, we estimate the elasticity of substitution to neighboring bank branches after a focal branch closes. Using granular footfall data, our estimates imply that only 18% of foot traffic redirects to nearby branches—82% of

[1]The U.S. Congress passed the Identity Theft and Assumption Deterrence Act in 1998 to criminalize identity theft. In 2024, the U.S. House of Representatives passed another act to provide additional assistance to victims of identity theft.

footfall disappears entirely. Our finding is consistent with evidence that physical banking is hyperlocalized, as minor inconveniences cause customers to adopt online payments and transactions (Choi and Loh, 2024). Second, we find that residents exposed to branch closures visit physical stores less and increase online transactions relative to in-store purchases. This finding is the first evidence that branch closures lead businesses and consumers to shift toward e-commerce.

Using MSA-year level data from the FTC Consumer Sentinel Network database, we test whether branch closures lead to more identity theft in the local area. A key threat to identification is that banks close branches due to local factors that are also correlated with rising consumer fraud. To address this concern, we use staggered exposures to postmerger consolidation between large regional/national banks as an instrument for branch closures (Nguyen, 2019). Mergers are not random and driven by the underlying economics of the banking business. However, an MSA with *both* acquirer and target branches is more likely to experience postmerger branch closures due to duplication in branch service for the consolidated bank.

The key identifying assumption is that MSA-level exposures to mergers between large banks are as good as randomly assigned with respect to local factors. We focus on mergers where both acquirer and target banks have at least U.S. $1 billion in premerger assets because these mergers are typically driven by broader strategic and synergistic objectives. Further tests suggest that these bank mergers are unlikely to be motivated by local factors because (i) the acquirers and targets are large and geographically diversified, and (ii) exposed MSAs account for only a small share of their overall deposits. Finally, there are no statistically significant pretrends in net branch closures between exposed and unexposed MSAs.

Our results from the Callaway and Sant'Anna (2021) difference-in-differences estimator indicate that branch closures lead to more identity theft. On average, MSAs exposed to large bank mergers have 2.79 more branch closures and 455.56 more reports of identity theft. Thus, the Wald estimate implies that each branch closure leads to an increase of +163.28 (= 455.56/2.79) identity theft reports. This estimate implies that the social costs are economically meaningful—a one standard deviation shock to branch closures corresponds to an increase of 2,318 identity theft cases, representing 1.6 times of its unconditional sample mean.

We perform two diagnostics on the results from our IV design. First, we eval-

uate the external validity of our local average treatment effect (LATE) using the Marbach and Hangartner (2020) complier framework. Complier MSAs are those that (do not) encounter branch closures due to the presence (absence) of merger exposures.[2] Because the LATE is an estimate of the treatment effect for only complier MSAs, it is uncertain whether we can generalize beyond complier MSAs. Reassuringly, we find that complier MSAs resemble the average MSA along most measurable dimensions, suggesting that our LATE has external validity. Next, we benchmark our IV estimate against the ordinary least squares (OLS) equivalent estimate. We find a close but larger (+213.42) OLS point estimate, which we speculate arises from uncorrected endogeneity (e.g., local economic conditions) that may drive both branch closures and identity theft.

Identity theft typically occurs online, so it is crucial for us to verify that branch closures affect consumer fraud through digital channels. We design two tests to do so. First, we expect consumers with limited digital capabilities to be more vulnerable to the adverse effects of forced digitalization. To shed light on this mechanism, we augment our difference-in-differences design to tease out heterogeneous effects of branch closures. We find that branch closures lead to more identity theft cases when (i) consumers are more reliant on bank branches, (ii) banks are less digitally focused to start with, and (iii) the local area has lower internet penetration rates. These patterns support the idea that branch closures may disproportionately impose social costs on some consumers who are ill-equipped or unable to safely engage with the digital economy. Second, our forced digitalization hypothesis predicts that consumers will increase their digital activity after branch closures. Exploiting novel microdata, we show that individual consumers exposed to branch closures spend significantly more time on mobile apps.

Next, we direct our attention to a vulnerable community—U.S. military veterans. Identity theft is a serious issue for U.S. military veterans. According to the FTC, veterans reported a record 45,882 bank-related identity theft cases in 2022, marking a 28.8% surge over three years. Compared to civilian Americans, veterans are more likely to fall prey to identity theft, and when victimized, suffer greater financial losses. To generate plausibly exogenous variation in veteran populations, we construct MSA-level exposures to veterans by exploiting the Vietnam

[2]Ultimately, the merged bank must select which branches to close. We emphasize that this layer of selection does not invalidate our identification strategy, which only requires that MSA exposures to bank mergers are as good as randomly assigned. However, it could affect the interpretation of our LATE.

War draft lotteries (Angrist and Chen, 2011). Overall, we find causal evidence that the effect of branch closures on identity theft is significantly stronger in areas with more military veterans.

We conjecture that the increase in identity theft after branch closures is due in part to more aggressive targeting of victims. In many identity theft schemes, phone calls are the first point of contact between the adversary and the consumer. Adversaries tend to impersonate trusted institutions like banks or government agencies on these calls to extract personal identifying information such as Social Security numbers and bank account details. To compound the problem, advances in telecommunications technology have enabled the rise of "robocalls", which are automated calls that can systematically reach large numbers of consumers. Using the FTC Do-Not-Call (DNC) Reported Calls database, we estimate that a one standard deviation increase in branch closures leads to a 6.75% increase over the unconditional probability of unwanted calls. These calls elevate the risk of identity theft and impose further social costs by wasting time, causing disruption, and hindering the provision of legitimate services.

The other adversarial tactic that we consider is phishing attacks. According to the FTC, a significant portion of identity theft cases stem from phishing attacks, where adversaries deceive consumers into providing personal information through deceptive emails or websites (FTC, 2024a). Phishing attacks trick individuals into sharing their personal information by using misleading emails or fraudulent websites. To identify phishing attacks, we exploit the idea that adversaries often clone the official brand website and use it as a template for malicious use. Using the search engine `Shodan`, we search for the historical volume of suspicious websites that share features of their legitimate counterparts but lack digital security certificates. Using a two-stage estimation approach, we find that branch closures in an MSA could increase the exposure of its residents to identity theft through phishing attacks.

Finally, we examine a testable implication on *physical* crime that arises from the shift to digital activity. If branch closures increasingly push consumers to adopt digital, noncash transactions, this shift should reduce the financial payoffs to crimes that involve physical cash. Consistent with this view, our Sobel-Goodman decomposition analysis reveals that identity theft has a negative mediating effect between branch closures and cash-related crimes (i.e., burglary, robbery, larceny), but not for cash-unrelated crimes. This finding extends the analysis

in Garmaise and Moskowitz (2006), which is perhaps the first study on the social externalities of bank activities. They find that a reduction in bank competition increased local property crime. Their sample ends in 1999, and the economic factors that drive crime may have changed considerably over the last two decades. Overall, our result suggests that branch closures drive identity theft through a shift away from cash usage and toward digital transactions.

A limitation of our study is that we do not evaluate the *overall* welfare effects of digitalization. Although identity theft is an unintended social cost of digitalization, we have not considered the nondigital counterfactual. Cash transactions create security and logistic costs, and the maintenance of bank branches requires significant resources. A welfare analysis that balances the costs of physical operations against the convenience, cost savings, and efficiency brought about by the digital economy is beyond the scope of our study. Based on our findings, the main takeaway message is that bank branches can serve as a vital social good in the digital age, offering security and consumer protection.

Our study connects to the literature on the value of data (Veldkamp, 2023; Veldkamp and Chung, 2024) and the economics of data privacy (Acquisti, Taylor, and Wagman, 2016; Tirole, 2023). Users bear privacy costs from digital businesses that over-collect data and under-invest in consumer data protection (Fainmesser, Galeotti, and Momot, 2023; Ramadorai, Uettwiller, and Walther, 2025). As demand for digital services rises, digital privacy concerns also increase (Chen, Huang, Ouyang, and Xiong, 2025). The data economy can create social externalities such as reductions in pro-social behaviors (Tirole, 2021), exposure to behavioral manipulation (Liu, Sockin, and Xiong, 2023; Acemoglu, Makhdoumi, Malekian, and Ozdaglar, 2025), and inadequate compensation for data loss and privacy violation (Cong, Xie, and Zhang, 2021). In an analysis of Apple's App Tracking Policy, Bian et al. (2024) find that restricting personal data collection curbs consumer fraud. Using branch closures as shocks to consumer behavior, our results complement the growing evidence on digital privacy risks by showing that increasing digital activities expose users to greater risks of identity theft.

Our paper also presents a social goods perspective on the value of bank branches. Traditionally, depository and lending activities occur through brick-and-mortar branches, such that proximity to branches improves income, employment, entrepreneur-

ship, financial inclusion, and health outcomes.[3] Branches remain important for banks to maintain market power, funding stability, and information sharing (Drechsler, Savov, and Schnabl, 2017; Benmelech, Yang, and Zator, 2023; Qi, De Haas, Ongena, Straetmans, and Vadasz, 2024). Our findings suggest that bank branches provide value as a social good by mitigating the rising risk of consumer fraud. This result relates to Garmaise and Moskowitz (2006), who study an earlier sample before widespread digitalization and find that branch closures are accompanied by increased property crime. Our evidence aligns with their finding that branch closures impose social costs.

Finally, we add to the growing evidence that digitalization and technological disruption differentially affect bank consumers. Jiang, Yu, and Zhang (2023) show that more elderly consumers become unbanked after digital disruption. Koont (2024) finds that the surplus from the digital banking revolution is mostly captured by the wealthier consumers. Fuster, Goldsmith-Pinkham, Ramadorai, and Walther (2022) show that digital financial technologies may have different effects on racial minorities. We document a social externality of digital transformation in the form of greater risk of identity theft. Our results show that an increase in digital activity due to bank branch closures disproportionately harms communities with lower internet penetration rates and U.S. military veterans.

2 How do branch closures affect identity theft?

Identity theft is an illegal activity involving the illicit acquisition of an individual's personal information, typically for financial gain. The Identity Theft and Assumption Deterrence Act of 1998 established identity theft as a distinct federal crime. Under 18 U.S.C. §1028(a)(7), identity theft is defined as any act of

> "knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

[3] See, for example, Jayaratne and Strahan (1996), Célerier and Matray (2019), Nguyen (2019), Martín-Oliver, Toldrà-Simats, and Vicente (2020), Bonfim, Nogueira, and Ongena (2020), Ji, Teng, and Townsend (2023), Amberg and Becker (2024), Sakong and Zentefis (2024), Cramer (2024), and Fonseca and Matray (2024).

According to the 2023 statistics from the FTC, the top three categories of identity theft account for more than half of all cases. 33% of reported cases are credit card fraud, which includes unauthorized transactions and fraudulent account openings. 13% of report cases are loan or lease in which adversaries use stolen identities to secure mortgages, auto loans, or personal loans. Bank account fraud, representing 11% of identity theft cases, involves unauthorized access to or creation of checking, savings, or investment accounts. The remaining cases comprise of government benefits fraud (8%), employment/tax-related fraud (7%), phone/utility scams (7%), and others (21%).

The FTC also breaks down the counts of identity theft reports by age groups.[4] Although older individuals are typically viewed as more vulnerable to fraud, identity theft also significantly affects the younger population. Consumers aged between 30 and 49 made 470,663 reports, accounting for 51% of all cases. Beyond these prime years of workforce participation, identity theft cases tend to steadily decline from age 50 onwards. We tabulate the breakdowns of identity theft reports by types and age groups in the Appendix.

Adversaries engage in identity theft by acquiring a victim's personal data, usually by employing a combination of both online and offline strategies. Impersonation is a common tactic, whereby the offender assumes the identity of bank personnel or government agency representative to deceives victims into divulging confidential information such as passwords or financial data. Social media mining is also used to gather publicly shared details and build comprehensive profiles to impersonate individuals. Cyberattacks exploit security vulnerabilities in online platforms to steal vast amounts of personal data, including Social Security numbers, banking details, and login credentials. Public Wi-Fi also poses a risk, as attackers can intercept personal data from phones and laptops connected to unsecured networks. Thieves may sift through discarded bank statements or tax documents to retrieve sensitive financial details. They may also install "skimmer" devices at ATMs, cash registers, and fuel pumps to extract card information.

We argue that identity theft emerges as an indirect consequence of digital banking. Digital banking offers valuable benefits and convenience, allowing consumers to conduct online purchases, manage investment portfolios, and access a variety of e-commerce platforms. Digital payments allow for financial inclusion

[4]The FTC received 1,036,903 reports of identity theft, of which 917,315 includes consumer age information.

for the previously un(der)banked. Moreover, banks invest heavily in security infrastructure, making their systems among the most secure in the world.

However, as financial transactions and economic activities change online, personal identifying data is transmitted in the process. Although electronic authentication methods are advancing, adversaries continue to bypass these defenses by employing tactics mentioned previously, such as phishing, malware infiltration, and social engineering. Adversaries continually improve their techniques and often the implementation of security countermeasures. This gap creates periods of vulnerability that allow identity thieves to impersonate authorities, intercept personal data, or gain unauthorized access to bank accounts.

In-branch banking can be less convenient and slower, but provides several guardrails to prevent identity theft. First, in-branch banking involves face-to-face interactions with bank staff. Bank employees can ask for additional forms of identification or conduct on-the-spot verification that automated systems may not perform. Second, physical bank branches are equipped with robust security measures such as surveillance cameras, secure storage areas for sensitive documents, and controlled access points, all of which serve as deterrents to potential identity thieves. Third, the human element of traditional banking often heightens customer awareness. Customers who engage directly with bank staff are more likely to receive security advice and remain vigilant to potential threats. Overall, bank branches could shield the most vulnerable segments from the risks of identity theft.

We are not suggesting that digital banking is insecure. Rather, the digital economy reduces physical touchpoints across a wide range of economic activities from secure cash transactions to in-person financial guidance. With over 13,000 bank branches closures since 2008, many consumers, particularly those who are less savvy with technology, have been pushed to engage with the digital economy. For those struggling to safely navigate digital platforms, this push can strip away the safeguards that in-branch or physical interactions once provided, exposing greater risk of identity theft.

3 Data and descriptive statistics

This section discusses the primary datasets used in our main empirical analysis. We obtain our key dependent variable, the number of identity theft reports (*ID theft reports*), from the Consumer Sentinel Network (CSN) maintained by the Federal Trade Commission (FTC). The CSN database is a collection of reports, covering types of consumer fraud including identity theft. It categorizes identity theft into seven major types related to credit cards, loans or leases, bank accounts, government documents or benefits, employment or tax, phone or utilities, and others. As an illustration, the Appendix provides a detailed breakdown of CSN identity theft report counts by types and subtypes for the year 2023.

The CSN is a comprehensive data source to analyze identity theft in the United States. It compiles data from consumer complaints submitted directly to the FTC and complaints shared by a wide range of data contributors. These contributors include law enforcement agencies (e.g., F.B.I. and U.S. Postal Inspection Service), state attorneys general and consumer protection offices (e.g., New York State Attorney General and Ohio Attorney General), federal government agencies (e.g., U.S. Department of Justice and U.S. Social Security Administration), consumer advocacy organizations (e.g., AARP Fraud Watch Network and National Consumers League), financial institutions (e.g., Mastercard International and JPMorgan Chase), and technology and telecommunications companies (e.g., Apple and Verizon Wireless). The Appendix contains a full list of these data contributors. Our sample covers 2009 to 2022, providing a rich panel with variation at the Metropolitan Statistical Area (MSA) and year level.

To measure bank branch closures, we use data from the Federal Deposit Insurance Corporation's (FDIC) Summary of Deposits (SOD) files. The SOD dataset provides annual branch-level data for all U.S. depository institutions. We compute *net branch closures* at the MSA-year level by subtracting the current year's branch count from the previous year's. A positive value indicates net branch closures, while a negative value indicates net additions of branches. The average MSA in our sample experiences 2.9 net branch closures per year with a standard deviation of 14.2, pointing to significant heterogeneity in branch activity across regions.

We employ a suite of demographic control variables to account for potential confounders that may influence both bank branch activity and identity theft rates.

These controls, sourced from the U.S. Census Bureau's American Community Survey (ACS), include population size, percentage aged 60+, unemployment rate, median household income, gender and racial makeup, and educational attainment (over high school). These controls capture essential socioeconomic traits at the MSA-year level, crucial for mitigating omitted variable bias in our estimates. For example, areas with more elderly or higher unemployment may be more prone to identity theft, possibly affecting the link between branch closures and fraud rates.

- Figure 1 here -

Figure 1 shows consumer fraud reports from 2009 to 2022, highlighting identity theft in blue. Identity theft made up a significant and varying part of total fraud. In 2009, it was 20.9% of 1.33 million reports, but this share dropped to 12.8% of 2.58 million reports in 2014. A striking pattern emerges in recent years. By 2020, the overall number of fraud reports exceeded 4.77 million, while identity theft reports also surged, making up nearly 30% of all incidents. The rise in identity theft coincides with economic shifts like increased digital banking and more online transactions, especially during the COVID-19 pandemic.

In terms of financial losses, Figure 1 reveals a steady upward trend in consumer fraud over the period. In 2009, total losses were around $1.38 billion, with relatively minor fluctuations in the following years. However, a significant spike occurs in the later years, with losses reaching $6.47 billion in 2022. This sharp rise suggests that, alongside the increase in fraud reports, the financial impact of each incident has escalated. This escalation may be driven by more sophisticated fraud schemes and the increasing stakes of digital fraud, particularly identity theft.

- Figure 2 here -

In Figure 2, blue circles depict the number of identity theft reports across MSAs in 2022. Larger circles indicate a higher number of reports. MSAs that are hit hard by identity theft are typically found in urban and coastal areas like New York City and Los Angeles. These affected regions usually have higher population densities, better access to digital services, and rely heavily on online transactions. They also tend to have higher income levels, making them attractive to adversaries. Given the substantial variation across regions, it is crucial to control for these demographic traits in our analysis to capture the relation between bank branch closures and identity theft.

- Table 1 here -

Table 1 summarizes the variables and pairwise correlations. Panel A shows that MSAs average 1,420 identity theft reports annually with a standard deviation of 5,320. The 90^{th} percentile of MSAs reports 2,470 reports, highlighting concentration in specific areas. MSAs experience an average of 2.9 net branch closures per year with a substantial standard deviation of 14.2. Decomposing this statistic, the average MSA has 3.9 branch closures and 1.0 branch opening. The average MSA has 18.4% of its population over 60, 50.1% male, 6.6% unemployed, 76.6% White, and 63.4% with at least a high school education. Average household income is \$56,100 with significant dispersion (σ = \$13,000). MSA population size varies widely, averaging 730,000 with a large standard deviation of 1,580,000.

Panel B of Table 1 shows that identity theft correlates positively with net branch closures (57%) and strongly with population size (76%), indicating a link between urbanization and identity theft. A 28% correlation with household income suggests higher-income areas may be more prone to fraud. In contrast, identity theft shows a negative association with both the percentage of white residents and individuals who finished high school, indicating possible distributional effects.

4 Branch closures and consumer behavior

Our evidence suggests that branch closures lead to more identity theft in the local area. In this section, we validate the underlying premise driving this increase—branch closures push both businesses and consumers to adopt digital noncash transactions. This adoption increases the risk of identity theft because their financial and personal identifying data are more frequently shared in transactions. We examine this premise from several angles, starting with the question of whether affected consumers substitute closed branches with nearby branches.

A central assumption underlying our hypothesis is that branch closures drive consumers online because there are no perceived close substitutes to the closed branches. Thus, we begin our analysis by investigating whether and how consumers affected by branch closures substitute visits to nearby branches.

Next, we examine the effects of branch closures on local businesses and consumers. For local businesses, branch closures increase the cost of handling cash transactions, often forcing them to adopt digital payments as a feasible and secure

alternative.[5] At the same time, consumers who rely on branches for in-person transactions must find alternative payment methods, often turning to internet-enabled banking and digital payments. Because digital payments operate as a two-sided market, this shift reinforces itself: As more consumers adopt digital transactions, merchants face stronger incentives to expand their digital payment infrastructure.

Therefore, branch closures not only push consumers toward online banking but also encourage broader engagement with e-commerce. Once consumers set up digital payment tools, they may increasingly favor the convenience of online shopping over in-person purchases. This creates a self-reinforcing cycle, where the increasing use of online banking and digital payments leads businesses to enhance their digital platforms, further improving accessibility and appeal. Over time, this shift can contribute to a decline in foot traffic for local physical stores, further entrenching the preference for online transactions. Retailers such as Nike and restaurants such as Domino's Pizza have strategically expanded their online presence in response to these trends. Findings from the Diary of Consumer Payment Choice survey administered by the U.S. Federal Reserve support this view: between 2016 and 2023, the proportion of online and remote purchases made by consumers more than doubled (Cubides and O'Brien, 2023).

In subsequent sections, we provide empirical evidence on how branch closures influence (i) consumer footfall at physical stores and (ii) online spending. Collectively, these analyses demonstrate that branch closures reshape economic activity, shifting consumers towards the digital economy. Although this change offers convenience, the delivery of digital services often requires consumers to share their personal identifying information, exposing them to a greater risk of identity theft.

4.1 Do affected consumers switch to nearby branches?

A central assumption underlying our hypothesis is that consumers are driven online because there are no perceived close substitutes to the closed branches.

[5]Banks serve an important function for local businesses as a place to store cash takings overnight. When bank branches close, local businesses face a dilemma. They could store cash in-store, but debt covenants and insurance contracts often forbid such behavior. Alternatively, businesses could arrange for their cash takings to be deposited at another bank branch. However, cash transportation requires time and effort and introduces additional security risks. These challenges make cash acceptance increasingly costly, particularly for small businesses with limited resources.

In principle, consumers who are affected by branch closures could simply travel further to another branch, hence avoiding the need to engage more with the digital economy. On the other hand, if physical banking is hyper-localized with high switching costs (Choi and Loh, 2024), consumers may not readily switch to other nearby branches.

To estimate the elasticity of branch visits between the closed branch and other nearby branches, we first collect weekly branch-level footfall data from the `pass_by` database. We focus on savings banks by filtering for "stores" tagged with the NAICS code for savings institutions (522120). Next, using the Google Geocoding API, we map the street address, zipcode, city, and state of every `pass_by` branch to its latitude and longitude coordinates. This step is crucial because we need to precisely compute the distances between `pass_by` branches and closed branches.[6] Then, for every `pass_by` branch, we merge in the total *net branch closures* that occur (i) within the past 180 days and (ii) within a 1-mile distance band.

$$\begin{aligned} \textit{bank branch visits}_{i,t} = \alpha + \beta \cdot \sum_{i'} \sum_{d=t-180}^{t-1} \textit{net branch closures}_{i',d} + \mathbf{X}_{z,t}^{\top}\boldsymbol{\lambda} + \varepsilon_{z,t}, \\ \text{s.t.} \quad \omega \text{ mi} \leq \text{distance}(i,i') \leq (\omega+1) \text{ mi} \end{aligned} \tag{1}$$

Finally, for branch i in week t and for branch closures/openings i' within the $(\omega, \omega+1)$ mile distance band, we estimate equation (1). The vectors $\mathbf{X}_{i,t}$ and $\boldsymbol{\lambda}$ represent vectors of control variables at the zipcode-year level and their corresponding coefficients, respectively.

- Table 2 here -

Table 2 shows little evidence that consumers affected by branch closures switch to other nearby branches. Column 1 shows that a branch closure is associated with 14.77 ($t = 2.61$) more visits per week to another branch within 0–1 miles. To put this estimate into context, the average branch closure/opening is surrounded by 8.14 other branches within 1 mile, and the average bank branch gets 665.89 visits per week. Thus, only 18% ($= (14.77 \times 8.14)/665.89$) of the foot traffic from closed branches redirects to nearby branches within a distance band of 0–1 mile. Due to higher costs for switching to further branches, columns 2–4 show an even weaker (and statistically insignificant) foot traffic redirection from closed branches to more

[6] The FDIC Summary of Deposits dataset provide the latitude and longitude coordinates of closed branches.

distant locations. For example, the implied elasticity of branch visits drops sharply from 18% to 5.1% between the 0–1 mile and 1–2 mile distance bands.

Overall, our findings support the view that physical banking patterns are hyper-localized and inelastic. Consumers inconvenienced by branch closures largely fail to switch to other branches even if they are in close proximity. As we show in the upcoming sections, these consumers readily adopt digital banking methods, which in turn allow them to engage more with the digital economy and rely less on physical stores.

4.2 Physical store visits

To test the premise that branch closures lead to a shift away from local physical stores, we collect store-level footfall (i.e., number of visits) data from the `pass_by` database. Then, we define *all visits* as the aggregated number of store visits at the zipcode-week level. For every zipcode-week area, we track the *net branch closures* that occur (i) within the past 180 days and (ii) between one and five miles away from its centroid. We impose the one-mile criterion to exclude mechanical decreases in footfall for stores near bank branches. Specifically, as consumers often combine banking and shopping activities on a trip, they may visit stores less simply because a nearby bank branch has closed. These mechanical decreases are likely driven by consumer convenience, and it is unclear whether they reflect a shift towards digital transactions or merely a reduction in combined trips.

$$\begin{aligned} \textit{all visits}_{z,t} = \alpha + \beta \cdot \sum_{z'} \sum_{d=t-180}^{t-1} \textit{net branch closures}_{z',d} + \mathbf{X}_{z,t}^{\top}\boldsymbol{\lambda} + \varepsilon_{z,t}, \\ \text{s.t.} \quad 1 \text{ mi} \leq \text{distance}(z, z') \leq 5 \text{ mi} \end{aligned} \tag{2}$$

For zipcode z in week t, we estimate equation (2). The vectors $\mathbf{X}_{i,t}$ and $\boldsymbol{\lambda}$ represent vectors of control variables at the zipcode-year level and their corresponding coefficients, respectively.

- Table 3 here -

Table 3 shows that branch closures spur decreases in physical store footfall. In a model with zipcode-level demographic controls and zipcode, week, and county-week fixed effects, column 1 shows a negative and statistically significant relation between *net branch closures* and *all visits* ($-1{,}661.29$, $t = 5.96$). To further sharpen

our test, we focus on visits to retail stores because they are more easily disrupted by digitalization than businesses such as dental clinics and auto repair shops. We classify a store as retail if its NAICS code is 442–444, 448, or 451–453 (Chava, Oettl, Singh, and Zeng, 2024). Using this classification, column 2 shows that a branch closure is associated with 280.80 ($t = 3.35$) fewer *retail visits*.

To measure the shift online, we construct *online spend gap*, defined as the difference in dollar value of online and in-store transactions at the zipcode-month level, compiled by the `SafeGraph` database. Next, we reestimate equation (2) with *online spend gap* as the dependent variable. Column 3 shows that a local branch closure is associated with an increase of \$1,714.77 ($t = 5.39$) in online transactions over in-store ones. Our estimated effect is economically significant, representing 15.6% of the magnitude of the median *online spend gap* (−\$11,017.05). We find a similar effect in the count of online transactions over in-store ones (*online transaction gap*) in column 4.

Overall, we validate the underlying premise by which branch closures affect identity theft. Driven by necessity and convenience, businesses and consumers increasingly shift to e-commerce after branch closures. However, this shift may increase the risk of identity theft as consumers' financial and personal identifying data are exchanged more frequently in the digital economy.

5 Branch closures and identity theft

We examine whether MSAs with bank branch closures have higher instances of consumer fraud, which we operationalize as the number of identity theft reports. To test this hypothesis, we estimate specification (3) for MSA i in year t.

$$\textit{ID theft reports}_{i,t} = \alpha + \beta \cdot \textit{net branch closures}_{i,t} + \mathbf{X}_{i,t}^{\top}\boldsymbol{\lambda} + \varepsilon_{i,t} \tag{3}$$

The vectors $\mathbf{X}_{i,t}$ and $\boldsymbol{\lambda}$ represent vectors of control variables at the MSA-year level and their corresponding coefficients, respectively.

- Panel A of Table III here -

Our estimates in Panel A of Table III show that MSAs with more bank branch closures experience higher volumes of identity theft. In column 1, we find that an additional bank branch closure is associated with 213.42 ($t = 5.91$) more *ID*

theft reports. Our estimated effect is economically significant. A standard deviation shock to *net branch closures* leads to an increase of 3,030.6 (= 14.2×213.42) identity theft cases, representing 2.13 times of its unconditional sample mean. In column 2, our findings remain unchanged as we control for various MSA demographic characteristics and saturate our models with MSA fixed effects and year fixed effects.

To sharpen our findings, we verify that our results are driven by MSAs with diminishing branch presence in our sample. To do so, we define Δ *branch* $(-)$ and Δ *branch* $(+)$ as the absolute values of *net branch closures* when it is positive and negative, respectively. Consistent with our priors, column 3 shows that a unit increase in Δ *branch* $(-)$ is associated with 166.92 ($t = 6.33$) more *ID theft reports*. In contrast, the effect of Δ *branch* $(+)$ on identity theft is much smaller and statistically insignificant. To make a tighter link between consumers and banks, we further use the CFPB Consumer Complaints Database to show that customers *of a bank* are more likely to submit identity theft complaints when its branches close in the local area. We discuss these additional results in the Appendix III.

Overall, we find that identity theft is more prevalent in MSAs with bank branch closures. Importantly, by controlling for MSA and year fixed effects, our findings cannot be attributed to persistent, unobserved factors that affect both bank branching decisions and identity theft.

6 Identification strategy

Although our regressions in the previous section control for MSA and year fixed effects, there remain concerns of time-varying local factors that could drive both branch closures and identity theft. To demonstrate causality, we require variation that is plausibly exogenous to such local factors, in the incidence of branch closures. Using an instrumental variable (IV) approach, we estimate the effect of branch closures in a staggered difference-in-differences model.

6.1 Instrument for bank branch closures

Following Nguyen (2019), we use staggered exposures to postmerger consolidation as an instrument for branch closures. Bank mergers create operational redundancy such that a merged institution often closes branches in areas where

the two previously separate banking networks overlap. Therefore, MSAs with both acquirer and target branches in situ are more exposed to postmerger branch closures.

The key identifying assumption is that MSA-level exposures to bank mergers are as good as randomly assigned with respect to local factors. This assumption is violated if there are systematic differences between exposed and control MSAs that would affect identity theft and the likelihood of mergers between banks of branches therein. For example, bank mergers could be more likely in economically distressed MSAs due to greater cost savings from branch consolidation. At the same time, local economic factors may be endogenous to consumer sophistication and hence susceptibility to fraud. In this case, even absent the merger, we would expect differences in identity theft cases between exposed and control MSAs.

To ensure that banks' merging decisions are plausibly exogenous to local factors, we focus on mergers where both acquirer and target banks have at least U.S. $1 billion in premerger assets. These mergers are often driven by broader goals to enter new markets and achieve synergy across business lines. By construction, these are large institutions with extensive branch networks. The median acquirer (target) in our sample holds $8.6 billion ($2.2 billion) in assets and controls 81 (24) branches across 10 (4) MSAs. As a benchmark, the median bank in the U.S. holds $0.19 billion in assets and controls only 3 branches in a single MSA. The median percentage of the acquirer (target) banks' deposits held in exposed MSAs before the mergers is only 1.03% (2.12%), so these mergers are unlikely to be motivated by local factors.

Overall, we identify 227 mergers between large banks, led by 136 unique acquirers between 2009 and 2022. These mergers are geographically diverse, covering 200 unique MSAs across 40 states.

6.2 Staggered difference-in-differences estimation

A MSA is first exposed in the year of a merger between large banks with branches in the area. Because the merger exposures are staggered across years and MSAs, we use the doubly robust Callaway and Sant'Anna (2021) difference-in-differences estimator. We recover the average treatment effects on treated (ATTs)

defined as follows.

$$\text{ATT}(g,t) = E[Y_t - Y_{g-1} \mid G_g = 1] - E[Y_t - Y_{g-1} \mid C = 1] \tag{4}$$

Among MSAs that were first exposed to merger shocks at year g (i.e., $G_g = 1$), the first expectation takes the difference in the outcomes of Y at year t and at year $g-1$. The second expectation computes the same difference, but only among control MSAs which are never exposed to the merger shocks (i.e., $C = 1$). These ATTs are the building blocks of the estimator.

- Figure 3 here -

To facilitate a transparent examination of our results, we present event-time plots in Figure 3. At every event-time $\tau \in [-10\,..\,+10]$ in years, we aggregate the ATT(g,t)'s by averaging over all exposed MSAs that have been observed at that event-time.

$$\text{ATT}(\tau) = \frac{1}{\sum_{g,t} 1(t-g=\tau)} \sum_{g,t} 1(t-g=\tau) \cdot \text{ATT}(g,t) \quad \text{for } \tau \in [-10\,..\,+10] \tag{5}$$

In the top subfigure, we find no statistically significant differences in net branch closures in the (blue) preexposure period.[7] However, we find a mostly increasing trend of net branch closures in the (red) postexposure period. These patterns validate the "first-stage" of our empirical design by showing exposed MSAs have significantly fewer bank branches after the shocks. In the bottom subfigure, we find a statistically significant and steady rise in identity theft reports in the postexposure period. The lack of pretrend differences supports our identifying assumption that the assignment of merger exposures is orthogonal to local factors that affect identity theft.

- Table 5 here -

We summarize the ATTs of merger exposures on branch closures and identity theft reports in Table 3. The preexposure ATT averages the ATT(τ)'s for event-time τ between -10 and -1. The postexposure ATT does likewise but for τ between $+1$ and $+10$. Equation (6) defines the overall ATT, which is the simple average of all

[7] For brevity, we truncate the plot at $\tau = -5$ by summing up the ATT(τ), $\forall \tau \leq -5$.

ATT(g,t)'s for all $t \geq g$.

$$\text{Overall ATT} = \frac{1}{\sum_{g,t} 1(t \geq g)} \sum_{g,t} 1(t \geq g) \cdot \text{ATT}(g,t) \tag{6}$$

Consistent with the parallel trends assumption holding in Figure 3, we find small preexposure ATTs on branch closures and identity theft reports. Rather, the treatment effects obtain after the merger exposures with large and statistically significant postexposure ATTs. The overall ATT on identity theft reports is positive and statistically significant ($+455.56, t = 2.72$). Given the ATT on branch closures of +2.79 ($t = 3.27$), a single branch closure would correspond to an increase of +163.28 (= 455.56/2.79) identity theft reports. Reassuringly, this estimate is both smaller and relatively close in magnitude compared to its OLS counterpart in column 1 of Table III.[8] We should expect OLS regressions to overestimate the effect of branch closures on identity theft because there may be observed and unobserved heterogeneity driving both of them at the MSA level.

6.3 External validity of LATE

While merger exposures are as good as randomly assigned to MSAs (i.e., the identifying assumption), the merged bank ultimately still selects which branches to close across the exposed MSAs. This potentially endogenous selection does not invalidate our identification strategy, which only requires that *exposure* to mergers is exogenously determined. However, it affects the interpretation of the local average treatment effect (LATE). For example, MSAs that are exposed to mergers and subsequently encounter branch closures might systematically differ from those that do not in ways that affect identity theft.

With heterogeneous treatment effects, the LATE identified above is the treatment effect on compliers. Drawing from the potential outcomes framework of Angrist, Imbens, and Rubin (1996), compliers are MSAs that (do not) encounter branch closures due to the (absence) presence of merger exposures. But, the population also contains (i) "always-takers" where branches would have closed regardless of merger exposures, (ii) "never-takers" where no branches close even with merger exposures, and (iii) "defiers" which do the opposite of the assignment. To

[8] Moreover, the closeness of economic magnitudes is indicative of a strong instrument (Jiang, 2017).

examine the generalizability of our LATE beyond compliers, we use the framework of Marbach and Hangartner (2020) to estimate covariate means within subpopulations. Crucially, similar covariate means between the compliers and the full sample increase confidence in the external validity of our LATE.

To fix ideas, every MSA has two unobserved potential treatment indicators $D(0)$ and $D(1)$ that manifest an observed treatment $D \in \{0,1\}$ representing the presence of branch closures. The indicator Z switches on if an MSA is exposed to mergers. The matrix below maps the treatment responses to Z of the subpopulations.

	$D(Z=0)$	$D(Z=1)$
Compliers	0	1
Always-Takers	1	1
Never-Takers	0	0
Defiers	1	0

Because we only observe the realized treatment D but not $D(0)$ and $D(1)$, we cannot classify individual MSAs into subpopulations. Specifically, compliers and always-takers assigned to the exposure group ($Z=1$) are observably identical. The same applies to compliers and never-takers assigned to the control group ($Z=0$). However, Marbach and Hangartner (2020) proposes a framework to estimate the mean of a covariate X within subpopulations by imposing four mild assumptions.

Assumption 1 (Monotonicity)**.** $D(1) \geq D(0)$.

Assumption 2 (Independence of instrument)**.** $D(0), D(1), X \perp\!\!\!\perp Z$.

Assumption 3 (Relevance condition)**.** $E[D \mid Z=1] \neq E[D \mid Z=0]$.

Assumption 4 (Probability bounds on assignment)**.** $0 < \Pr(Z=1) < 1$.

Assumption 1 is standard in IV analysis and posits that the instrument cannot have an opposite effect on any subpopulation, thereby ruling out defiers (Angrist, Imbens, and Rubin, 1996). Assumption 2 implies the independence of Z with both X and $D(Z)$, which holds if merger exposures are randomly assigned across MSAs. Assumption 3 is the relevance condition, which guarantees that the fraction of compliers is nonzero. The assumption 4 strictly bounds the probability of assignment between 0 and 1 to ensure there is variation in Z across MSAs.

Under assumptions 1 and 2, observable and unobservable always-takers draw

from the same distribution of X. So, we can profile the covariate mean for always-takers by focusing on the observable subset of nonencouraged ($Z = 0$) MSAs that experience branch closures:

$$E[X \mid D(0) = D(1) = 1] = E[X \mid D = 1, Z = 0] \tag{7}$$

By the same logic, we can profile the covariate mean for never-takers by focusing on encouraged ($Z = 1$) MSAs that do not experience branch closures:

$$E[X \mid D(0) = D(1) = 0] = E[X \mid D = 0, Z = 1] \tag{8}$$

We cannot immediately estimate the covariate means for compliers because they are observably identical to always-takers and never-takers when $Z = 1$ and $Z = 0$, respectively. Instead, we first decompose the population mean into a linear combination of subpopulation means by the Law of Iterated Expectations:

$$\begin{aligned} E[x] = \quad & E[X \mid D(1) > D(0)] \cdot \Pr[D(1) > D(0)] \\ + \quad & E[X \mid D(1) = D(0) = 1] \cdot \Pr[D(1) = D(0) = 1] \\ + \quad & E[X \mid D(1) = D(0) = 0] \cdot \Pr[D(1) = D(0) = 0] \end{aligned} \tag{9}$$

Substituting in equations (7) and (8) and expanding all conditionals, we can express the covariate mean for compliers as a function of observables.

$$\begin{aligned} E[X \mid D(1) > D(0)] = & \left(E[X] - \frac{E[X 1_{\{D=0,Z=1\}}]}{\Pr[Z = 1]} - \frac{E[X 1_{\{D=1,Z=0\}}]}{1 - \Pr[Z = 1]} \right) \\ & \left(1 - \frac{\Pr[D = 0, Z = 1]}{\Pr[Z = 1]} - \frac{\Pr[D = 1, Z = 0]}{1 - \Pr[Z = 1]} \right)^{-1} \end{aligned} \tag{10}$$

We map the population moments in equation (10) to their sample analogs in the Internet Appendix.

- Table 6 here -

Table 6 presents the estimated covariate means in 2010 for the full sample and subpopulations. Against the secular trend of branch closures in the U.S., always-taker MSAs make up a large proportion of our sample. Always-taker MSAs tend to have smaller, older populations and fewer bank branches, suggesting that they are relatively unattractive banking markets. In contrast, never-taker MSAs that have

no branch closures irregardless of merger exposures have significantly larger populations, more branches, and higher household incomes. These MSAs are likely population centers where branch presence may be profitable or strategically important.

Complier MSAs have slightly larger populations but are otherwise representative of the average MSA in our sample, supporting the generalizability of our LATE. Notably, we find that compliers have significantly fewer identity theft cases than the average MSA. Thus, among MSAs eligible for postmerger branch consolidation, branch closures tend to occur in areas that are already less prone to identity theft for reasons unobserved to us. One possible reason is that consumers in complier MSAs may be more digitally savvy, making digital banking a less costly substitute for physical branches. Such consumers are also less likely to be victims of identity theft. In this case, our estimated treatment effects may underestimate the impact of branch closures in the average MSA where consumers are less digitally savvy.

7 Mechanism: The digital channel

We propose that branch closures push consumers to engage more with the digital economy, thereby exposing them to greater risk of consumer fraud. To provide evidence of this mechanism, we design two sets of tests showing that branch closures affect consumers through the digital channel. First, we examine whether the effect of branch closures on identity theft is stronger in areas where consumers are less prepared for digital engagement. Second, we directly test whether branch closures lead to greater mobile app usage, validating the shift toward digital economic interactions.

7.1 Heterogeneous effects of branch closures

Previously, we use large bank mergers to carefully identify the effect of branch closures on consumer fraud. However, those results in themselves do not speak to the mechanism by which some consumers are pushed to engage with the digital economy after branch closures. To flesh out this mechanism, we retain the difference-in-differences framework but distill our main merger-exposure IV by the ability of bank customers to safely engage with the digital economy. We expect

branch closures to have a stronger effect on identity theft when consumers are less able to make the digital transition.

We first classify each large bank merger by the acquirer-bank customers' reliance on bank branches. Following Jiang, Yu, and Zhang (2023), we measure *branch reliance* of a bank as the ratio of the number of branches to its total deposits. A high *branch reliance* measure of a bank implies that its customers are likely more accustomed to physical banking and hence less able or prepared to go online. Among the set of large bank mergers, we classify a merger as having high (low) *branch reliance* if its value is above (below) the yearly median. We predict that branch closures has a stronger effect on identity theft when consumers rely more on bank branches in the first place.

- Table 7 here -

The results in Panel A of Table 7 support our prediction. The IV in columns 1 and 2 is an MSA's exposure to large bank mergers in which the acquirer has high *branch reliance*. On average, this exposure leads to 11.67 (t = 2.70) net branch closures and 2,362.36 (t = 2.92) ID theft reports. Thus, the Wald estimate reveals that a merger-induced branch closure causes 202.43 (= 2,362.36/11.67) more cases of identity theft. We find weaker results in columns 3 and 4 where the IV is an MSA's exposure to mergers characterized by low *branch reliance*. The second-stage estimate is smaller than one-fifth that in column 2. Moreover, since the first-stage estimate is statistically insignificant, the Wald estimate will be noisy and uninformative (Jiang, 2017). Therefore, branch closures may disproportionately affect consumers who rely more on bank branches because they are less able to or prefer not to engage digitally.

In Panel B, we classify bank mergers by the *digital focus* of the acquirers. We measure the *digital focus* of a bank as the ratio of the all-time download volume of its mobile app on the `Google Play Store` to its number of branches. A digitally focused bank likely has fewer number of branches per mobile app user, compared to another bank that has a digital presence but also caters to the physical banking preferences of some customers. So, customers of a bank with lower (higher) *digital focus* are more (less) likely to be pushed online after branch closures. Columns 1 and 2 indicate that a branch closure leads to 145.96 (= 281.70/1.93) more cases of identity theft in MSAs exposed to mergers with low *digital focus*.[9] Consistent

[9]We classify mergers by the *digital focus* of their acquirers. An acquirer is labelled as low (high)

with our prediction, this effect is much weaker (86.11) when we switch to bank mergers marked by high *digital focus*.

In Panel C, we use Census Bureau data to separate exposed MSAs by the proportion of people who has an internet subscription (*consumer tech-savviness*). Columns 1 and 2 show that a branch closure leads to 208.54 (= 398.31/1.91) more cases of identity theft in MSAs with low *consumer tech-savviness*. This effect is 15.4% smaller among MSAs where consumers are more tech-savvy. Consistent with our prior findings, our results suggest that branch closures have a stronger effect on identity theft in areas where consumers are less prepared to engage with the digital economy.

Overall, we augment our difference-in-differences design to shed light on how branch closures lead to more consumer fraud. We find that the treatment effect is stronger when (i) consumers are more reliant on bank branches, (ii) banks are less digitally focused to start with, and (iii) consumers are less tech-savvy. Therefore, our findings support our proposed mechanism in which branch closures may disproportionately harm some consumers who are ill-equipped or unable to safely engage with the digital economy.

7.2 Mobile app usage

Our results in Section 4 indicate that consumers visit physical stores less after branch closures in the local area. However, it remains unclear whether consumers also engage more with the digital economy. It is crucial to explore these questions for two reasons. First, identity theft typically occurs online. So, we need to demonstrate that consumers spend more time online to validate the link between branch closures and identity theft. Second, the lower frequency of consumer visits to physical stores—in itself—may be driven by local economic conditions, which in turn correlate with branch closures. Thus, directly showing that consumers substitute their physical consumption with digital consumption provides a sharper test of our proposed mechanism.

We measure consumer-level mobile application (app) consumption using the `Magnify` database from Global Wireless Solutions (GWS). GWS curates a panel of opted-in consumers using Android smartphones that is demographically representative of the United States population. Within the panel, GWS continuously tracks

digital focus if its value is below (above) the yearly median.

every consumer's mobile activity 24 hours a day, seven days a week. When a consumer uses her smartphone, we can observe among many statistics the (i) name of app used, (ii) time and duration of app usage, and (iii) her current latitude and longitude coordinates. Crucially, we can infer the zipcode of a consumer's primary residence by her most frequented location between 9.00 pm and 6.00 am in her local time zone, which we determine by her location data. Finally, we aggregate every consumer's *mobile app usage* to the monthly level and merge in branch closures occurring in her residence county in that month. In all, we assemble a micro-dataset of mobile app usage by 194,530 consumers between 2019 and 2022.

The structural relation of interest is the effect of local branch closures in county z on a consumer's (i) mobile app usage in month t. The vectors $\mathbf{X}_{i,z,t}$ and $\boldsymbol{\lambda}$ represent vectors of county and consumer characteristics and their corresponding coefficients, respectively.

$$\textit{mobile app usage}_{i,z,t} = \alpha + \beta \cdot \textit{net branch closures}_{z,d} + \mathbf{X}_{i,z,t}^{\top}\boldsymbol{\lambda} + \varepsilon_{i,z,t} \tag{11}$$

The OLS estimate for β is unbiased if *net branch closures* are orthogonal to $\varepsilon_{i,z,t}$. In general, this assumption is unlikely to hold because there may be unobservable forces (e.g., consumer preferences to live in a particular area) driving both branch closures and mobile app usage. The identification of β is also threatened by reverse causality—greater digital adoption in the local area leads banks to concentrate branch closures there.

To overcome these identification challenges, we instrument for branch closures with consumers' staggered exposures to large bank mergers. Although our dataset of mobile app usage has a relatively short sample period, its high frequency (monthly) and granularity (consumer-level) ensure that we have ample statistical power to perform this test. We present the Callaway and Sant'Anna (2021) ATTs of merger exposures on mobile app usage in Table 8.

- Table 8 here -

Our results indicate that branch closures in the local area lead consumers to increase mobile app usage. The first stage in column 1 shows that consumers exposed to large bank mergers encounter 0.072 (t = 3.96) more branch closures per month. This is an economically sizable effect, representing a 16.7% increase over the number of branch closures (0.432) encountered by the average consumer in a month. In the second stage contained in column 2, we find that consumers

exposed to merger exposures spend 2.76 (t = 3.20) more hours on mobile apps. Taken together, the Wald estimate reveals that a merger-induced branch closure causes an increase of 38.33 (= 2.760/0.072) hours in mobile app usage in a month, or more than 1.2 hours more per day.

Overall, using novel microdata on mobile app usage, we show that branch closures cause consumers to engage more with the digital economy. These findings validate the link between branch closures and identity theft, which typically occurs online. Moreover, our results help to reject the notion that local economic conditions alone drive the observed shifts in consumer behavior. While banks may strategically close branches in locales where digital adoption is higher among consumers, the effect identified by our IV design is unlikely to suffer from this reverse causality bias.

8 Adversarial activities

As branch closures push consumers to rely more on digital services, their personal identifying information (PII) are more widely shared across platforms, creating greater exploitation opportunities for adversaries. Thus, we would expect to observe a rise in adversarial actions that directly affect consumers in areas impacted by branch closures. These actions often begin with unwanted calls, where adversaries impersonate trusted institutions to extract sensitive information. Vulnerable populations, such as military veterans, are particularly at risk due to their frequent interactions with financial institutions and the high value of their benefits. Finally, as consumers' reliance on digital banking grows, phishing attacks targeting their financial information also become more prevalent.

We begin by exploring the vulnerability of military veterans to identity theft. Veterans are an important group to study because they face a higher risk of identity theft. They are often targeted for their valuable benefits and frequently have to share personal information to access these benefits. So, veterans should be disproportionately affected by branch closures. Using an instrument based on the Vietnam War draft lotteries, we obtain sharper identification on how branch closures disproportionately affect regions with more veterans.

Next, we examine the prevalence of unwanted calls in local areas after branch closures. Many identity theft schemes are initiated through phone calls, with ad-

versaries impersonating trusted institutions to extract sensitive information. Advancements in telecommunications technology, including robocalls, have amplified this threat, particularly in areas where consumers rely on digital interactions due to branch closures.

Finally, we investigate phishing attacks, which are a major driver of identity theft. Adversaries are increasingly impersonating bank websites to deceive consumers into sharing personal and financial information. We show that areas with branch closures experience higher exposure to phishing attacks, and this exposure is positively associated with identity theft reports.

8.1 Veterans' vulnerability to identity theft

Identity theft is a serious issue for U.S. military veterans. According to the FTC, veterans reported a record 45,882 bank-related identity theft cases in 2022, marking a 28.8% surge over three years. They are more than twice as likely to be victims of identity theft than civilian Americans. Furthermore, the American Association of Retired Persons (AARP) estimates that veterans who are victims of fraud and scams are around 40% more likely to lose money and often lose more money than civilians.

Veterans are particularly vulnerable to identity theft for four reasons. First, veterans are attractive targets for adversaries because of the significant financial value of veteran benefits such as disability compensation, pensions, and healthcare. Second, veterans often share their personal identifiable information. For example, to claim a military discount in-store, veterans must present their DD214, a document that includes a veteran's full name, SSN, and date of birth, and address. Third, the transition to civilian life often involves financial adjustments and increased interactions with financial institutions, which may lack robust security measures against identity theft. Fourth, many veterans are elderly and may be unfamiliar with digital security practices, making them more susceptible to online fraud.

If branch closures affect identity theft, then we should expect this effect to be greater in MSAs with more veterans. To test this hypothesis, we encounter the following endogeneity problem. Military veterans facing financial hardship may concentrate in economically vulnerable areas. These areas might face more branch closures and inherently have higher rates of identity theft due to unobserved risky

financial behaviors, such as using unsecured credit or seeking aid through insecure channels. Consequently, a spurious relation might exist between veteran population, branch closures, and identity theft.

To generate plausibly exogenous variation in veteran populations, we construct MSA-level exposures to veterans by exploiting the Vietnam War draft lotteries (e.g., Angrist and Chen, 2011). The draft lotteries held in 1971 and 1972 involved males aged 19 years old in those years. This implies that males born 19 years earlier in 1951 and 1952 would have been at risk of conscription in the respective lotteries. Our idea is that these lotteries "seeded" more veterans in MSAs that happen to have more eligible-age males in those years. To operationalize the instrument, we define *draft share* as the MSA share of males aged eight and nine in the 1960 U.S. Census. The MSA shares of veterans are highly persistent across time. On average, a percentage point of *draft share* (i.e., constructed from the 1960 Census data) is associated with 0.74 percentage points of MSA shares of veterans in our sample period. Overall, absent any systematic displacement patterns, an MSA with higher *draft share* is likely to have more veterans in our sample period.

The central identifying condition is that *draft share* must be plausibly exogenous to local conditions that may affect identity theft. There are two reasons why this condition is likely satisfied. First, the distribution of males aged eight and nine in 1960 across MSAs predates the emergence of modern identity theft and its determinants more than six decades later. Specifically, childbearing decisions and subsequent gender of births in the 1950s are unlikely connected to recent identity theft trends. Second, the draft lotteries were implemented uniformly in all MSAs. So, their effects on veteran population changes are driven by national policy rather than local economic or social conditions. In a regression of *draft share* on MSA characteristics, no characteristic has a partial R^2 of more than 0.01% except for *population* with a partial R^2 of 35.9%. This exception is unsurprising because *population* is mechanically correlated with *draft share* by construction, but it behooves us to control for it in our tests.

- Table 9 here -

The structural relationship of interest is the interacted effect of veteran population and branch closures in MSA i on local identity theft reports at year t:

$$\textit{ID theft reports}_{i,t} = \alpha + \beta \cdot (\textit{veterans}_{i,t} \times \textit{net branch closures}_{i,t}) + \mathbf{X}_{i,t}^{\top}\boldsymbol{\lambda} + \varepsilon_{i,t} \quad (12)$$

The variable *veterans* (abbreviated by v) is the number of male veterans ($\times 10^5$) aged 55–74 in the MSA. We focus on this age range because males subjected to the draft lotteries would have been between 58 and 70 years old in our sample period (2010–2022).[10] As a benchmark, we first estimate an OLS regression of equation (12) in column 1 of Table 9. We find that a 100,000 increase in the number of *veterans* is associated with 5,089.43 ($t = 2.13$) more identity theft reports in the MSA. More importantly, the interaction term *veterans* × *net branch closures* has a positive and statistically significant loading. This suggests that branch closures exacerbate the vulnerability of veterans to identity theft.

To address endogeneity concerns, we estimate a two-stage instrumental variable (IV) regression, using *draft share* as an instrument for *veterans*. Column 2 reports the first-stage regression. We observe that *draft share* has a significantly positive association with *veterans* (481.49, $t = 88.24$), with a high R^2 of 84.5%. The F-statistic of 1,123.32 exceeds the Stock and Yogo (2005) critical value at the 10% maximal IV size threshold (16.38). Following Jiang (2017), we also perform a partial R^2 decomposition on the first-stage regression and find that *draft share* alone explains 65.4% of the variance in *veterans*. Therefore, our results indicate that *draft share* is a strong instrument for veteran population, fulfilling the relevance condition.

Next, we interact the instrumented *veterans* (i.e., $\widehat{v}$) with *net branch closures* in the second-stage regression. The estimated loading on the interaction term in column 3 ($+3.65, t = 5.49$) is 40% smaller than its OLS counterpart in column 1 but remains highly significant. This comparison suggests that our IV approach adjusts for the upwards bias in the OLS estimate due to endogeneity concerns. Our IV estimate is also economically significant. Evaluated at the mean of $\widehat{v}$ ($= 1.8 \times 10^5$), a unit standard deviation increase in *net branch closures* leads to 336.87 more *ID theft reports*. This incremental increase represents 23.7% of the unconditional mean of *ID theft reports*.

Overall, we find causal evidence that branch closures significantly increase the incidence of identity theft in areas with more military veterans. Our findings underscore the importance of considering the welfare costs associated with branch closures, particularly in vulnerable or economically fragile communities.

[10] Our Census Bureau data does not have a more detailed breakdown of MSA-level veteran populations by age.

8.2 Unwanted calls

In many identity theft schemes, phone calls are the first conduit between the adversary and the consumer. Adversaries tend to impersonate trusted institutions like banks or government agencies on these calls to extract personal identifying information such as Social Security numbers and bank account details. Greater engagement with the digital economy and increased phone-based interactions after branch closures make consumers more vulnerable to these attacks for two reasons. First, consumers' phone contact details are often shared in the delivery of digital services. In turn, security breaches on the end of the service providers may expose these details to adversaries. Second, as consumers increasingly rely on digital and phone-based interactions, adversaries can more readily exploit their trust placed on these systems.

To compound the problem, advancements in telecommunications technology have enabled the rise of "robocalls", which are automated calls that can reach large numbers of consumers at low cost. This trend prompted the FTC to alert consumers to the use of robocalls in phone scams, especially in relation to identity theft (FTC, 2024b). In a notable enforcement action, the FTC fined VoIP (Voice-over-Internet-Protocol) provider XCast Labs U.S. $10 million in January 2024 for enabling billions of illegal robocalls, many which impersonated government agencies to commit fraud.[11]

We collect data to test whether unwanted calls are more prevalent following branch closures in the local area. From the FTC Do-Not-Call (DNC) Reported Calls database, we first collect 1,015,744 complaints of unwanted calls and robocalls—which we collectively term as unwanted calls for brevity—lodged between 2014 and 2022. Next, we aggregate them at the MSA-day level and merge in net branch closures in the MSA over the past 180 days. Because not all unwanted calls are related to identity theft, we also collect the number of telemarketing calls received at the MSA-day level to control for baseline telemarketing activity. This control addresses the concern that increased unwanted calls after branch closures are merely due to broader telemarketing trends.

To test our hypothesis, we estimate the following OLS models for MSA i on

[11] Under the FTC's Telemarketing Sales Rule, an illegal robocall is one that, among other violations, fails to obtain prior consent from the recipient, disregards the National Do-Not-Call (DNC) registry, or uses false or misleading information to induce sales or payments.

day d:

$$\left\{ \begin{array}{c} 1(unwanted\ calls)_{i,d} \\ unwanted\ calls_{i,d} \end{array} \right\} = \alpha + \beta \cdot \sum_{t=d-180}^{d-1} net\ branch\ closures_{i,t} + \mathbf{X}_{c,d}^{\top} \boldsymbol{\lambda} + \varepsilon_{c,d} \quad (13)$$

where the vectors $\mathbf{X}_{i,d}$ and $\boldsymbol{\lambda}$ represent vectors of control variables at the MSA-year level and their corresponding coefficients, respectively.

- Table 10 here -

Our results in Table 10 suggest that consumers receive more unwanted calls following branch closures in the local area. The dependent variable in columns 1 through 3 is an indicator 1(*unwanted calls*) that switches on if there is at least one unwanted call or robocall reported by consumers in a MSA to the FTC on a given day. On the extensive margin, column 1 shows that a branch closure in the local area is associated with a 0.121 ($t = 2.59$) percentage points higher probability of receiving any unwanted calls in a MSA-day. This estimate is economically significant—a one standard deviation increase in *net branch closures* leads to a 6.75% increase over the unconditional probability of unwanted calls (25.4%).

To sharpen our findings, we then distinguish between unwanted calls received on wireless devices and wired devices. We posit that, following branch closures, consumers share more personal data via mobile apps and websites, which are more accessible on wireless devices than on wired ones. Column 2 shows a significantly positive relation between wireless unwanted calls and branch closures. In comparison, the estimated loading on *net branch closures* in column 3 is 39% smaller and statistically insignificant. Finally, we replicate our analysis on the intensive margin by swapping the dependent variable to *unwanted calls*—the count of unwanted calls received by consumers at the MSA-day level. Our conclusions remain unchanged by our results in columns 4 to 6.

Overall, our evidence indicates that unwanted calls rise following bank branch closures, with wireless devices being particularly affected. The ease of accessing personal information on mobile devices makes wireless communication more vulnerable. As consumers engage more with the digital economy after branch closures, their risk of phone-based identity theft could increase. This section also suggests that consumers in the local area are increasingly targeted after branch closures.

8.3 Phishing attacks

According to the Federal Trade Commission (FTC), a significant portion of identity theft cases stem from phishing attacks, where adversaries deceive consumers into providing personal information through deceptive emails or websites (FTC, 2024a). The adversaries then use the information to open bogus accounts or access existing ones. As bank branches close, consumers increasingly shift to online banking and expand their digital footprints, making them more susceptible to phishing attacks.

In phishing attacks, adversaries often clone the brand's official website and use it as a template for malicious use.[12] Thus, many phishing websites have the same exact "favicons" (i.e., abbreviation for favorite icons) as their legitimate counterparts. Favicons are small logos shown on internet browser tabs to provide a recognizable brand identity to consumers. By detecting the appearances of suspicious websites using the favicons of a bank's website, we can potentially track the intensity of phishing attacks on its consumers.

To identify phishing attacks, we begin by hand-collecting "favicons" from websites of the top 100 U.S. banks by total assets in 2022. Next, we represent every favicon as an integer hash using the MMH3 (MurmurHash3) hashing algorithm. For example, the favicon of the Wells Fargo Bank website maps to the hash value "893468414".[13] We then query this hash value on the `Shodan` search engine to obtain the monthly number of web servers that are hosting websites with the same favicon. `Shodan` indexes devices connected to the internet, including their open ports, running services, and potential vulnerabilities. To exclude legitimate websites from our query, we filter out those with secure-socket-layers (SSL) certificates, which authenticate website identities and enable secure data transmission.[14]

We create a novel measure of consumers' exposure to phishing attacks at the MSA-bank-month level. For bank b servicing the set S_b of MSAs indexed by i in month m, we construct a MSA-bank-month measure of *phishing exposure* as the product of (i) the month-over-month change in the number of phishing sites

[12] Typically, they obtain unlicensed developer kits of the official website from underground markets.

[13] This favicon can be found at `https://www.wellsfargo.com/favicon.ico`.

[14] Some of the remaining websites might not be phishing websites, but are still suspicious from a cybersecurity standpoint. Even so, this measurement noise likely biases against us finding results.

impersonating a bank, and (ii) the population weight of the MSA relative to all MSAs serviced by the bank.

$$phishing\ exposure_{i,b,m} := \Delta_{m-1,m}(num.\ phish\ sites)_b \times \frac{population_{i,m}}{\sum_{i \in S_b} population_{i,m}} \quad (14)$$

Intuitively, phishing attacks on a bank affect an MSA relative to its population weight, as larger populations have more potential victims, thereby increasing overall exposure. So, *phishing exposure* could vary over time due to the emergence of phishing attacks and shifts in the bank's operational exposure to different MSAs.

- Table 11 here -

To investigate the relation between *phishing exposure* and branch closures, we estimate the equation (15) at the MSA-bank-month level.

$$phishing\ exposure_{i,b,m} = \alpha + \beta \cdot net\ branch\ closures_{i,b,m} + \varepsilon_{i,b,m} \quad (15)$$

Column 1 of Table 11 shows that branch closures are positively and significantly associated with *phishing exposure*. This suggests that banks that close branches tend to be targeted by more phishing attacks, with MSAs that have larger population weights being hit harder.

Next, we examine whether phishing attacks has an effect on identity theft at the MSA level. We aggregate *phishing exposure* to the MSA-year level by averaging their predicted values, weighted by the number of branches every bank operates in the MSA.

$$MSA\ phishing_{i,t} := \sum_{\text{year}(m)=t} phishing\ exposure^{(\text{pred})}_{i,b,m} \times \frac{(num.\ branches)_{i,b,m}}{(num.\ branches)_{i,m}} \quad (16)$$

Column 2 shows that *MSA phishing* has a positive and statistically significant relation with identity theft. A standard deviation increase in *MSA phishing* is associated with 375.40 (= 0.0245 × 15,300) more reports of identity theft. In columns 3 and 4, we repeat our analysis using an out-of-sample variant of *MSA phishing*. Using predictive loadings from equation (15) estimated between 2018–2019, we continue to find that *MSA phishing* is strongly associated with identity theft in 2020–2022.

Overall, our results indicate that branch closures in an MSA could make its

consumers more attractive targets of phishing attacks. Furthermore, higher exposures to these attacks are associated with more identity theft reports.

9 Mechanism: Shift toward digital transactions

Branch closures may indirectly impact crime through economic forces that also influence identity theft. Specifically, branch closures increasingly push consumers to adopt digital, noncash transactions, which in turn expose them to identity theft. Consequently, this shift may reduce the incidence of crimes such as robberies, which tend to involve cash or items of immediate value. As cash usage decreases after branch closures, the financial payoffs to robberies in the local area may also decrease. Concurrently, criminals facing resource constraints may substitute away from cash-related crimes towards cybercrimes such as identity theft.

Alternatively, the mediating channel above may be absent. Rather, branch closures might be directly associated with criminal activity for reasons unrelated to identity theft. For example, branch closures may herald local economic declines, with local businesses struggling and unemployment rates rising. The accompanying social instability and desperation may lead to more crimes in local areas. However, branch closures could also lead to a decline in nearby businesses and services, thereby reducing foot traffic and the potential for opportunistic crime.

- Figure 4 here -

To distinguish between the two channels, we perform Sobel-Goodman decompositions to investigate whether identity theft mediates the relation between branch closures and crime. Figure 4 presents the schematic diagram of these decompositions. For MSA i in year t with a vector of controls $\mathbf{X}_{i,t}$ used in Table III, we first estimate the total effect of branch closures on crime, represented by γ^c.

$$crime_{i,t} = \alpha + \gamma^c \cdot net\ branch\ closures_{i,t} + \mathbf{X}_{i,t}^{\top}\boldsymbol{\lambda} + \varepsilon_{i,t} \tag{17}$$

Next, we estimate from equations (18) and (19) γ^a, γ^b, and $\gamma^{c'}$, which we use to

decompose the total effect γ^c into its direct and indirect components.

$$\textit{ID theft reports} = \kappa + \gamma^a \cdot \textit{net branch closures}_{i,t} + \mathbf{X}_{i,t}^\top \boldsymbol{\mu} + \eta_{i,t} \tag{18}$$

$$\textit{crime}_{i,t} = \phi + \gamma^b \cdot \textit{ID theft reports} + \gamma^{c'} \cdot \textit{net branch closures}_{i,t} + \mathbf{X}_{i,t}^\top \boldsymbol{\Gamma} + \zeta_{i,t} \tag{19}$$

The direct effect is simply $\gamma^{c'}$ from equation (19), whereas the indirect effect of branch closures on crime obtains from the product of γ^a and γ^b. To assess the statistical significance of this product, we compute the z-statistic using the Sobel test.

$$z = \gamma^a \gamma^b \left[(\gamma^a)^2 (\sigma^b)^2 + (\gamma^b)^2 (\sigma^a)^2 \right]^{-\frac{1}{2}} \tag{20}$$

Finally, we quantify the mediating role of identity theft in the relation between branch closures and crime as the ratio of the indirect effect to the total effect.

$$\frac{\overbrace{\gamma^a \gamma^b}^{\text{indirect effect}}}{\underbrace{\gamma^c}_{\text{total effect}}} = \frac{\gamma^c - \gamma^{c'}}{\gamma^c} = 1 - \frac{\gamma^{c'}}{\gamma^c} \tag{21}$$

If the effect of branch closures on crime primarily acts through economic forces (e.g., use of digital transactions) related to identity theft, we expect the ratio $\gamma^a \gamma^b / \gamma^c$ to be larger.

We collect data on nine major types of crime reported in the United States. From the Federal Bureau of Investigation (FBI) `Crime Data Explorer` API, we first download annual reported incidences of every crime type at the Originating Agency (OA) level. Next, we aggregate these incidences to the MSA-year level using the latitude-longitude coordinates of the OAs. Then, we classify the types of crime by their relation to cash use. Perpetrators of burglary, robbery, and larceny, often aim to obtain cash or valuables. In contrast, motor vehicle theft, arson, homicide, aggravated assault, rape, and human trafficking usually lack a direct motive involving physical cash.

- Table 12 here -

Table 12 presents our results from Sobel-Goodman decompositions. Controlling for MSA and year fixed effects, row 1 shows that an additional branch closure is associated with 86.85 (γ^a) more cases of identity theft. This pattern is consistent with our baseline findings in Table III. There are 1.38 (γ^b) fewer cases of all crimes

per unit increase in identity theft, indicating that economic forces driving identity theft also tend to dampen conventional crime. The product $\gamma^a \gamma^b$ estimates that identity theft as a mediating channel accounts for 119.99 fewer crimes per branch closure, or 45.05% of the total effect (−266.33). These patterns support the view that the shift to digital, noncash transactions drives identity theft and reduces the financial payoffs of conventional crimes. Nevertheless, there remains a sizeable direct link between branch closures and criminal activity (54.95% = 1 − 45.05%) unexplained by the identity theft channel.

To sharpen our analysis, we separately perform the decomposition on every type of crime in rows 2 through 10. For crimes related to cash use (i.e., burglary, robbery, and larceny), we continue to find a negative and statistically significant indirect effect mediated by identity theft. This effect ranges from 42.26% to 51.93% of the estimated total effect. These results further imply a connection between the declining use of physical cash and identity theft. Consistent with this idea, we fail to find a mediating role for identity theft in the effect of branch closures on crimes that are unrelated to cash use. We find statistically insignificant indirect effects for motor vehicle theft, arson, homicide, aggravated assault, rape, and human trafficking. This is unsurprising as these crimes are likely driven by economic forces orthogonal to digital transactions and cash use.

Overall, our findings help validate that identity theft is likely driven by the shift towards digital, noncash transactions after branch closures. The significant mediating effect of identity theft on cash-related crimes points to changing financial incentives for criminals as cash usage declines. In contrast, we find no such effect for crimes unrelated to cash use, further supporting our proposed mechanism. Our findings also suggest that the shift to the digital economy is reshaping criminal behavior.

10 Conclusion

The digitalization of financial services has reshaped consumer banking and financial interactions. We examine the unintended consequences for consumers who shift from brick-and-mortar banking to online financial services. We find that after branch closures, consumers engage more with the digital economy, exposing them to a greater risk of identity theft. Technological change often creates distributional effects that exacerbate existing inequalities in disadvantaged communi-

ties. Our findings highlight the potential for digitalization to exacerbate inequalities among consumers, particularly impacting vulnerable communities such as military veterans and the less digitally savvy. This study adds to the literature on the real effects of digitalization and the potential for a tradeoff between the benefits and risks of digital financial services.

Our findings underscore the need for caution as societies transition towards a digital economy. This includes promoting financial literacy, providing support to consumers experiencing financial difficulties, and investing in cybersecurity measures to prevent cybercrime. Moreover, the results highlight the complexity of navigating the digital landscape and underscore the importance of proactive policy responses. Policymakers now spend substantial efforts to educate the public and have created cybercrime networks to quickly alert and shut down fraudulent transactions. More research is needed to understand the long-term impacts of digitalization and to develop strategies to mitigate the risks associated with it.

Finally, we caveat that we do not evaluate the *overall* welfare effects of digitalization. We have not considered the additional logistical, security, and operational costs in a non-digital counterfactual (e.g., a cash-based economy). These costs must also be balanced against the convenience, cost savings, and efficiency brought about by the digital economy. However, our evidence indicates that consumers who are pushed onto the digital economy may suffer large social costs in the form of identity theft. Thus, bank branches can remain a vital social good in the digital age, providing security and consumer protection.

References

Acemoglu, D., Makhdoumi, A., Malekian, A., and Ozdaglar, A. (Mar. 2025). "When Big Data Enables Behavioral Manipulation". American Economic Review: Insights 7, 19–38.

Acquisti, A., Taylor, C., and Wagman, L. (2016). "The economics of privacy". Journal of economic Literature 54, 442–492.

Amberg, N. and Becker, B. (2024). *Banking Without Branches*. Working paper. Stockholm School of Economics.

Angrist, J. and Chen, S. (2011). "Schooling and the Vietnam-era GI Bill: Evidence from the draft lottery". American Economic Journal: Applied Economics 3, 96–118.

Angrist, J., Imbens, G., and Rubin, D. (1996). "Identification of causal effects using instrumental variables". Journal of the American statistical Association 91, 444–455.

Armantier, O., Doerr, S., Frost, J., Fuster, A., and Shue, K. (2024). "Nothing to hide? Gender and age differences in willingness to share data". Working paper.

Benmelech, E., Yang, J., and Zator, M. (2023). *Bank branch density and bank runs*. Tech. rep. National Bureau of Economic Research.

Bian, B., Pagel, M., Raval, D., and Tang, H. (2024). *Consumer Surveillance and Financial Fraud*. Tech. rep. Working paper.

Bonfim, D., Nogueira, G., and Ongena, S. (Nov. 2020). ""Sorry, We're Closed" Bank Branch Closures, Loan Pricing, and Information Asymmetries". Review of Finance 25, 1211–1259.

Callaway, B. and Sant'Anna, P. (2021). "Difference-in-differences with multiple time periods". Journal of Econometrics 225, 200–230.

Célerier, C. and Matray, A. (2019). "Bank-Branch Supply, Financial Inclusion, and Wealth Accumulation". The Review of Financial Studies 32, 4767–4809.

Chava, S., Oettl, A., Singh, M., and Zeng, L. (2024). "Creative destruction? Impact of e-commerce on the retail sector". Management Science 70, 2168–2187.

Chen, L., Huang, Y., Ouyang, S., and Xiong, W. (2025). *The data privacy paradox and digital demand*. Tech. rep. Working paper.

Choi, H.-S. and Loh, R. K. (2024). "Physical frictions and digital banking adoption". Management Science 70, 6597–6621.

Cong, L. W., Xie, D., and Zhang, L. (2021). "Knowledge Accumulation, Privacy, and Growth in a Data Economy". Management Science 67, 6480–6492.

Cramer, K. F. (2024). "Bank presence and health". Working paper.

Cubides, E. and O'Brien, S. (2023). *2023 Findings from the Diary of Consumer Payment Choice*. Working paper. Federal Reserve Bank of San Francisco.

Drechsler, I., Savov, A., and Schnabl, P. (2017). "The deposits channel of monetary policy". The Quarterly Journal of Economics 132, 1819–1876.

Fainmesser, I., Galeotti, A., and Momot, R. (2023). "Digital privacy". Management Science 69, 3157–3173.

Fonseca, J. and Matray, A. (2024). "Financial inclusion, economic development, and inequality: Evidence from Brazil". Journal of Financial Economics 156, 103854.

FTC (2024a). *Phishing Scams*. Accessed: 2024-07-11. URL: https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams.

— (2024b). *Unwanted Calls*. Accessed: 2024-10-18. URL: https://consumer.ftc.gov/unwanted-calls-emails-and-texts/unwanted-calls.

Fuster, A., Goldsmith-Pinkham, P., Ramadorai, T., and Walther, A. (2022). "Predictably unequal? The effects of machine learning on credit markets". Journal of Finance 77, 5–47.

Garmaise, M. J. and Moskowitz, T. J. (2006). "Bank Mergers and Crime: The Real and Social Effects of Credit Market Competition". Journal of Finance 61, 495–538.

Hamdi, N., Kalda, A., and Sovich, D. (2024). *The Costs of Financial Fraud Victimization*. Working paper. University of Kentucky.

Harrell, E. and Langton, L. (2013). *Victims of identity theft, 2012*. US Department of Justice, Office of Justice Programs, Bureau of Justice.

Jayaratne, J. and Strahan, P. E. (1996). "The Finance-Growth Nexus: Evidence from Bank Branch Deregulation". The Quarterly Journal of Economics, 639–670.

Ji, Y., Teng, S., and Townsend, R. M. (2023). "Dynamic bank expansion: spatial growth, financial access, and inequality". Journal of Political Economy 131, 2209–2275.

Jiang, E. X., Yu, G. Y., and Zhang, J. (2023). *Bank Competition amid Digital Disruption: Implications for Financial Inclusion*. Working paper. UCLA.

Jiang, W. (2017). "Have instrumental variables brought us closer to the truth". Review of Corporate Finance Studies 6, 127–140.

Koont, N. (2024). *The Digital Banking Revolution: Effects on Competition and Stability*. Working paper. Stanford University.

Liu, Z., Sockin, M., and Xiong, W. (2023). *Data privacy and algorithmic inequality*. Tech. rep. Working paper.

Marbach, M. and Hangartner, D. (2020). "Profiling compliers and noncompliers for instrumental-variable analysis". Political Analysis 28, 435–444.

Martín-Oliver, A., Toldrà-Simats, A., and Vicente, S. (2020). *The Real Effects of Bank Branch Closings and Restructurings*. Working paper. University of Luxembourg.

Nguyen, H.-L. (2019). "Are credit markets still local? Evidence from bank branch closings". American Economic Journal: Applied Economics 11, 1–32.

Qi, S., De Haas, R., Ongena, S., Straetmans, S., and Vadasz, T. (July 2024). "Move a little closer? Information sharing and the spatial clustering of bank branches". Review of Finance 28, 1881–1918.

Ramadorai, T., Uettwiller, A., and Walther, A. (2025). "The Market for Data Privacy". Working paper.

Sakong, J. and Zentefis, A. K. (2024). *Bank Branch Access: Evidence from Geolocation Data*. Working paper. Federal Reserve Bank of Chicago.

Stock, J. and Yogo, M. (2005). "Testing for Weak Instruments in Linear IV Regression". *Identification and Inference for Econometric Models*. Ed. by D. Andrews. New York: Cambridge University Press, 80–108.

Tirole, J. (2021). "Digital dystopia". American Economic Review 111, 2007–2048.

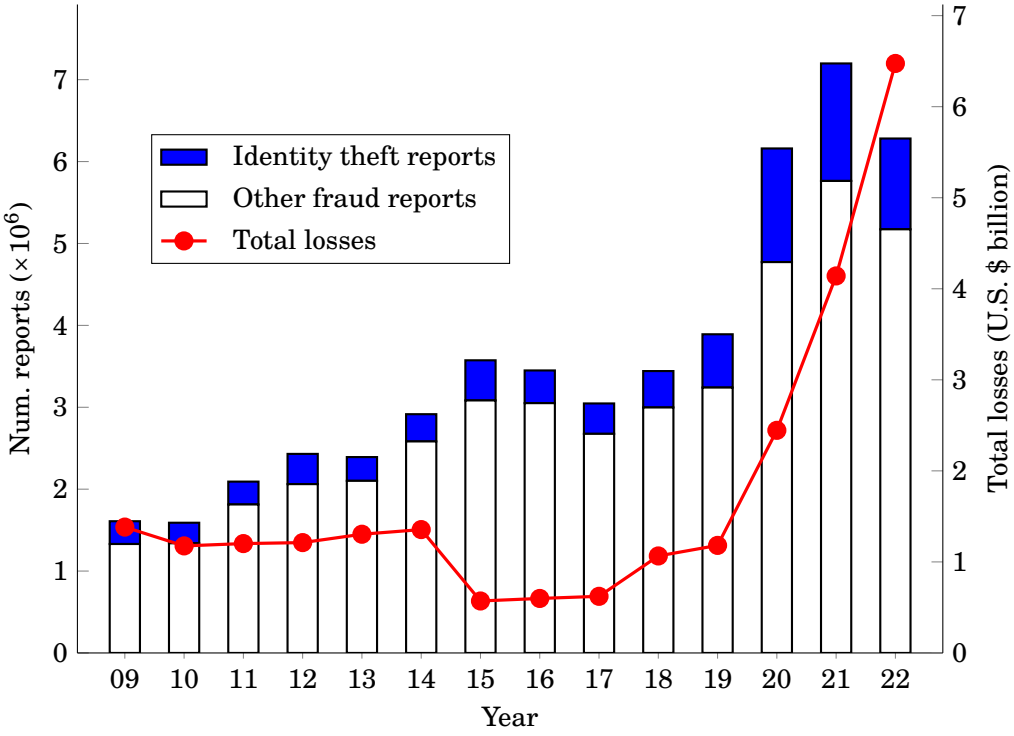
— (2023). "Competition and the industrial challenge for the digital age". Annual Review of Economics 15, 573–605.

Veldkamp, L. (Jan. 2023). "Valuing Data as an Asset". Review of Finance 27, 1545–1562.

Veldkamp, L. and Chung, C. (June 2024). "Data and the Aggregate Economy". Journal of Economic Literature 62, 458–84.

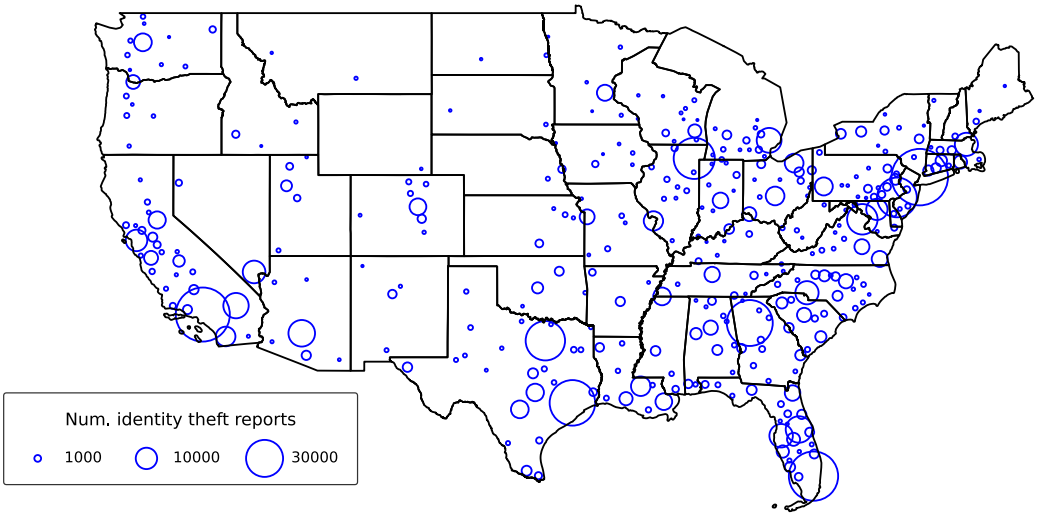
Yin, W., Hay, J., and Roth, D. (2019). "Benchmarking zero-shot text classification: Datasets, evaluation and entailment approach". arXiv preprint arXiv:1909.00161.

Figure 1. Annual trends of consumer fraud in the U.S.



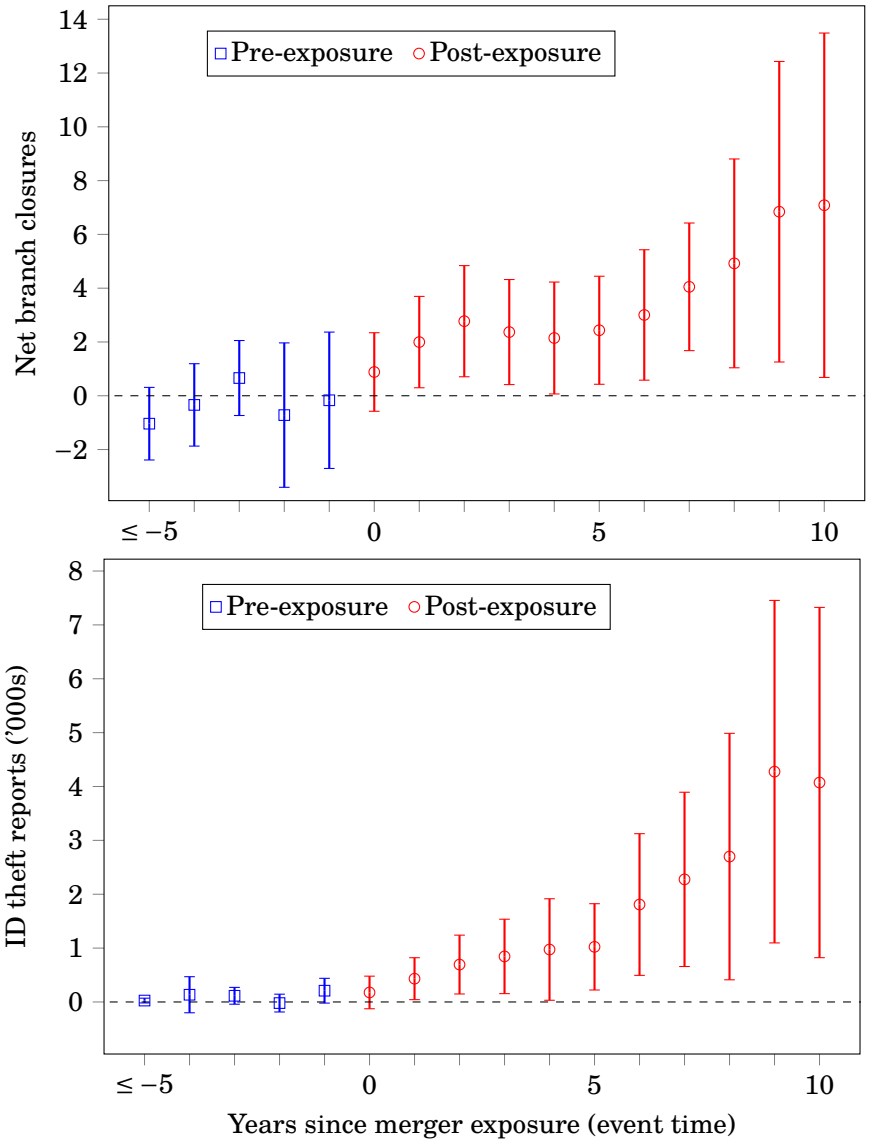
This figure plot the national annual trends of consumer fraud statistics. The volumes (in millions) of identity theft and all other consumer fraud are represented in the stacked barcharts. Reported total losses (in U.S. billion dollars) are plotted as a trend line. Data on consumer fraud are collected from the Consumer Sentinel Network, administered by the U.S. Federal Trade Commission.

Figure 2. Geography of identity theft reports in the U.S.



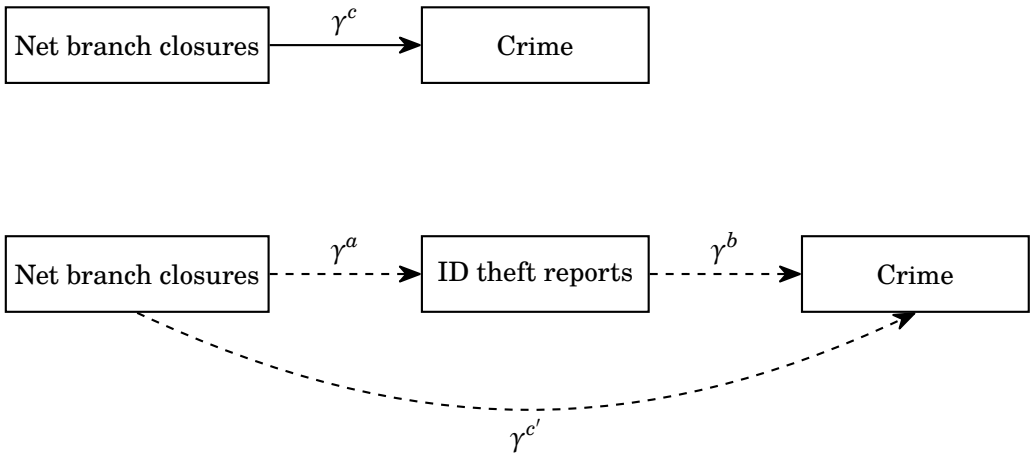
This figure plots the volumes of identity theft reports at the MSA level in the year 2022. Larger circles reflect higher numbers of identity theft reports. Data on identity theft volume are collected from the Consumer Sentinel Network, administered by the U.S. Federal Trade Commission.

Figure 3. Dynamic effects of merger exposures on identity theft



This figure plots the average treatment effects on treated (ATTs) on *net branch closures* and *ID theft reports*, and their respective 95% confidence intervals by event time (years). The MSA-year number of *ID theft reports* is compiled by the Consumer Sentinel Network of the Federal Trade Commission. The variable *net branch closures* is the negative year-on-year change in bank branches within a MSA. ATTs are estimated from the Callaway and Sant'Anna (2021) doubly-robust estimator. A MSA is first exposed in the year when a merger occurs between large banks with branches in the area.

Figure 4. Schematic diagram of the Sobel-Goodman decomposition analysis



This figure presents the schematic diagram of our Sobel-Goodman decomposition analysis. We begin with the total effect γ^c of *net branch closures* on *crime*: Crime $\sim \gamma^c \cdot$ Net branch closures. The variable *crime* is one of the following FBI crime categories: burglary, robbery, larceny, motor vehicle theft, arson, homicide, aggravated assault, rape, and human trafficking. Next, we decompose γ^c into the indirect effect ($\gamma^a\gamma^b$) and its direct effect ($\gamma^{c'}$) by estimating two regressions: (i) ID theft reports $\sim \gamma^a \cdot$ Net branch closures and (ii) Crime $\sim \gamma^b \cdot$ ID theft reports $+ \gamma^{c'} \cdot$ Net branch closures. The proportion of total effect explained by the mediating variable (i.e., *ID theft reports*) is $\gamma^a\gamma^b/\gamma^c$, where $\gamma^c = \gamma^a\gamma^b + \gamma^{c'}$.

Table 1. Descriptive statistics

Panel A: Summary statistics (N = 4,266)

	Mean	S.D.	P10	P50	P90
ID theft reports ($\times 10^3$)	1.42	5.32	0.08	0.28	2.47
Net branch closures	2.9	14.2	−1	1	8
Δ Branch (−)	3.9	12.0	0	1	8
Δ Branch (+)	1.0	7.0	0	0	1
Over 60	18.4	7.1	10.5	17.2	26.8
Male	50.1	1.3	48.6	50.1	51.6
Unemployed	6.6	2.9	3.6	6.0	10.5
White	76.6	13.5	60.0	80.0	90.0
High school	63.4	35.4	9.3	85.7	92.0
Household income ($\times 10^3$)	56.1	13.0	41.8	53.8	72.8
Population ($\times 10^5$)	7.3	15.8	1.2	2.7	15.6

Panel B: Pairwise correlations (% pts.)

		A	B	C	D	E	F	G	H
A	ID theft reports								
B	Net branch closures	57							
C	Over 60	4	10						
D	Male	(9)	(11)	(40)					
E	Unemployed	(5)	(10)	(39)	28				
F	White	(28)	(16)	5	7	(16)			
G	High school	(16)	(11)	(54)	32	33	25		
H	Household income	28	22	29	(21)	(50)	(23)	(40)	
I	Population	76	57	(6)	(2)	(3)	(27)	(1)	31

Panel A reports the summary statistics of the variables used in our main analysis. The MSA-year number of *ID theft reports* is compiled by the Consumer Sentinel Network of the Federal Trade Commission. Branch closures data are collected from the Summary of Deposits files of the Federal Deposit Insurance Corporation. Demographic data are collected from the U.S. Census Bureau. The statistics for the variables *over 60*, *male*, *unemployed*, *white*, and *high school* are reported in percentage points. Panel B reports the Pearson pairwise correlations between the variables used in the main test. Correlations are rounded to their nearest integers and expressed in percentage points. Negative values are contained in parentheses.

Table 2. Elasticity of bank branch visits

Dependent variable: Bank branch visits

	(1)	(2)	(3)	(4)
Distance band	0–1 miles	1–2 miles	2–3 miles	19–20 miles
Net branch closures	14.77	3.29	3.83	0.19
	(2.61)	(1.24)	(1.65)	(0.17)
Over 60	−2.37	−2.40	−2.39	−2.42
	(4.66)	(4.63)	(4.63)	(4.71)
Male	0.13	0.19	0.20	0.20
	(0.17)	(0.24)	(0.26)	(0.26)
Unemployed	0.00	0.00	0.00	0.00
	(6.35)	(6.33)	(6.32)	(6.33)
White	−0.01	−0.01	−0.01	−0.01
	(5.71)	(5.73)	(5.73)	(5.71)
High school	−1.26	−1.20	−1.21	−1.16
	(1.97)	(1.93)	(1.93)	(1.82)
log(Household income)	−97.66	−97.99	−97.91	−98.73
	(6.41)	(6.44)	(6.48)	(6.45)
log(Population)	49.47	48.66	48.60	48.64
	(8.49)	(8.05)	(8.06)	(8.06)
# Obs.	11,676,567	11,676,567	11,676,567	11,676,567
R^2	0.595	0.595	0.595	0.595
County-Week FE	✓	✓	✓	✓
Bank-Week FE	✓	✓	✓	✓
County cluster	✓	✓	✓	✓
Bank cluster	✓	✓	✓	✓
Week cluster	✓	✓	✓	✓
Implied elasticity	18.1%	5.1%	7.8%	0.7%

This table presents estimates from OLS regressions. The dependent variable is *bank branch visits*—the weekly number of visits received by a bank branch, compiled by the `pass_by` database. For every bank branch, we merge in the *net branch closures* of neighboring bank branches that are within the distance band stated in each column. The variable *net branch closures* is the negative change in the number of bank branches over the past 180 days. We calculate the distances separating bank branches using their latitude and longitude coordinates. These coordinates are sourced from the FDIC SOD dataset and through geocoding the `pass_by` branch addresses via the Google Maps geocoding API. t-statistics are reported in parentheses.

Table 3. Bank branch closures and physical store visits

	(1)	(2)	(3)	(4)
Dependent variable	All visits	Retail visits	Online spend gap ($)	Online transaction gap (#)
Net branch closures	−1,661.29	−280.80	1,714.77	24.81
	(5.96)	(3.35)	(5.39)	(5.76)
Over 60	66.25	11.79	144.16	2.23
	(1.33)	(1.00)	(1.08)	(1.15)
Male	18.52	2.48	−230.15	−3.04
	(0.25)	(0.13)	(1.18)	(1.07)
Unemployed	−109.02	−25.31	868.91	10.79
	(1.45)	(1.41)	(4.19)	(3.74)
White	0.22	0.85	−16.87	−0.28
	(0.42)	(5.56)	(7.58)	(8.74)
High school	5.45	−6.16	766.97	11.93
	(0.06)	(0.28)	(3.15)	(3.43)
log(Household income)	−2,278.35	−228.80	8,852.59	93.31
	(1.17)	(0.49)	(1.73)	(1.24)
log(Population)	1,388.33	246.14	−8,602.01	−63.08
	(0.96)	(0.70)	(1.57)	(0.77)
Unit of obs.	Zipcode-Week		Zipcode-Month	
# Obs.	3,188,792		619,727	
R^2	0.950	0.945	0.887	0.890
Zipcode FE	✓		✓	
Week FE	✓			
County-Week FE	✓			
Month FE			✓	
County-Month FE			✓	
Zipcode cluster	✓		✓	

This table presents estimates from OLS regressions. The dependent variables are *all visits*, *retail visits*, *online spend gap*, and *online transaction gap*. The variable *all visits* (*retail visits*) is the weekly number of all (retail) store visits in a zipcode, compiled by the `pass_by` database. A store is in the retail sector if its NAICS code is in 442, 443, 444, 448, 451, 452, or 453 (Chava, Oettl, Singh, and Zeng, 2024). The variable *online spend gap* (*online transaction gap*) is the monthly dollar value (number) of online transactions less that of offline transactions in a zipcode, compiled by the `SafeGraph` database. For every zipcode, we merge in the *net branch closures* of neighboring zipcodes that are within 5 miles but more than 1 mile away. The variable *net branch closures* is the negative change in the number of bank branches over the past 180 days. t-statistics are reported in parentheses.

Table 4. Bank branch closures and identity theft

Panel A. Dependent variable: ID theft reports

	(1)	(2)	(3)
Net branch closures	213.42	87.01	
	(5.91)	(3.23)	
Δ Branch (−)			166.92
			(6.33)
Δ Branch (+)			4.97
			(0.91)
Over 60		−53.35	−64.33
		(1.00)	(1.28)
Male		−136.07	−120.92
		(3.46)	(3.26)
Unemployed		83.78	74.92
		(1.98)	(1.84)
White		−45.01	−42.55
		(1.81)	(1.81)
High school		90.19	83.27
		(2.88)	(2.73)
log(Household income)		168.47	68.41
		(0.15)	(0.06)
log(Population)		1,150.77	1,328.55
		(0.86)	(1.08)
# Obs.	4,266	4,266	4,266
R^2	0.324	0.690	0.709
MSA FE		✓	✓
Year FE		✓	✓
MSA cluster	✓	✓	✓

This table presents estimates from OLS regressions. All variables are constructed at the MSA-year level. The dependent variable is the number of *ID theft reports* at the MSA-year level, compiled by the Consumer Sentinel Network of the Federal Trade Commission. The key independent variable is *net branch closures*, which is the negative year-on-year change in the number of bank branches. The variables Δ *branch* (−)/(+) are the absolute values of *net branch closures* when it is positive and negative, respectively. t-statistics are reported in parentheses.

Table 5. Merger exposures and identity theft

Average treatment effect on treated (ATT)

	(1)	(2)
Outcome:	Net branch closures	ID theft reports
Pre-exposure	−0.76	34.85
	(1.83)	(1.51)
Post-exposure	3.51	608.18
	(3.57)	(2.81)
Overall	2.79	455.56
	(3.27)	(2.72)
Wald estimate	163.28	
MSA cluster	✓	✓

This table presents average treatment effects on treated (ATTs) on *net branch closures* and *ID theft reports* from the Callaway and Sant'Anna (2021) doubly-robust estimator. The variable *net branch closures* is the negative year-on-year change in the number of bank branches within a MSA. The MSA-year number of *ID theft reports* is compiled by the Consumer Sentinel Network of the Federal Trade Commission. The *pre* (*post*)*-exposure averages* are the aggregated ATTs before (after) merger exposures. A MSA is first exposed in the year when a merger occurs between large banks with branches in the area. t-statistics are reported in parentheses.

Table 6. Complier characteristics analysis

Characteristics	Full sample	Compliers	Never-takers	Always-takers
Demographics and ID theft				
ID theft reports ($\times 10^3$)	0.60	0.26	1.37	0.37
Over 60	11.7	11.2	11.0	12.1
Male	50.8	50.5	50.7	50.9
Unemployed	10.2	11.6	9.7	10.1
White	80.2	83.7	78.0	80.3
High school	86.1	84.0	87.0	86.2
Household income ($\times 10^3$)	45.9	46.6	46.9	45.2
Population ($\times 10^5$)	4.15	4.94	6.05	3.04
Num. branches	120.9	119.8	174.0	95.8
Digital adoption (having:)				
Internet subscription	74.7	76.2	76.0	73.6
Any computing devices	85.7	86.1	86.4	85.3
Desktop/laptop	76.6	77.0	77.4	76.1
Smartphone	72.8	72.6	73.8	72.3
Proportion of sample (% pts.)	100	19	26	55

This table shows how mean characteristics of complier MSAs compare to the full sample and non-compliers. Characteristics of compliers and non-compliers are computed using the methodology outlined in Marbach and Hangartner (2020). The demographic and ID theft characteristics are taken as of the year 2010. The digital adoption characteristics are taken as of the year 2015 (earliest year available). We report in percentage points the proportions of the sample made up of compliers, never-takers, and always-takers.

Table 7. Heterogeneous effects of bank branch closures on identity theft

Average treatment effect on treated (ATT)

	(1)	(2)	(3)	(4)
	Net branch closures	ID theft reports	Net branch closures	ID theft reports
Panel A. Bank mergers by branch reliance:				
	High		Low	
Pre-exposure	0.47	64.28	0.42	53.93
	(1.14)	(2.25)	(2.26)	(1.81)
Post-exposure	19.52	4,444.48	1.70	656.88
	(2.76)	(2.58)	(2.05)	(3.03)
Overall	11.67	2,362.36	1.03	440.27
	(2.70)	(2.92)	(1.48)	(3.09)
Wald estimate	202.43		—	
MSA cluster	✓	✓	✓	✓
Panel B. Bank mergers by digital focus:				
	Low		High	
Pre-exposure	0.15	12.15	0.27	5.35
	(0.49)	(1.38)	(1.29)	(0.72)
Post-exposure	3.27	555.73	2.66	119.29
	(2.79)	(2.78)	(1.59)	(1.01)
Overall	1.93	281.70	2.66	229.06
	(2.20)	(2.30)	(1.72)	(1.94)
Wald estimate	145.96		86.11	
MSA cluster	✓	✓	✓	✓

(Continued next page)

Table 7. (continued)

Average treatment effect on treated (ATT)

	(1)	(2)	(3)	(4)
	Net branch closures	ID theft reports	Net branch closures	ID theft reports
Panel C. Bank mergers by consumer tech-savviness:				
	Low		High	
Pre-exposure	0.15	−4.34	0.43	45.67
	(0.37)	(0.97)	(1.55)	(1.50)
Post-exposure	2.47	534.21	5.21	1,120.46
	(2.20)	(2.17)	(3.19)	(2.74)
Overall	1.91	398.31	3.79	668.13
	(2.02)	(2.31)	(2.79)	(2.62)
Wald estimate	208.54		176.29	
MSA cluster	✓	✓	✓	✓

This table presents average treatment effects on treated (ATTs) on *net branch closures* and *ID theft reports* from the Callaway and Sant'Anna (2021) doubly-robust estimator. The variable *net branch closures* is the negative year-on-year change in the number of bank branches within a MSA. The MSA-year number of *ID theft reports* is compiled by the Consumer Sentinel Network of the Federal Trade Commission. The *pre* (*post*)*-exposure averages* are the aggregated ATTs before (after) merger exposures. A MSA is first exposed in the year when a merger occurs between large banks with branches in the area. We classify bank mergers based on the (i) *branch reliance* of the acquirer (Panel A), (ii) *digital focus* of the acquirer (Panel B), and (iii) *consumer tech-savviness* in the exposed MSA (Panel C). The *branch reliance* of a bank is the ratio of its number of branches to its total deposits. The *digital focus* of a bank is the ratio of the download volume of its mobile app on the `Google Play Store` to its number of branches. The *consumer tech-savviness* of an MSA is the proportion of consumers who has an internet subscription. t-statistics are reported in parentheses.

Table 8. Merger exposures and mobile app usage

Average treatment effect on treated (ATT)

	(1)	(2)
Outcome:	Net branch closures	Mobile app usage
Pre-exposure	0.005	0.046
	(1.76)	(0.07)
Post-exposure	0.052	5.337
	(0.99)	(1.71)
Overall	0.072	2.760
	(3.96)	(3.20)
Wald estimate	38.33	
MSA cluster	✓	✓

This table presents average treatment effects on treated (ATTs) on *net branch closures* and *mobile app usage* from the Callaway and Sant'Anna (2021) doubly-robust estimator. The variable *mobile app usage* is the number of hours spent on mobile applications in a month by each Android smartphone consumer in an opted-in panel, compiled by `GWS Magnify`. We determine every consumer's residence by her most-frequented zipcode between 9:00 PM and 6:00 AM (local times) and match it to the county. The variable *net branch closures* is the negative change in the number of bank branches in the month, matched to the consumers' residences at the county level. The *pre* (*post*)*-exposure averages* are the aggregated ATTs before (after) merger exposures. A MSA is first exposed in the year when a merger occurs between large banks with branches in the area. *t*-statistics are reported in parentheses.

Table 9. Military veterans, branch closures, and identity theft

	(1)	(2)	(3)
	OLS	1st stage	2nd stage
Dependent variable:	ID theft reports	Veterans	ID theft reports
v: Veterans	5,089.43		
	(2.13)		
Draft share		481.49	
		(88.24)	
v × Net branch closures	6.07		
	(5.33)		
$\widehat{v}$ × Net branch closures			3.65
			(5.49)
$\widehat{v}$			1,531.35
			(1.12)
Net branch closures	–22.56		17.17
	(0.87)		(0.92)
# Obs.	4,138	4,138	4,138
R^2	0.719	0.845	0.703
F	11.83	1,123.32	11.29
Controls	✓	✓	✓
MSA FE	✓		✓
Year FE	✓	✓	✓
MSA cluster	✓	✓	✓

This table presents estimates from OLS and IV regressions. The variable *veterans* (abbreviated as v) is the number of male veterans aged 55–74 in an MSA. Both *veterans* and its instrumented variant are scaled by a factor of 10^5. The variable *draft share* is the MSA's population share of males who were eight or nine years old during the 1960 census. The variable *net branch closures* is the negative year-on-year change in the number of bank branches. The number of *ID theft reports* is compiled by the Consumer Sentinel Network of the Federal Trade Commission. For brevity, we include but suppress the estimates of control variables (used in Table III) in our models. t-statistics are reported in parentheses.

Table 10. Bank branch closures and unwanted calls

	(1)	(2)	(3)	(4)	(5)	(6)
Dependent variable:	1(Unwanted calls)			Unwanted calls		
Unwanted call type	All	Wireless	Wired	All	Wireless	Wired
Net branch closures	0.121	0.153	0.094	1.509	0.792	0.362
	(2.59)	(2.92)	(1.68)	(2.28)	(1.95)	(1.65)
Marketing calls	3.222	1.348	0.426	–32.798	–17.152	–4.357
	(9.28)	(3.60)	(1.35)	(10.26)	(11.27)	(4.62)
Over 60	–0.587	–0.913	–0.288	–6.584	–4.592	–1.038
	(1.81)	(3.24)	(1.43)	(3.28)	(4.02)	(2.09)
Male	–1.154	–1.020	–0.685	–5.369	–3.118	–1.395
	(4.12)	(4.22)	(4.13)	(3.31)	(3.50)	(3.38)
Unemployed	0.476	0.346	0.242	1.974	0.750	0.473
	(2.11)	(1.76)	(1.79)	(1.75)	(1.12)	(1.67)
White	–0.067	–0.049	–0.033	–0.241	–0.095	–0.049
	(1.93)	(1.61)	(1.59)	(1.29)	(0.94)	(0.94)
High school	0.055	0.053	0.012	0.412	–0.045	0.067
	(1.23)	(1.39)	(0.31)	(1.68)	(0.43)	(0.63)
log(Household income)	14.029	9.547	11.342	88.100	42.194	25.868
	(2.75)	(2.10)	(3.32)	(2.85)	(2.42)	(3.39)
log(Population)	26.327	18.146	8.298	62.158	37.937	7.831
	(3.37)	(2.96)	(2.01)	(1.70)	(2.06)	(0.82)
# Obs.	1,113,936	1,113,936	1,113,936	1,113,936	1,113,936	1,113,936
R^2	0.375	0.350	0.272	0.553	0.489	0.360
MSA FE	✓	✓	✓	✓	✓	✓
Year FE	✓	✓	✓	✓	✓	✓
MSA cluster	✓	✓	✓	✓	✓	✓

This table present estimates from OLS regressions. The dependent variables are 1(*unwanted calls*) and *unwanted calls*. The indicator 1(*unwanted calls*) switches on if there is at least one unwanted call or robocall reported by consumers in a MSA to the FTC on a given day. The variable *unwanted calls* is the number of unwanted calls and robocalls reported by consumers in a MSA to the FTC on a given day. The key independent variable in all columns is *net branch closures*, which is the negative year-on-year change in the number of bank branches in a MSA over the past 180 days. t-statistics are reported in parentheses.

Table 11. Bank branch closures and phishing sites

	(1)	(2)	(3)	(4)
	In-sample		Out-of-sample	
Dependent variable	Phishing exposure	ID theft reports ($\times 10^3$)	Phishing exposure	ID theft reports ($\times 10^3$)
Net branch closures	0.024		0.058	
	(6.09)		(9.08)	
MSA phishing		15.30		4.11
		(2.07)		(3.00)
Over 60		0.21		0.03
		(2.13)		(0.41)
Male		0.05		−0.17
		(0.51)		(1.74)
Unemployed		0.37		0.22
		(2.36)		(1.88)
White		−0.03		0.02
		(1.61)		(1.04)
High school		0.06		0.01
		(2.63)		(0.54)
log(Household income)		−0.95		1.94
		(0.71)		(1.19)
log(Population)		0.02		13.38
		(0.01)		(1.70)
Unit of obs.	Bank-MSA-Month	MSA-Year	Bank-MSA-Month	MSA-Year
Sample period	2018–22	2018–22	2018–19	2020–22
# Obs.	49,888	1,725	12,723	1,063
R^2	0.001	0.834	0.006	0.946
MSA FE		✓		✓
Year FE		✓		✓
MSA cluster		✓		✓

This table presents estimates from OLS regressions. The dependent variable *phishing exposure* in column 1 is the monthly number of websites that use the favicon of the legitimate bank website but lack secure-sockets-layer (SSL) certification, weighted by the population of a MSA where the bank operates. The independent variable is *net branch closures*, which is the negative month-on-month change in the number of bank branches within the MSA. The dependent variable in column 2 is the number of *ID theft reports* compiled by the Consumer Sentinel Network of the Federal Trade Commission. The key independent variable is *MSA phishing*—the weighted sum of predicted *phishing exposure*, aggregated to the MSA-year level. The sum is weighted by the number of branches operated by banks in a given MSA-year. Columns 3 and 4 are the out-of-sample analog of columns 1 and 2. t-statistics are reported in parentheses.

Table 12. Sobel-Goodman decomposition: Bank branch closures, identity theft, and crime

	Crime	γ^a	γ^b	$\gamma^a\gamma^b$ Indirect eff.	$\gamma^{c'}$ Direct eff.	$\gamma^a\gamma^b+\gamma^{c'}$ Total eff.	Indirect/Total (% pts.)	MSA-year mean ($\times 10^3$)
(1)	All crimes	86.85	−1.38	−119.99	−146.34	−266.33	45.05	19.54
		(3.08)	(5.15)	(2.65)	(3.62)	(4.55)		
Crimes related to cash use								
(2)	Burglary	86.85	−0.34	−29.11	−39.77	−68.89	42.26	3.15
		(3.08)	(5.44)	(2.68)	(4.86)	(5.36)		
(3)	Robbery	86.85	−0.11	−9.09	−12.15	−21.24	42.81	0.70
		(3.08)	(4.89)	(2.61)	(4.21)	(3.38)		
(4)	Larceny	86.85	−0.90	−78.40	−72.56	−150.96	51.93	11.98
		(3.08)	(5.35)	(2.67)	(2.85)	(4.36)		
Crimes unrelated to cash use								
(5)	Motor vehicle theft	86.85	−0.02	−1.35	−10.16	−11.50	11.69	1.73
		(3.08)	(0.52)	(0.52)	(2.13)	(2.25)		
(6)	Arson	86.85	0.00	−0.19	−1.01	−1.20	15.79	0.10
		(3.08)	(1.05)	(0.99)	(2.38)	(3.50)		
(7)	Homicide	86.85	0.00	0.09	−0.19	−0.10	−84.62	0.04
		(3.08)	(1.17)	(1.09)	(1.71)	(0.84)		
(8)	Aggravated assault	86.85	−0.03	−2.64	−7.82	−10.45	25.23	1.77
		(3.08)	(0.68)	(0.66)	(2.08)	(2.68)		
(9)	Rape	86.85	0.01	0.79	−2.88	−2.09	−37.92	0.11
		(3.08)	(1.82)	(1.57)	(3.45)	(3.06)		
(10)	Human trafficking	86.85	0.00	0.09	−0.04	0.05	193.62	0.00
		(3.08)	(1.85)	(1.58)	(0.83)	(1.95)		

This table presents results from our Sobel-Goodman decomposition analysis on bank branch closures, identity theft, and crime. Figure 4 contains the schematic diagram of our Sobel-Goodman decomposition analysis. Every numbered row represents a specification with a specific crime type. All specifications include control variables used in Table III and fixed effects at the MSA and year levels. We suppress their estimated coefficients for brevity. Standard errors are clustered at the MSA level. z-statistics are reported in parentheses.

Appendix to:
The Digital Economy and Consumer Fraud

Kenny Phua Chishen Wei Gloria Yang Yu

Abstract

The Appendix contains supplementary information and additional tests for the paper "The Digital Economy and Consumer Fraud". The contents of the Appendix are organized as follows.

Section I Detailed statistics of identity theft reports.

Section II Data contributors of the FTC Consumer Sentinel Network database

Section III Branch closures and CFPB consumer complaints.

I Detailed statistics on identity theft reports

We present detailed statistics on identity theft reports from the Federal Trade Commission (FTC) Consumer Sentinel Network database in 2023. Panel A provides a breakdown of these reports by the types and subtypes of identity theft. Panel B provides a breakdown of these reports by identity theft types and age groups.

- Table I here -

II Data contributors of the FTC Consumer Sentinel Network database

We provide the list of organizations that provide data to the FTC Consumer Sentinel Network database.

- Table II here -

III Branch closures and consumer complaints

Identity theft in financial services is a particularly serious problem. According to the FTC, there were 614,711 reports of identity theft related to credit card and bank fraud in 2022. These reports account for 44.2% of all identity theft cases, marking a 16.8% year-over-year increase. During the same period, there was a decline in most non-financial services fraud such as government benefits fraud, phone & utilities fraud. This contrast may indicate that identity thieves are shifting their focus towards targets in the financial services sector.

Traditionally, physical bank branches offered robust security measures. Consumers could verify transactions in person, reducing the risk of fraud that can occur through remote or digital transactions. Bank branches also deter fraud through surveillance, security guards, and limited business hours. As branches close, inconvenienced consumers may be forced to use less secure financial services such as internet banking, which expose them to data breaches and phishing attacks. Moreover, as economic activities shift online after branch closures (i.e., Section 4), personal identifying information and financial details are often shared

across multiple platforms, further amplifying the risk of identity theft. Therefore, branch closures, along with the rapid digitalization of economic activities, facilitate identity theft in the financial services sector.

To examine the impact of branch closures on potential consumer harm, we turn to the Consumer Complaint Database (CCD) maintained by the Consumer Financial Protection Bureau (CFPB). The CCD complements the FTC dataset in three ways. First, the CCD only covers complaints related to financial services, establishing a more direct connection to consumer harm that is most likely induced by branch closures. Second, the CCD links individual consumer complaints to specific financial institutions. This linkage allows us to assess how branch closures by particular banks may correlate with consumer grievances. Third, many CCD complaints include detailed consumer narratives, allowing us to identify the nature of complaints that arise after branch closures.

We process the CCD data as follows. We start by hand-matching the names of banks on the CCD to their FDIC identifiers. These banks are inherently large because only depository institutions with over $10 billion in assets are subject to CFPB oversight. Altogether, we match 386,549 complaints to 136 banks that operate branches in 2,533 counties. While we observe consumer and bank branch locations by zipcode, we cannot confirm whether a consumer used a specific bank branch in their residential zipcode. Thus, we aggregate at the bank-county-month level consumer complaints and branch closures within the past 180 days.

Our primary hypothesis is that branch closures are followed by a higher incidence of complaints filed by consumers in the area. To test this hypothesis, we estimate equation (I) for county c, bank b, on day d.

$$1(\textit{complaint})_{c,b,d} = \alpha + \beta \cdot \sum_{t=d-180}^{d-1} \textit{net branch closures}_{c,b,t} + \mathbf{X}_{c,d}^{\top}\boldsymbol{\lambda} + \varepsilon_{c,d}\,, \qquad \text{(I)}$$

where the vectors $\mathbf{X}_{c,d}$ and $\boldsymbol{\lambda}$ represent vectors of control variables at the county-year level and their corresponding coefficients, respectively.

- Table III here -

The results in Table III indicate that branch closures are followed by a higher incidence of consumer complaints. Column 1 shows that a branch closure in the county is associated with a 326 bps (t = 9.78) higher probability of complaints

lodged by consumers of the bank in the area. As we have both county and month fixed effects, this finding is not explained by unobserved heterogeneity across counties or variation in complaint incidence across time. Next, we saturate the model with bank-county, county-month, and bank-state-month fixed effects. This stringent specification help us rule out endogeneity concerns related to (i) banks matching to specific geographies and (ii) unobserved heterogeneity in consumers across counties in a given month. With this specification in column 2, we continue to find a significantly positive, albeit smaller, relation between branch closures and incidence of complaints.

To sharpen our analysis, we use a zero-shot-learning model, the `bart-large-mnli` model developed by `Facebook`, to classify the nature of every complaint (**bian2023consumer**). For every complaint narrative, we apply the hypothesis format "I am reporting a case of {label}" with the following labels: "fraud", "harassment", "inaccuracy", and "identity theft". The model then produces a probabilistic score for each label, indicating the likelihood that the complaint matches each category. Then, we assign the label with the highest score to the complaint, thereby classifying the complaints according to their nature.

Having classified complaints that are related to identity theft, we reestimate equation (I). Column 3 shows that when a bank closes a branch in the county, the probability of identity-theft related complaints from its local consumers increases by 34 bps ($t = 3.71$). Applying the more stringent set of fixed effects in column 4, we continue to find a significantly positive relation (+17 bps, $t = 2.00$) between branch closures and identity theft complaints. This estimate is also economically significant, given that the average bank-county-month has a 18.8 bps probability of receiving an identity theft complaint.

Overall, we exploit the CCD to pin down a more direct link between a bank's branch closure and its consumers. Our findings suggest that branch closures are followed by greater consumer harm, especially in the form of exposure to identity theft.

IV Mobile app usage and consumer fraud

As a natural follow-up test, we examine whether greater mobile app usage is associated with more identity theft. To prepare for this test, we aggregate mobile

app usage and branch closures data to the MSA-year level to match the granularity of our identity theft data. We deploy a two-stage methodology in this test. The underpinning idea is that branch closures push consumers to rely more on mobile apps, and this reliance in turn leads to more identity theft. In the first stage, we regress mobile app usage on branch closures in a model saturated with year fixed effects. In the second stage, we regress the number of identity theft reports on the fitted values of mobile app usage.

- Panel B of Table III here -

Column 1 of Panel B shows that a branch closure predicts 80.21 (t = 7.36) minutes more usage of finance and retail mobile apps. Decomposing this effect in columns 2 and 3, we find that a branch closure predicts that consumers in the average MSA spend 21.57 (t = 5.28) and 58.63 (t = 8.30) more minutes on finance and retail mobile apps, respectively. In columns 3 through 6, we find that predicted mobile app usage is associated with a positive and statistically significant increase in identity theft. Notably, we find that on a per-minute-usage basis, the effect of finance mobile apps on identity theft ($+10.48, t = 3.09$) is 2.7 times that of retail mobile apps ($3.86, t = 3.09$). Thus, increased engagement with the digital economy leads to more identity theft, particularly in finance, as sensitive personal data in financial transactions are likely more attractive to adversaries.

Table I. Detailed statistics on identity theft reports

Panel A. Breakdown of identity theft reports by types

Identity theft type	Subtype	Num. reports
Credit card	New accounts	381,122
	Existing accounts	44,855
Loan or lease	Apartment or house rented	13,201
	Auto loan/lease	52,070
	Business/personal loan	81,342
	Federal student loan	6,815
	Non-federal student loan	10,921
	Real estate loan	7,551
Bank account	Debit cards, electronic funds transfer, or ACH	42,148
	Existing accounts	18,723
	New accounts	84,335
Govt. documents or benefits	Driver's license issued/forged	8,977
	Govt. benefits applied for/received	82,419
	Other govt. documents issued/forged	9,096
	Passport issued/forged	1,623
Employment or tax-related	Employment or wage-related	31,207
	Tax	60,970
Phone or utilities	Landline telephone – existing accounts	1,125
	Landline telephone (new accounts)	4,578
	Mobile telephone (existing accounts)	7,853
	Mobile telephone (new accounts)	43,225
	Utilities (existing accounts)	1,896
	Utilities (new accounts)	28,725
Other identity theft	Email or social media	19,534
	Evading the law	5,526
	Insurance	11,402
	Medical services	13,683
	Online shopping or payment account	18,058
	Other	205,505
	Securities accounts	5,513

(Continued next page)

Table I. (continued)

Panel B. Breakdown of identity theft reports by age groups

Age group	< 19	20-29	30-39	40-49	50-59	60-69	70-79	> 80
Identity theft type								
Bank account	1,833	20,558	36,859	28,804	20,589	14,339	7,076	2,132
Credit card	2,501	71,900	122,246	84,604	53,438	27,974	10,899	2,852
Employment or tax-related	13,774	16,826	17,827	13,765	10,869	7,877	3,899	1,261
Govt. documents or benefits	1,989	11,373	21,791	19,095	16,061	9,692	3,274	987
Loan or lease	874	26,152	44,611	30,730	20,437	11,264	4,117	1,069
Other identity theft	2,415	42,673	66,702	45,545	27,768	13,665	5,174	1,417
Phone or utilities	622	13,653	23,066	16,770	11,801	6,974	2,582	650

This table presents detailed statistics on identity theft reports from the Federal Trade Commission (FTC) Consumer Sentinel Network database in 2023. Panel A provides a breakdown of these reports by the types and subtypes of identity theft. Panel B provides a breakdown of these reports by identity theft types and age groups.

Table II. Data contributors to the FTC Consumer Sentinel Network database

AARP Fraud Watch Network
Alaska Attorney General
Apple Inc.
Arvest Bank
AT&T Corporation
Australian Competition and Consumer Commission
Best Buy Co. Inc.
Canada Competition Bureau
Capital One Bank
Colorado Attorney General
Comcast Corporation
Connecticut Department of Consumer Protection
Consumer Financial Protection Bureau
Corporation for National and Community Service
Costco Wholesale Corporation
Craigslist
Cybercrime Support Network
Discover Bank
Dominion Energy
eBay
FedEx
First National Bank of Omaha
Florida Attorney General, Office of Citizen Services
Florida Department of Agriculture and Consumer Services
Grants.gov
Handshake
Hawaii Office of Consumer Protection
Hewlett-Packard
Idaho Attorney General
Indeed
Indiana Attorney General
International Association of Better Business Bureaus
Internet Crime Complaint Center
Iowa Attorney General
Iowa, Clinton County Sheriff's Office
JPMorgan Chase & Co.
LinkedIn
Los Angeles County Department of Consumer Affairs
Louisiana Attorney General
Maine Attorney General
Massachusetts Attorney General
MasterCard International
Michigan Attorney General
Microsoft Corporation Cyber Crime Center
Mississippi Attorney General
MoneyGram International

(Continued next page)

Table II. (Continued)

National Consumers League
National Council on Aging
National Grid
Nebraska Attorney General
Nevada Attorney General
Nevada Department of Business and Industry
New Mexico, Albuquerque
New York State Attorney General
North Carolina Department of Justice
Ohio Attorney General
Ohio, Cuyahoga County Department of Consumer Affairs
Oregon Department of Justice
Pennsylvania Attorney General
PeopleClaim
PepsiCo, Inc.
Petscams.com
PrivacyStar
Prosperity Bank
Publishers Clearing House
Rent Group, Inc.
Sages Theater, Inc.
Scam Advisor
Scam Detector
Society of Citizens Against Relationship Scams
South Carolina Department of Consumer Affairs
Tennessee Division of Consumer Affairs
U.S. Bureau of Prisons
U.S. Citizenship and Immigration Services
U.S. Customs and Border Protection
U.S. Department of Defense
U.S. Department of Education
U.S. Department of Health and Human Services, Office of Inspector General
U.S. Department of Justice, Consumer Protection Branch
U.S. Department of Justice, Disaster Fraud Task Force
U.S. Department of Justice, Elder Fraud Hotline
U.S. Department of Justice, Executive Office for Immigration Review
U.S. Department of Justice, Task Force on Market Integrity and Consumer Fraud
U.S. Department of the Treasury, Internal Revenue Service
U.S. Department of Veterans Affairs
U.S. Drug Enforcement Administration
U.S. Federal Bureau of Investigation
U.S. Federal Communications Commission
U.S. Marshals Service
U.S. Parole Commission
U.S. Patent and Trademark Office
U.S. Postal Inspection Service
U.S. Social Security Administration

(Continued next page

Table II. (Continued)

United Parcel Service
USA.gov
Utilities United Against Scams
Valve Corporation
Verizon Wireless
Walmart Corporation
Washington State Attorney General
Western Union Company
Wisconsin Department of Agriculture, Trade and Consumer Protection
Xerox Corporation
Zelle
Zillow Group

This table contains the list of data contributors to the Federal Trade Commission (FTC) Consumer Sentinel Network database.

Table III. Bank branch closures and consumer complaints

Dependent variable ($\times 10^2$): 1(Complaint)

	(1)	(2)	(3)	(4)
Type of complaint	Any	Any	ID theft	ID theft
Net branch closures	3.26	0.23	0.34	0.17
	(9.78)	(2.88)	(3.71)	(2.00)
Over 60	0.19		0.00	
	(5.99)		(0.30)	
Male	−0.06		−0.03	
	(2.54)		(4.13)	
Unemployed	0.26		0.00	
	(4.60)		(0.48)	
White	−0.16		−0.01	
	(9.75)		(8.09)	
High school	0.07		0.01	
	(2.80)		(3.83)	
log(Household income)	7.36		−0.18	
	(8.12)		(2.33)	
log(Population)	4.90		0.12	
	(28.07)		(6.47)	
# Obs.	1,374,000	1,374,000	1,374,000	1,374,000
R^2	0.115	0.597	0.011	0.251
County FE	✓		✓	
Month FE	✓		✓	
Bank-County FE		✓		✓
County-Month FE		✓		✓
Bank-State-Month FE		✓		✓
County cluster	✓	✓	✓	✓
Bank-Month cluster		✓		✓

This table presents estimates from OLS regressions. The dependent variable is 1(*complaint*), an indicator that switches on if a bank receives a CFPB complaint in a county-month. In columns 3 and 4, we employ zero-shot learning techniques to identify CFPB complaints that are related to identity theft. Specifically, we use the `bart-large-mnli` model (Yin, Hay, and Roth, 2019) to detect contextual mentions of identity theft. The key independent variable is *net branch closures*, which is the negative change in the number of bank branches over the past 180 days in the county. t-statistics are reported in parentheses.

Table III. (continued)

Panel B. Mobile app usage and identity theft

	(1)	(2)	(3)	(4)	(5)	(6)
	App duration					
Dependent variable:	Finance & Retail	Finance	Retail	ID theft reports		
Net branch closures	80.21	21.57	58.63			
	(7.36)	(5.28)	(8.30)			
App duration						
Finance & Retail$^{(pred)}$				2.82		
				(3.09)		
Finance$^{(pred)}$					10.48	
					(3.09)	
Retail$^{(pred)}$						3.86
						(3.09)
County controls				✓	✓	✓
# Obs.	1,341	1,341	1,341	1,337	1,337	1,337
R^2	0.314	0.339	0.303	0.590	0.590	0.590
Year FE	✓	✓	✓	✓	✓	✓
Year cluster	✓	✓	✓	✓	✓	✓

This table presents estimates from OLS regressions. The dependent variables are *app duration* and *ID theft reports*. The variable *app duration* is the number of minutes spent on mobile applications in a month by each Android smartphone consumer in an opted-in panel, compiled by `GWS Magnify`. We further classify mobile applications as "finance" or "retail" (shopping) oriented. The number of *ID theft reports* is compiled by the Consumer Sentinel Network of the Federal Trade Commission. The key independent variable is *net branch closures*. The residence zipcode of a consumer is her most-frequented zipcode between 9.00 pm and 6.00 am in the sample. The variable *net branch closures* is the negative change in the number of bank branches over the past 180 days, matched to the consumers' residences at the county level. For brevity, we suppress the estimates of county-level control variables (used in Table III) in our models. t-statistics are reported in parentheses.