Market Pressure or Regulatory Pressure? U.S. Small Bank Pre-emptive IT investment to privacy regulations[1]

Jin Huang, Xiangyu Lin, Xiaomeng Shi, S. Sarah Zhang[2]

This version: Sep 2024

Abstract

We assess how banks react to announcements of privacy protection regulation proposals. Employing a Difference-in-Differences framework, we uncover the proactive actions taken by U.S. small banks in anticipation of these proposals. Our findings reveal that the announcement of privacy protection regulation proposals leads to a 27.49% increase in IT investment by U.S. small banks. Market and regulatory pressure are how proposals influence bank IT investment. Particularly, the evidence of market pressure lies in banks with greater competitive pressure from their rivals, particularly motivated to enhance their IT investments. However, our research also finds that this surge in IT investment does not immediately translate into benefits for small banks.

JEL Classification: G21, G28, G31

Keywords: Regulation proposals; Data privacy; IT investment; small banks; Cybersecurity risk

[1] We thank Prof. Francesco Vallascas, Prof. Sergey Tsyplakov, Dr. Conghui Hu, Dr. Rouzhi Wang, Dr. Liyu Yang and Seminar participants for the helpful discussion in the European Financial Management Association (EFMA), Spring serum of 2024 China Banking & Corporate Finance Conference (CBCF), and Jinan University. We thank Yibing Wang (Kings College London) for detailed discussion on the proposal. All errors are ours.

[2] School of Intelligent Finance and Business, Xi'an Jiaotong-Liverpool University, China, Jin.Huang02@xjtlu.edu.cn (J. Huang);
Alliance Manchester Business School, University of Manchester, UK, xiangyu.lin@postgrad.manchester.ac.uk (X. Lin);
International Business School Suzhou, Xi'an Jiaotong-Liverpool University, China, Xiaomeng.Shi@xjtlu.edu.cn (X. Shi);
Alliance Manchester Business School, University of Manchester, UK, sarah.zhang@manchester.ac.uk (S. S. Zhang);

1. Introduction

With the progression of technology and the evolution of the internet, an increasing number of individuals are opting to entrust their data to cloud services. However, heightened consumer apprehensions regarding data sharing and privacy infringement have brought the risk of data breaches and network security to the forefront of both public and regulatory attention. (Chen et al., 2023). In response, various countries have introduced policies and legislation concerning data privacy and security to safeguard the data privacy of consumers and individuals. For instance, the European Convention on Human Rights, established in 1950, upholds the right of every individual to privacy, family life, and correspondence. Building upon this foundation, the General Data Protection Regulation (GDPR) enacted by the EU was officially enforced by the European Parliament in 2016, taking effect on May 25, 2018. Among the 194 countries worldwide, 137 have implemented legislation to ensure the protection of data and privacy.[3]

Starting in 2018, U.S. states have been proposing and implementing multiple legislations dedicated to safeguarding the personal rights of state residents. A notable example is the California Consumer Privacy Act (CCPA), affording consumers active control over the utilization of their personal information by companies. The CCPA outlines stringent regulations for companies to ensure the security and integrity of collected data. Additionally, it introduces new rights for California residents, encompassing the ability to request access to and deletion of personal information and the option to opt out of the sale of personal information to third parties. As of 2022, 39 states have put forth proposals and laws about privacy. Non-compliance with these regulations may lead to substantial financial penalties and legal repercussions.

To adhere to these privacy laws proposals and announcements, particularly within specific sectors like banking, the anticipatory reinforcement of data privacy measures, access controls, and monitoring becomes imperative. This frequently entails the modernization of systems and substantial investments in software and IT infrastructure, encompassing network upgrades and information systems

[3] Worldwide data protection related privacy legislation among 194 countries can be seen from here: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

enhancements to fortify defenses against security incidents. Additionally, increased investment in data management and processing systems is deemed essential.

This paper focuses on analyzing the pipeline impact of the Privacy Protection Act proposals on the IT investment of small banks in the United States. The study focuses on such banks, as due to limited resources, the burden of regulatory compliance for small banks could be disproportionate to the size and impact small banks' operational activities more significantly. According the industrial news, after the initiative of CCPA, the first privacy protection regulation in California, many smaller enterprises have encountered significant challenges in meeting compliance costs. Specifically, these smaller firms are predisposed to bear a disproportionately higher share of compliance expenditures relative to their larger counterparts. [4] Additionally, the very professional congress report focusing on small and small banks' difficulties in complianting with Data Privacy, and Cybersecurity Regulation points out that, Some banks, particularly small banks and small credit unions, may find it difficult to comply with regulatory standards due to lack of resources.[5] Since the majority of small banks are not exempted from privacy protection proposals, we thereby narrow our focus on the small banks' responses to such proposals.

On the other hand, we focus on proposals on account of two aspects. Firstly, existing research confirms the anticipatory effects of regulatory proposals on targeted businesses. For instance, Chang et al. (2023) demonstrate that firms with higher exposure to impending regulations exhibit heightened concerns regarding future political risks. This increased apprehension often leads these firms to augment their overhead costs in preparation for potential regulatory changes. On the other hand, among all first proposed regulation in each state, only three have been settled and have or will com into enforcement, while the others are vastly in procedure. Therefore, we explore the proactive effect of these proposals.

Our study utilizes a sample of U.S. small banks with assets below $10 billion spanning from 2010 to 2022, encompassing a total of 7,603 banks. The findings indicate a significant increase in IT investment among small banks in the United States following the announcement of the Privacy

[4] See https://shuftipro.com/blog/initial-ccpa-compliance-costs-could-hit-55-billion-report/
[5] See https://crsreports.congress.gov/product/pdf/R/R47434/2

Protection Act proposals. In terms of scale, the introduction of the Privacy Protection Act often prompts banks to respond to anticipated policy implementation, leading to a substantial 27.49% increase in IT investment in the subsequent year. Furthermore, employing event study results allows for a dynamic examination of the long-term effects of privacy protection acts on IT investments. On average, small banks respond instantly to the proposal announcements by increasing IT investment as the preparation, and such responses will last for approximately three years. These results withstand various robustness tests, including examinations on sub-samples, normalized IT investment, and causality. In our mechanism analyses, we suggest that market pressure instead of regulatory pressure is the mechanism through which proposals influence bank IT investment.

Our contributions are threefold. Firstly, we contribute to law and finance literature by extending the understanding of how early-stage regulation proposals, as opposed to finalized regulations, impact financial institutions. The current literature predominantly focuses on the aftermath of enacted regulations, limited studies account for the substantial adjustments made by relevant parties years before the regulations are formally finalized (Chang et al., 2023). Studies have documented that even before these regulatory changes are finalized and promulgated, the high cost associated with regulatory exposure prompts firms to strive to maintain a leading position in anticipation of future regulatory developments (Bessembinder et al., 2018; Hendricks et al., 2023; Trebbi & Xiao, 2019; Chang et al., 2023). As the likelihood of proposed rules becoming formal regulations increases, firms may face more significant impacts, especially when these changes are both imminent and profound, prompting them to take immediate action (Chang et al., 2023). Our research complements existing literature on the implementation of final regulations by suggesting that regulation proposals have a pipeline effect on exposed banks as well and reveals the pre-emptive actions that banks take in anticipation of these changes.

Second, we contribute to the increasing scholarly focus on organizations' RegTech by offering empirical evidence of how small banks respond to impending regulatory changes with strategic IT investments. RegTech, an abbreviation for Regulatory Technology, involves the utilization of technology to aid financial institutions in meeting regulatory compliance requirements (Charoenwong et al.,2024). Financial institutions increasingly rely on IT to ensure compliance with reporting, capital,

consumer protection, and risk management regulations (Deloitte, 2023). Focusing on the pre-implementation phase of the Privacy Act, we highlight the pre-emptive technological measures banks employ to meet anticipated compliance requirements. This insight enriches the understanding of technology's role in regulatory adherence within the financial sector. Concurrently, we focus on the general adoption of information technology rather than specific technologies (such as ATMs, E-payment, or Robo-advising) as discussed in previous studies (Hannan and McDowell, 1984; Crouzet et al., 2023; Lewellen and Williams, 2021). This approach allows us to better understand the evolving nature of financial intermediaries as they increase their technological investments.

Last but not least, via detailed mechanisms, we relate to the literature on factors influencing bank IT investment by illustrating the underlying motivations driving banks to increase their IT investments (Chai et al., 2011; Hernando & Nieto, 2007; Yannelis & Zhang, 2021; Bofondi & Lotti, 2006; Modi et al., 2022). We show that banks' decisions to invest in IT are driven by market pressures. Specifically, We argue market pressures stemming from competition compel banks to make IT investments following the proposal of privacy regulations.

The subsequent sections of this paper are organized as follows: Section 2 provides the background of Privacy legislation proposals and outlines our hypotheses. Section 3 introduces the data and research methods. The main empirical results are presented in Section 4. In Section 5 we delve into the mechanism analysis. Section 6 investigates the tangible impact of IT investments on bank performance. Finally, Section 7 concludes the paper.

2. Related literature and hypothesis development

2.1 What is the Privacy Regulation? The California Consumer Privacy Act and other regulation proposals

The California voters approved the California Consumer Privacy Act (CCPA) of 2018 to empower consumers with greater control over the collection and exchange of their personal information.[6] The

[6] See https://cppa.ca.gov/regulations/pdf/cppa_act.pdf for more details.

regulation was first introduced in January and signed into law six months later in 2018. The state's regulation is a set of rules declaring businesses' duties when they collect personal information and granting customers rights to know their active controls and options for the businesses making use of personal information.

The CCPA mandates that businesses must inform customers before or at the time of collecting personal information about the types, the purpose, and whether it is sold or shared of the information collected. Such collections must be reasonably necessary and proportionate to achieve the purpose, and additional agreements shall be made if the collected information is traded to a third party, declaring the sale purpose and the third party's obligations when using the information. Besides, CCPA imposes strict rules on how firms should help to ensure security and integrity after the data collection, referring to the firm's ability to detect security incidents, requiring the firm's ability to protect their customers' data information. Firms will receive punishment for security incidents under this set of rules. CCPA came into effect on the first day of the year 2020.

Besides the requirements for more transparent and in-time disclosures to customers, customers themselves have more rights to protect their privacy after the CCPA comes into enforcement. Among all granted rights, customers now could choose to limit, or even opt out of the usage, share, and sale of personal information autonomously. Consumers are entitled to statutory damages and the right to take legal action if a company fails to establish and maintain reasonable security measures and practices, leading to unauthorized exposure. This applies when the company fails to establish and uphold reasonable security measures and practices. In compliance with offering required extra service, sector-specific industries, banks, in particular, must update their system to handle customers' multiple choice and inquiries commonly. Businesses are required to present consumer data in an accessible format when responding to data requests, which could necessitate investment in hardware and IT infrastructure. Due to the fast pace of technological progress, it's essential for businesses to continuously update and enhance their IT systems.

The CCPA differentiates from the Gramm-Leach-Bliley Act (GLBA) enacted in 1999. Firstly, while the federal law of GLBA mandates financial institutions to provide customers with privacy notices explaining the information-sharing activities and to implement information protection, this

represents only part of the act's purpose. The GLBA also removes legal barriers for Bank Holding Companies (BHCs), allowing them to convert into Financial holding companies (FHCs) as well, where BHCs could engage in a broader range of activities than before.[7] In contrast, the CCPA focuses solely on customer information protection only applied to firms in all industries that serve the local citizens.[8] Secondly, the CCPA set more stringent regulatory requirements on data sharing transparency and protection than the GLBA. While the GLBA requires financial institutions to explain their information-sharing practices, the CCPA grants more autonomous rights to consumers. These rights include access to the personal information a business collects and the right to request the deletion of their personal information. Additionally, violations of the GLBA can result in criminal charges, whereas CCPA violations can lead to consumer lawsuits, potentially damaging a firm's reputation.[9]

CCPA's approval kicks off over all states issuing and voting for privacy protection proposals. By the end of 2022, there are already 39 states that have released privacy protection regulations proposals.[10] Table 1 presents proposed state privacy protection regulation proposals by 2022. Accordingly, states keep issuing proposals addressing various aspects of data breach issues and privacy protection work. For instance, the New York state proposed the S224 bill in January 2019, known as the "Shield Act", enhancing data security requirements restricting the disclosure of personal information by businesses, and expanding data breach notification requirements. The bill was signed into law in the same year. The act significantly strengthens the state's data security by requiring companies' mandatory development and implementation of safeguard instruments to protect private information. As new laws are being proposed and existing ones are being amended, the landscape of privacy regulation in the U.S. is continually evolving. Even though most proposals have not been signed into regulations by the state's government, with the kick-offs of privacy regulations enforced in other states, banks may begin to prepare for the anticipated regulatory requirements, impacting their strategies and operations consequently. Approximately two-thirds of the initial 39 proposals in each state establish compliance

[7] Sec. 102 in GLBA. See https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf for more information.
8 FHCs could engage in a wider range of financial activities, such as insurance, Merchant banking activities, etc.
[9] Sec. 1798.150. in CCPA.
[10] See https://iapp.org for more details.

thresholds that banks must meet, based either on having gross revenues above a certain threshold or on sharing a specific amount of customer information.[11]

[Insert Table 1 here]

2.2 Hypothesis Development

There are already studies that confirm the anticipatory effect of regulation proposals on targeted businesses. By deriving a firm-level exposure to the regulation pipeline, Chang et al. (2023) find that firms with greater exposure express more concerns about future political risk, increasing their overhead costs to prepare for potential regulation changes. Hendricks et al. (2023) confirm the regulation proposals' anticipatory effect in the banking industry as well. In response to the proposed changes in Basel III, banks implemented strategic changes in financial reporting and modified their business models to minimize their vulnerability to the proposed rule before regulators finalized the regulation. Both highlight the interplay between targeted firms and the proposed regulations. Hence, there is no basis to believe that the privacy legislations in our study, which encompass all proposals for privacy protection regulation, are exceptions to these typical regulatory proposals.

The recent wave of privacy legislation necessitates banks to significantly enhance their customer data protection capabilities. Laws like the California Consumer Privacy Act (CCPA) mandate businesses, including banks, to safeguard the security and integrity of customer data. Following Sarathy and Robertson (2003), we classified The compliance costs associated with privacy legislations into following key components: 1) The costs of granting access to data collected on each customer, 2) The costs of providing notice of privacy policies, 3) The costs of obtaining individual consent, 4) The costs of creating greater transparency, and 5) The costs of granting customers choices, such as the ability to opt out or opt in to the database.

[11] Regulatory proposals generally include exemptions from compliance, and this is also true for the state's privacy protection proposals. We conducted a preliminary review of small banks' compliance with these proposals. On average, over 50% of small banks with available call report information meet the gross revenue threshold and would thus be subject to such regulations if the proposals are finalized. Since we do not have access to the number of customers whose information has been shared, the actual number of small banks meeting the compliance standards could be higher than our initial statistics suggest. Additionally, since the proposals are currently only at the announcement stage, smaller banks that exceed the compliance requirements might be concerned about the final version and could take preemptive actions in response. This addresses coverage concerns of regulation proposals on small banks.

1) The costs of granting access to data collected on each customer

Privacy regulations typically specify that customers can make requests to access the personal data that a company has collected about them. Implementing or upgrading technology to manage data access requests efficiently can be costly. Banks may need to invest in new software or systems to handle these requests. For example, in response to the CCPA, a community bank in California has created a CCPA request form that allows customers to request access to their data[12].

2) The costs of providing notice of privacy policies

Banks are required to provide privacy notices to their customers to inform them about how their personal data is being collected, used, shared, and protected. These notices are a crucial part of compliance with various data privacy regulations. Most banks have a dedicated privacy policy page on their websites. This page typically contains detailed information about the bank's data privacy practices. For example, following the implementation of the CCPA, many small banks have created dedicated pages for CCPA disclosures, requests, and rights for their stakeholders.[13] According to Chander et al (2021), the cost of annual privacy notice for GLBA alone is about $9 million per financial institution.

3) The costs of obtaining individual consent

Banks and other businesses are required to obtain individual consent for certain data processing activities under privacy regulations, particularly when it involves the sale of personal information. To comply with these requirements, banks must update their systems to provide customers with an intuitive interface that facilitates the consent process. The House of Representatives' Committee on Commerce estimated that the cost of compliance with the Children's Online Privacy Protection Rule (COPPA) for obtaining consent ranges from $35,000 to $60,000 per year per person. This estimate includes costs for personnel overseeing offline consent processes, responding to inquiries, reviewing phone consents, and managing permission forms on the website.

4) The costs of creating greater transparency

[12] The following link shows a CCPA request form.
https://forms.office.com/Pages/ResponsePage.aspx?id=rYchVW_dF0G40S9CZ0buzSGCxQmj24hFk5Wj-dkP0-FUNTZCT0RSRTJOWVJBNURIMTJETlBBN0hNNy4u

[13] https://www.ovcb.com/california-privacy/

While all the aforementioned points contribute to greater transparency, an important addition is the requirement for data breach notification. The frequency of data breaches is higher than anticipated, and under privacy protection regulations, banks are required to report these incidents to customers and regulators. A survey by the Ponemon Institute[14] revealed that data breaches are widespread among the companies surveyed: 'About half of the respondents experienced GDPR data breaches that had to be reported to regulators.'

5) The costs of granting customers choices

Most privacy proposals aim to grant customers the right to opt out of personal information sharing and sales while also protecting personal privacy in this process. Banks need to update their internal systems to strictly differentiate between customers who choose to opt-out and those who join in information sharing. Banks must also be prepared to handle customer requests because according to the CCPA they can change their preference at any time. These seemingly straightforward tasks not only require technological updates but also necessitate repeated testing of the system's compliance and security to prevent any accidents.

The compliance costs arising from these five categories can be substantial, and all are directly related to IT expenses. To enable these options safely, banks must upgrade their network and information systems to detect and counter security incidents, malicious activities, and illegal actions. Failure to do so can lead to security incidents that trigger speculation and result in penalties. Consequently, banks are motivated to make substantial additional investments in IT to strengthen data privacy, access control, and monitoring systems.

Large banks, due to their advantages in resource access, have initiated IT investment for decades and should be well-prepared for technology issues, while small banks' IT development is relatively backward. The privacy proposals and regulations commonly do not exempt specific firms or financial institutions, requiring small banks to improve data security systems as well.[15] Such small banks thereby

[14] Ponemon Institute, Keeping Pace in the GDPR Race: A Global View of GDPR Progress in the United States, Europe, China and Japan 2 (2019).
[15] The CCPA allows the exemption for certain categories of data that have been regulated by prior Gramm-Leach-Bliley Act announced in 1999.

may face more regulatory challenges. Following the above facts, we raise out baseline hypothesis as follows:

H1: Privacy Legislation proposals have a positive anticipatory effect on small banks' IT investment.

The competition in the banking industry has intensified recently, particularly with the rise of FinTech lenders. These FinTech companies, leveraging their technological innovations, have captured a significant market share, thereby shrinking the space for traditional banks in both the mortgage market (Fuster et al., 2019) and payment services (Parlour et al., 2022). In this competitive landscape, regulatory proposals serve as indicators of increasing customer awareness regarding privacy concerns. Privacy protection has therefore emerged as a new battleground in the banking industry. Banks that demonstrate a strong commitment to compliance can enhance customer trust and loyalty, which is vital for retaining existing clients and attracting new ones. By prioritizing privacy and data security, these banks can differentiate themselves from competitors, potentially gaining a competitive edge in the market and motivating them to invest in IT. In an analysis of the implications of the GDPR for U.S. firms, Voss and Houser (2019) suggests that U.S. companies can leverage their compliance with the GDPR and by actively complying with privacy regulations and publicly promoting these measures, these companies can gain a distinct competitive advantage based on trust, setting themselves apart from firms that only minimally comply with the law. Such a competitive advantage is essential for sustaining a business in highly competitive markets.

Non-compliance with privacy regulations can result in significant fines, legal penalties and loss of reputation, further diminishing a bank's ability to compete effectively. Banks cannot afford to lose market shares and bear such financial and reputational risks in highly competitive markets. Therefore, the effect of privacy regulation on IT investment is expected to be particularly pronounced in environments characterized by heightened competitive pressures.

H2: Privacy legislation proposals have a stronger effect on small banks facing more competition from rivals.

Banks may need to adhere to regulatory proposals due to heightened regulatory scrutiny. Empirical studies find that intensive supervision from regulators ensures banks' compliance (Delis and Staikouras, 2011). This is because greater regulatory intensity entails more rigorous oversight, such as frequent inspections and more information advantage in monitoring. For example, insights acquired by supervisors during supervisory actions such as enforcement actions and examinations enable them to implement appropriate corrective measures for imprudent banks, thereby ensuring regulatory compliance. Banks, facing increased scrutiny, are at a greater risk of being detected for any non-compliance by regulatiors, whether it's intentional or unintentional. Besides, even though privacy protection regulations are proposed by the state government, small banks' regulation violations and corresponding punishment, which increases the bank's regulation compliance risk, are very likely to trigger the bank's federal regulator's attention. Therefore, banks may have to allocate additional resources to compliance efforts in response to increased regulatory pressure. Therefore, we propose the following hypothesis:

H3: Privacy legislation proposals have a stronger effect on small banks with high regulatory intensity.

3. Data and Methodology

3.1 Sample Selection

To study the impact of the privacy protection regulation proposals on IT investments among U.S. small banks, we obtained our sample of the U.S. commercial banks and branches of separate RSSD ID with assets less than $10 billion from 2010 to 2022 from the Bank regulatory Database. The financial data and indicators are collected from Bank regulatory and FDIC, along with state-level demographic data from the Census.

Consumer privacy legislation is proposed to strengthen the privacy of consumers' data protection. Since 2018, various states in the United States have introduced privacy protection bills, underscoring the increased importance of consumer personal data protection in the banking sector. We collect consumer privacy bills issued by different states in the United States since 2018 from the International Association of Privacy Professionals (IAPP).

In our empirical analysis, we divided small banks into two groups – a treatment group and a control group – to assess the impact of consumer privacy legislation on commercial banks' IT investment. We employed location information data obtained from the Compustat database to ascertain the impact of the state's consumer privacy legislation on the commercial bank. The banks located in states that have proposed or enacted consumer privacy legislation are our treatment group, and the banks in the states that have not proposed or enacted consumer privacy legislation are our control group. Our focus is on the small commercial bank's location rather than that of the parent BHC. The majority of small banks with assets less than $10 billion are small banks that typically operate within certain regional areas to serve local customers and communities. The sample selection of small banks is based on the Dodd-Frank Act stress tests (DFAST)[16] and Bord et al. (2021). We limited banks to BHC-affiliated commercial banks with assets of less than $10 billion. Our final sample included 70,979 bank-year observations across 7,603 banks, of which 4,121 commercial banks are headquartered in the treated states and 3,482 firms in the control states.

To measure banks' IT investments and expenditures, we utilized a database constructed by Modi et al. (2022) from regulatory filings, rather than relying on Aberdeen data inferred from survey waves, to circumvent the inaccuracies and lack of transparency often found in marketing survey data. Modi et al. (2022) point out that the market survey data, such as Aberdeen data, could be plagued by errors and opaque imputations, while information directly from the regulatory filings is likely to be of much higher quality due to the legal obligation and resources involved in these filings.

The small banks' IT investment proxy, built upon the work of Kovner et al. (2014), involves text analysis of public regulatory filings (Call Reports) from U.S. banks, offering a new approach to

[16] The Dodd-Frank Act stress tests (DFAST) are required for any bank with more than $10 billion in assets, but these are bank-run tests that are reviewed by the Federal Reserve, rather than Federal Reserve –implemented tests.

measuring bank IT spending. Information extracted from regulatory filings is likely of higher quality due to the legal obligations and scrutiny involved. Bank data and IT expenses reported in the Call Reports—quarterly regulatory filings to the FDIC—do not specifically require banks to report IT investments or expenses. Hence, Modi et al. (2022) used text analysis to reclassify expense descriptions containing any IT-related keywords like "software" "computer" or "internet" as "IT expenses" This method offers a more comprehensive understanding of the growth in technological investments across financial intermediaries, beyond focusing on specific technological applications, which could lead to narrower and more subjective evaluations (Modi et al., 2022).

3.2 Empirical Methods

To test the impact of the Privacy Protection Act on the IT investment of banks, we mainly estimate the following Difference in Differences model, as shown in equation (1):

$$IT\_Invest_{i,s,t+1} = \alpha + \beta PrivacyAct_{i,t,s} + \gamma Control_{i,t,s} + \varphi_i + \omega_t + \tau_s + \epsilon_{i,t,s} \quad (1)$$

where *i*, *t*, and *s* represent firms, states, and years, respectively. The main independent variable, $PrivacyAct_{i,t,s}$ is a binary variable that equals one if the state has proposed privacy legislation in the current or previous years, and zero otherwise. The dependent variable IT_Invest denotes the IT investment and expenditure of small banks one year after the announcement of privacy protection regulation proposals. We measure all dependent variables at t +1 to mitigate reverse causality, and there is inevitably a lag because banks' responses to policy implementation are often not timely. We will check the dynamic effects between announcements and IT investments at different times in section 4.3. At the same time, *Controls* in Model (1) include various bank characteristics and local demographics following the prior studies' framework focusing on the bank-level regulatory intervention outcomes (e.g., Hirtle et al., 2020; Srivastav & Vallascas, 2022). We incorporate bank size, profitability (using ROA as a metric), loan ratio, deposit ratio, and leverage to account for bank-specific characteristics. We also control for the state's demographics, including bank HHI, population, unemployment rate, and economic policy uncertainty that might influence the state's decision on whether to propose privacy protection regulations. Definitions for all control variables are displayed in Table A1.

The baseline model includes year-fixed effects ω_t and bank-fixed effect φ_i to control for time-invariant omitted bank characteristics and time-specific factors. In addition, we also control state-fixed effect τ_s, because firms can relocate their headquarters to other states (Goetz et al., 2013). The standard errors are clustered at the bank level.

4. Empirical Results

4.1 Summary Statistics

Table 2 provides descriptive statistics for the variables used in our analyses. We winsorize all continuous variables at the 1st and 99th percentiles to mitigate the effects of potential outliers. Our sample contains a total of 70,758 firm-year observations, of which approximately 80% of the bank-year observations have an IT spending value of 0. The mean value of the Privacy Protection Act is 0.118, indicating that 11.8% of the overall bank-year observations are located in the state with the enactment of a serious Privacy Protection Act. Banks in our sample have an average total asset of 0.2 billion, with an average ROA of 0.9%, a Loan ratio of 61.7%, and a deposit ratio of 68.5%. Statistics are consistent with prior studies focusing on small banks' issues.

[Insert Table 2 about here]

4.2 Baseline Result

To test the impact of consumer privacy legislation on bank IT investment, we use the Difference-in-Differences model in Equation (1) to examine. Coefficient β denotes the difference in IT investment in commercial banks before and after the proposals of the consumer privacy legislation, relative to the control group.

[Insert Table 3 about here]

Table 3 Panel A reports the baseline regression estimates of the privacy protection regulation proposals on banks' IT investment. We first analyze the sample of all U.S. bank holding companies, with the primary results shown in columns (1) to (3). These columns provide estimates of IT investment

based on different combinations of control variables and fixed effects for the full sample. Column (1) includes firm, state, and year-fixed effects, but excludes any control variables. The coefficient indicates that the introduction of consumer privacy proposals led to a 71.392 increase in IT investment for the experimental group of commercial banks compared to the control group. This change represents a 37.4% increase relative to the average IT investment of 190.788. In columns (2) and (3), we add firm-level control variables and macroeconomic control variables commonly used in prior studies of bank IT investment: ROA, Loan_ratio, Ln(asset), Deposit_ratio, Leverage, as well as HHI, population, unemployment rate, and EPU (Hirtle et al., 2020; Srivastav and Vallascas, 2022). Across all models, the Privacy Act displays a consistently significant positive coefficient, suggesting that the privacy protection proposals had a positive impact on banks' IT investment. After adding the control variables in columns (2) and (3), the economic and statistical significance of the coefficients remains robust. In column (2), we include firm and year fixed effects, while in column (3), we further add state fixed effects. Specifically, the results in column (3) show that IT investment increased significantly by 34.00%, relative to the sample mean of 190.788.

Next, we focus on small banks for several reasons: (1) large banks typically operate across state lines, making it difficult to assess the spillover effects of state-level privacy protection laws on branches in other states; (2) small banks face a disproportionately higher compliance cost relative to large banks following the introduction of new regulations; (3) small banks often face unique challenges due to regulatory changes and frequently address these issues on their websites, demonstrating a higher level of concern compared to larger banks; and (4) limitations in the dataset.

Therefore, we shift our focus to small banks, with the results presented in columns (4) to (6) of Table 3. Columns (4)-(6) present the estimates for IT investment based on the full sample with a combination of control variables and fixed effects, respectively. Column (4) contains firm, state, and year-fixed effects, but does not include any control variables, the coefficient shows that the introduction of the consumer privacy proposals led to a rise in IT investment in commercial banks in the experimental group compared to the control group by 60.672. This change is an increase of 31.8 %

when compared to the average IT investment of 190.788.[17] The economic significance and statistical significance of the individual coefficients of the proposal remain after adding control variables in Columns (5)-(6). In Column (5) we add bank and year-fixed effects, and in Column (6) further add state-fixed effects. Specifically, the results in Column (3) show a significant 27.49% increase in investment relative to the average IT investment sample mean of 190.788.

At the same time, we want to explore the long-term effect of consumer privacy proposals on commercial bank IT investment. In Panel B, we present the effects of consumer privacy proposals on commercial bank IT investment in the current year, the next year, the year after the next, and the year after the next two years. Consistent with Panel A, we first focus on all U.S. bank holding companies (Columns (1)-(3)). Then, we shift our attention to the more affected small banks (Columns (4)-(6)).

As mentioned above, commercial banks' reaction to consumer privacy proposals is not immediate and needs time to manifest and process. In Columns (1) and (4) of Panel B, the introduction of the consumer privacy proposal boosts all banks' and small banks' IT investment in the current year by 17.8% and 16.8%, respectively which is significant at the 5% level.

Columns (2) –(3) and Columns (5) – (6) of Panel B show the impact of the consumer privacy proposal on banks over the next two and three years, and we find that the impact effect is statistically decreasing from year to year. When banks start to update their technology adoption, initially, this includes significant investments and expenses to upgrade networks and information systems to detect and address security incidents, malicious activities, and illegal actions. Once the initial system upgrades and implementations are completed, subsequent investments such as staff training, system maintenance, and software upgrades continue over time. However, these costs, although recurring, are not captured under IT investments in accounting measures (Modi et al., 2022). This distinction reflects the shift from capital expenditures to operational expenditures, with the latter often having less visibility in financial reporting compared to the more substantial initial investments.

[17] (60.672/190.788) = 31.8 %.

4.3 Robustness

After the baseline specifications, we conduct various additional tests to validate the evidence. Including: (i) Exclude all observations from the five states that successfully enacted privacy legislation (Table A2); (ii) Include a sample of large banks or exclude tiny banks (Table A3); (iii) Exclude observations for the Covid period 2020-2022 (Table A4) and, (iv) address the potential influence of overall fintech development; (ii) address the potential influence of IT investment zero inflation issues.

Firstly, In 2023, California, Virginia, Colorado, Connecticut, and Utah formally implemented laws related to privacy and data protection. Given the significant impact of successful privacy legislation on banks, and to demonstrate the pre-implementation effect of such laws on bank IT investment, we aim to mitigate potential concerns by providing alternative evidence.[18] We excluded all observations from the five states that successfully enacted privacy legislation, retaining 83% of the sample, as shown in Columns (1) and (2) of Table A2. The findings remain robust and significant, indicating that proposals for privacy protection legislation increase the emphasis and investment in IT across banks.

[Insert Table A2 about here]

To compare IT investments across banks better, we also normalize the value by dividing them by the bank's non-interest expenses and report the result in Column (3) of Table A2 in the Appendix. The pattern in the baseline is consistent across the normalization method.

Secondly, privacy regulations have set forth requirements for businesses. For instance, the CCPA proposal in 2018[19] stipulated that the regulations would apply to businesses meeting at least one of the following conditions: (A) annual gross revenues over 25 million dollars ($25,000,000); (B) possession of the personal information of 50,000 or more consumers, households, or devices; or (C) earning more than half of its annual revenue from selling consumers' personal information. However, there were discrepancies between the proposal and the actual legislation. By the time of its implementation in 2020,

[18] California's California Consumer Privacy Act (CCPA) became effective on January 1, 2020.California Privacy Rights Act (CPRA) and Virginia's Consumer Data Protection Act (CDPA) became effective on January 1, 2023. Colorado's Colorado Privacy Act (CPA) and Connecticut's privacy legislation took effect on July 1, 2023. Utah's Utah Consumer Privacy Act (UCPA) became effective on December 31, 2023.

[19] See https://www.gibsondunn.com/wp-content/uploads/2018/07/california-consumer-privacy-act-of-2018.pdf for more details.

[20] the criteria for businesses under point B were revised to (B) Alone or in combination, annually buying, selling, or sharing the personal information of 100,000 or more consumers or households. Consequently, banks that were included under the business scope in the proposal phase of the privacy bill, as well as those initially excluded, had incentives to adopt and enhance hardware infrastructure to address potential security challenges and possible penalties. To demonstrate the actual impact of privacy legislation on bank IT investments, we have utilized alternative evidence to mitigate concerns arising from the business conditions.

[Insert Table A3 about here]

We include big banks and small banks but exclude tiny banks in column (1), only small banks and very small banks in column (2), and we limited our analysis to banks that made IT investments during our sample period (2010-2022).[21] The results, consistent with the baseline findings, indicate that the proposal of the Privacy Protection Act has effectively prompted banks to enhance their investments in software and hardware through its regulations and requirements.

Thirdly, with COVID-19 and the social distancing requirements, people increasingly relied on digital solutions for financial transactions and managing finances. This greatly accelerated the development of financial technology and online banking (Fu and Mishra, 2022). Considering the potentially significant impact of the pandemic on banks' IT systems, to demonstrate the actual influence of privacy legislation on banks' IT investments, we employed alternative evidence to alleviate potential concerns. In column (1) of Table A4, we exclude observations after COVID-19 and its aftermath; in column (2), we retained observations from the period 2015 to 2020, a time when advancements in artificial intelligence and machine learning offered development opportunities for financial institutions. This approach allows us to measure the real impact of privacy legislation more accurately on banks' IT investments. In Columns (3) and (4), we exclude samples in 2020 where most states enacted the stay-at-home policies which were released in early 2021. We check the contemporaneous effect in Column (3) and the lagged effect in Column (4).

[20] See https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 for more details.
[21] In our paper, we define "tiny banks" as those whose total assets are in the lowest 10% of all U.S. commercial banks in our sample.

[Insert Table A4 here]

In addition, Some may argue that the small banks' IT investment decisions follow the overall trend of technology enhancement and the threat from Fintech lenders rather than respond to the regulation proposal. If it were true, small banks headquartered in less Fintech access states would increase less in such expenses due to limited threat from rivals and there would be no significant investment anomalies in banks across states. To test whether it is such a case, we employ the state's internet access ratio as the proxy for access to Fintech lenders report the regression result in Column (1) –(2) of Table A5, and replace the IT investment with the investment anomaly based on the median of IT investment for all banks in our sample within each year

[Insert Table A5 here]

Results in Table A4 and A5 are consistent with baseline findings, indicating that privacy protection legislation has led to increased IT investments by banks, and has alleviated concerns regarding IT investments related to the rapid development of artificial intelligence and fintech, as well as the rapid growth of online banking during the COVID-19.

Last but not least, to address the potential influence of IT investment zero inflation issues, we introduced robustness checks in our regression due to the variance of the dependent variable (2050.409) being substantially higher than its mean (190.788). Following Li et al.(2017), we employed both the Poisson model and the zero-inflated Poisson (ZIP) regression model, given that the frequency of count=0 accounts for approximately 80% of the sample.

Specifically, the first stage (zero-inflation stage) fits whether the count variable is zero. In this stage, we used Non-interest expense as an instrumental variable to model whether the dependent variable takes a zero value since IT investment is measured based on whether it ranks among the top three non-interest incomes. The second stage involves fitting the Poisson distribution model, where we used the Vuong option. The Vuong test compares the fit of the ZIP model to the ordinary Poisson regression (Vuong, 1989), with a Z-test result of 165.78, indicating the superiority of the ZIP model.

[Insert Table A6 here]

The ordinary Poisson regression result is shown in column (1) of Table A6, which indicates that for each unit increase in the proposal of the Privacy Act, there is a 0.158 unit increase in the log of bank

IT investments for the following year. Columns (2) and (3) display the results of the zero-inflated Poisson regression. In Column (2), the inflation coefficient for Non-interest expense suggests that each unit increase in non-interest income reduces the log odds of zero inflation by 0.00. In Column (3), the coefficient for the Privacy Act indicates that for each increase in the proposal, the log of bank IT investments for the following year increases by 0.144 units. We additionally narrow samples to those firms which ever have IT investment across the window which shown in column (4). This aims to eliminate the bias from firms never investing in IT. The result is robust and the effect is stronger based on the larger regression coefficient.

In summary, we consistently find evidence that BHC commercial banks that are hit by the consumer privacy legislation increase their IT-related investments compared to BHC commercial banks that are not affected by the consumer privacy legislation.

4.4 Dynamic DID Model

We extend our analysis by examining the dynamic impact of consumer privacy legislation proposals. Specifically, we employ robust estimators introduced by dynamic models to replicate our results, addressing concerns about the reliability of the OLS model (Borusyak et al., 2021; Callaway & Sant'Anna, 2021; Sun & Abraham, 2021). Given the different years in which privacy protection law policies were proposed or enacted, the event study method considers that observed covariates satisfy the parallel trends assumption (Baker et al., 2022).

$$IT\_Invest_{i,s,t} = \alpha + \sum_{k=-5}^{k=3} \delta_k \times D_{i,t,s}^{k} + \gamma Control_{i,t,s} + \varphi_i + \omega_t + \tau_s + \epsilon_{i,t,s} \qquad (2)$$

where dummy variable $D_{i,t,s}^{k}$ capture periods preceding and following the proposal event, and δ_k is the parameter of interest in the event study analysis. More specifically, we decompose the periods before and after the event into nine bins: (i) If the state where a commercial bank is located proposes privacy protection proposals in the fifth, fourth, third, second, or first year after this year, the indicators are equal to 1 (*period=-5*, *-4*, *-3*, *-2*, *-1*); (ii) if the state proposes or enacts privacy protection legislation in the current year, the indicator is equal to 1 (*period=0*); (iii) if the state proposed or enacted privacy

protection legislation 1 year, 2 years, or 3 years ago, the indicators are equal to 1 (*period=1*, *2*, *3*). By replacing the test variable *PrivacyAct* with this set of binary variables $D_{i,t,s}^{k}$, we re-estimate the regression in Equation (2).[22]

[Insert Figure 1 about here]

Figure 1 presents the results of the event study, covering event study plots constructed using four different estimators: Borusyak et al. (2021) (orange circle markers); the dynamic version of the TWFE model with OLS estimation (purple with triangle markers); Sun & Abraham (2021) (blue diamond markers) and Callaway & Sant'Anna (2021) (red cross markers). Results from the event study constructed with these four different estimators all indicate estimates consistent with the parallel trends assumption. Regardless of the chosen estimator, coefficients for the pre-introduction five years of the privacy protection legislation remain close to zero, suggesting no significant differences in IT investments between the treatment and control groups before the proposal of privacy protection legislation.

At the same time, our dynamic model further confirms that the impact of privacy protection proposals is not immediate. Similar to the findings of Hendricks et al. (2022), where U.S. banks were not required to implement Basel III until several years after the proposal was introduced, most of the substantial effects of the privacy protection proposals only became evident several years after their enactment. The post-first to third periods provide dynamic observations of the treatment effect, with all robust estimators revealing a gradual increase in the treatment effect on IT investments after the introduction of privacy protection laws.

[22] In TWFE model and Callaway and Sant'Anna (2022) method, we included all control variables consistent with baseline model. Due to model setup, we did not include control variables in Borusyak et al. (2021) and Sun and Abraham (2021) methods, but we control all the bank, year and state fixed effects.

4.5 Falsification Tests

We implement two falsification tests to validate further the causal interpretation of our baseline results that address the concern that our results may be driven by other omitted shocks that overlap with the privacy protection regulation proposals.

[Insert Figure 2 about here]

We first generate experimental groups randomly and implement 500 runs of placebo tests based on whether the state has announced a proposal already (Dang et al., 2021). In each of the 500 times iterations, we keep the actual year of the event while assigning the treatment to prior control groups. We re-estimate the equation (1) with new random treatment group samples, get a new coefficient for each iteration, and graph the distribution of estimated coefficients in Figure 2. The assumption is that, if the effect in the baseline is driven by other factors rather than privacy legislation, there would be no significant difference between the estimated coefficients in the placebo tests and the result in the baseline. As shown in Figure 2, the placebo coefficients are distributed centrally around zero, which is far away from the true estimated value.[23] This validates the causal effect of privacy legislation on small banks that anticipated more IT investment.

[Insert Table 4 about here]

Additionally, we implement a time falsification test as well to validate the causal interpretation of the baseline results. We put the year when the state announced the first privacy protection proposals 4 years back and re-estimate the equation (1) with the placebo test. As the treatment time is false now, we should not observe an increased IT investment after the announcement of proposals in placebo times. As in Table 4, the results show that the treatment effect is not significant for any specifications in the three columns, representing the dynamic responses. Conclusively, both falsification tests support the causal effect in our baseline.

[23] We did not draw the line for true estimated value in the graph, as the coefficient 52.448 is located outside the range of the graph.

4.6 Regulation Proposal Counts

According to statistics in Table 1, over half of the states have announced multiple proposals. The number of these proposals represents the potential diversity of regulatory burdens for banks. We therefore examine whether the count of proposals contributes to increased IT investment.

We employ five additional proxies to quantify the regulation proposals for each state. These include counting the number of proposals announced in the current year, creating a dummy variable to indicate whether a state announced a proposal in the current year, cumulating the total number of proposals up to the present, and adopting two status proxies to measure the proposal status. All definitions are detailed in the Appendix A1.

As Table 5 illustrates, we find that in addition to the introduction of the first privacy protection regulation, the number of proposals also impacts the magnitude of small banks' IT investment. Small banks increase their IT investment in response to a greater number of proposal announcements in the previous year (Column (1)) and more cumulative proposals up to the last year (Column (3)). Furthermore, a state's announcement of a proposal in the previous year alone can trigger investment (Column (2)). According to Column (4), proposals at different stages have varying impacts on the banks' responses. On average, enacted regulations have a stronger impact than mere proposal announcements and voting approval.

[Insert Table 5 about here]

4.7 Proposal heterogeneity

Even though all first announced proposal(s) is (are) addressing privacy protection in each corresponding state, there are still heterogeneities in specific requirements or limitations across different proposals. One of the most significant divergencies among the series of proposals is about the explicitly granted customer's lawsuit against data breach incident, which is also the primary improvement compared to the 1998 Gramm-Leach-Bliley Act. We go through the proposals again and find that, according to statistics, 17 out of the 39 states' first privacy protections explicitly grant customers the right to file lawsuits directly against financial institutions for violations of the Act while the others do not. We

therefore test the heterogeneity of the response to different proposal requirements based on whether customer lawsuit right is granted.

As shown in Table A7, we split samples based on whether the state announced a proposal that explicitly grants customer lawsuit rights against institutions that break the regulation. Column (1) comprises observations that grant such right while Column (2) includes the left samples. Accordingly, even though the effect of the proposal announcement we find in the baseline is marginally significant among the first group of samples, the economic magnitude among the two sub-groups is not significantly different. Therefore, even though the requirements vary among each state's specific proposals in terms of customer rights, banks respond consistently to the privacy protection proposal announcement.

5. Mechanisms

5.1 Market Pressure

We posit that the underlying mechanism is as follows: banks facing intense market competition are likely to increase their investments in IT to maintain a competitive edge following the introduction of privacy protection laws. In contrast, when market competition is less intense, banks may lack the incentive to adjust their investments in response to regulatory changes. To validate our second hypothesis, we consider several variables capturing this dimensional change. We utilize two company-level market competitiveness measures based on text analysis: a product similarity measure (Hoberg & Phillips, 2016) and a product liquidity measure (Hoberg et al., 2014). The former gauges the extent to which a company's products and services have substitutes in the market, while the latter measures the frequency of new products and services appearing in the market. They employ text analysis of product descriptions in company 10-K filings to determine a more flexible TNIC classification as a substitute for the traditional SIC industry classification, capturing the competitive pressure from existing and potential rivals. Since FinTechs offer similar products and services to traditional banks, the market

competitiveness indicator provided by Hoberg and Phillips also captures competition from FinTechs according to the new industry classification.

[Insert Table 6 about here]

We conducted subsample tests. As shown in Columns (1) and (2) of Table 6, in comparison to samples where market competition is less intense, banks in markets with a higher frequency of new products and services, and thus higher pre-existing competition threats, doubled their IT investments on average after the introduction of consumer privacy legislation compared to the control group. This indicates that banks with greater pre-existing competition threats in their product markets are more motivated to adjust their IT investments in response to the introduction of privacy protection laws.

In Columns (3) and (4), we further divide banks into two samples based on the level of product similarity. We find that banks with high product similarity, indicating a higher likelihood of facing competition-induced pressure, significantly increased their IT investments after the introduction of privacy protection laws compared to the control group. However, banks with low product similarity did not make targeted adjustments in IT investments after the introduction of privacy protection laws.

In summary, businesses, especially banks, facing competition pressures higher than the median are more likely to significantly enhance their IT investments. This finding aligns with our predictions.

5.2 Regulatory Pressure

To measure regulatory intensity, we employ the driving distance (in kilometers) between the bank's headquarters and its primary regulators, namely the OCC, FDIC, and Fed. This variable is from Google API and intended to capture the costs associated with regulatory enforcement and the averse of local information advantage in monitoring. The rationale behind this variable is that regulatory oversight activities at the bank level are closely linked to interactions with their primary regulators. Therefore, we posit that the cost of enforcement increases as the distance from the primary regulator grows. Proximity to the primary regulator reduces costs for regulators in their regular interactions with banks, thus influencing the regulatory intensity. Additionally, local regulators, compared to distant ones, possess an advantage in information gathering during supervision. Several studies consistently

demonstrate that geographical proximity to the primary regulator influences banks' decisions in response to banking regulation (Berninger et al., 2018; Lim & Armitage, 2016).

Based on the above discussion, we anticipate observing increased levels of bank IT investment after the proposal announcement when the distance between the bank's headquarters and its primary regulators is closer. Distance is measured by the driving time between the bank's headquarters and its primary regulator. As shown in Table 7, we categorize distance into two subgroups. Column (1) displays the results for distances above the sample median, where the coefficient of PrivacyAct is not significant. In Column (2), the results for distances below the sample median show a positive and statistically significant coefficient of PrivacyAct at the 5% level. We then examine the specific heterogeneity among each regulation agency. Columns (3) and (4) focus on banks supervised by the FDIC. Only the results for distances below the sample median to the FDIC show positive and statistically significant coefficients. Similarly, Columns (5) and (6) concentrate on banks supervised by the FED, where only the results for distances below the sample median to the FED exhibit positive and statistically significant coefficients. Turning to Columns (7) and (8) for the OCC, unlike the FDIC and Fed, the results for distances above the sample median to the OCC are positive and statistically significant.

[Insert Table 7 about here]

Meanwhile, it is observed that the coefficient comparison tests for most of the groups do not reject the hypothesis that the two regression coefficients in each pair are equal. This indicates that the heterogeneity in responses arising from passive regulation compliance is not significant. Therefore, small banks increase IT investment in response to privacy regulation proposals, as they are likely more concerned about falling behind their competitors than merely complying passively.

6. Further analysis effect of IT Investment

6.1 Exposure to Cyberattack Risks and Cyber Attack Prevention

We further investigated the impact of cyberattacks on the customer data protection channel. First, We examine whether exposure to cyberattack risks influences bank IT investment following the proposal

of privacy legislation. Next, we explored whether substantial IT investments lead to tangible scale effects and benefits in terms of enhanced cybersecurity.

In the face of heightened cybersecurity risks, managers are motivated to invest in IT to safeguard their organizations, particularly in response to privacy legislation proposals. This is because the formal enactment of privacy laws holds banks accountable for any failure to protect customer privacy resulting from cyberattacks. We hypothesize that the anticipatory impact of privacy legislation proposals will be more pronounced for banks with greater exposure to cybersecurity risks.

To gauge cybersecurity risk exposure, we utilize a cybersecurity risk exposure index developed by Florackis et al. (2022), which measures a bank's vulnerability to cyberattack events. Banks are classified into high or low cybersecurity risk exposure groups based on whether their cybersecurity risk exposure index exceeds or falls below the sample yearly median value. The estimation results in Table 8 columns (1) and (2), indicate a positive and significant coefficient for the high cybersecurity risk exposure group. Overall, these findings support the notion that privacy legislation proposals influence bank IT investment through the channel of cybersecurity risk exposure.

[Insert Table 8 about here]

Afterward, we explore whether the increased IT investment will help prevent cyber attacks on small banks. Small banks increase IT investment to ensure compliance with potential regulations about private data protection while successful cyber attacks would result in data breaches. Therefore, we explore small banks' IT investment aiming to stop data breach incidents work efficiently. To ascertain this, we develop the following regression model (4):

$$Cyber\ Attack_{i,s,t} = \alpha + \beta IT\_Invest_{i,s,t} + \gamma Control_{i,t,s} + \varphi_i + \omega_t + \tau_s + \epsilon_{i,t,s} \quad (4)$$

where the variable $Cyber\ Attack_{i,s,t}$ represents the number of successful cyber attacks experienced by bank *i* in year *t*. To control for time-invariant factors, we include the same control variables as in the baseline model along with fixed effects for banks, years, and states.

Given that the count of cyber attack events is non-negative integers, we employ Poisson regression to study the potential impacts of successful cyber attacks. This model's regression coefficientsβ directly interpret the logarithmic impact of IT investment and enhanced security measures on the rate of cyber

attack incidents, providing intuitive and specific results. Concurrently, we also construct an Ordinary Least Squares (OLS) regression.

[Insert Table 9 about here]

The results, displayed in Table 9, indicate no significant statistical difference in coefficients, whether using Poisson or OLS regression. In models (1) and (3), lagged one-year IT investments serve as independent variables; in model (2), the variable is the total IT investment over the past two years. The primary dependent variable is the number of successful cyber attacks each bank experiences annually.

The Poisson regression results are shown in columns (1) and (2) of Table 9 indicating that banks with higher IT investments did not experience more cyberattacks. Neither prior year nor cumulative IT investments significantly alter the incidence of cyber-attacks. The OLS results in column (3) also indicate that increases in IT investments do not escalate cyber security incidents. These findings imply that although small banks have increased their IT investments to counter potential cyber threats, such investments have neither significantly reduced the frequency of cyber attacks nor data breaches. However, they have not exacerbated the situation either. This stability suggests that while the investments maintain security conditions, only certain types of IT investments may be sufficient to enhance defenses and reduce incident rates. This may indicate a need for more precise and effective IT security strategies in small banks to effectively counter increasingly complex cyber threats.

6.2 Proactive effect of IT investment

Thus far, our empirical analysis suggests that privacy legislation encourages small banks' IT investment. An intuitive follow-up question is whether their IT investment could influence the bank's competitiveness, efficiency, and asset quality. Evaluating the impact of innovation requires understanding how the economic fundamentals of a company or its industry evolve. It is crucial to navigate the extensive journey from concept through implementation to actual profitability (David et al., 2018). Next, we conduct additional analyses to evaluate how the small banks' IT investment affects

their performances and check if the influence is consistent with prior evidence that exists in large banks. To ascertain this, we develop the following regression model (3):

$$Perf_{i,s,t} = \alpha + \beta IT\_Invest_{i,s,t} + \gamma Control_{i,t,s} + \varphi_i + \omega_t + \tau_s + \epsilon_{i,t,s} \quad (3)$$

where $Perf_{i,s,t}$ denotes groups of proxies representing small banks' characteristics for bank i headquartered in states in the year t. We also include the same control variables as the baseline and a matrix of bank, year, and state fixed effects to control for these time-invariant factors. The coefficient of paramount interest is β.

We first examine whether small banks' IT investment increases their profitability and competitiveness, to assess the relationship between technological input and economic benefits (West et al., 2014). As we have confirmed that the impact of privacy legislation is more pronounced in more profitable banks and banks facing more intense competition, we examine whether IT investment can sustain profitability and establish competitive advantages for small banks. We adopt ROE as the measure of profitability (Pennacchi & Santos, 2018) and the bank's market share, which denotes the ratio of the bank's total deposits over the sum of all banks' deposits in each state. [24] As Teece (1986) and Helfat and Raubitschek (2018) argue, innovative firms often fail to reap significant economic returns from their innovations, while customers, imitators, and other industry participants benefit. Consequently, the consumer rights protected by privacy laws ensure that consumers ultimately benefit from banks' investments in IT. Small banks will be disappointed to see that, as shown in Panel A of Table 9, increased IT investment will reduce banks' ROE while making an insignificant contribution to increasing the bank's market share. It is assumed that the increased expenses may decrease the net income, reducing the bank's profitability consequently. At the same time, according to the results in Column (2) of Panel A, small banks' IT investment could not be converted into simultaneous competitiveness, as the coefficient for IT investment is not pronounced. This aligns with the notion that the relationship between the depth of innovation and innovation performance often follows an inverted U-shape, where the positive effects in the short term may not be observable (Kobarg et al., 2019).

[Insert Table 9 about here]

[24] The result is consistent for ROA.

Some may thereby raise the argument that the decreased profitability is only the result of increased expense; on the other side, such expenses may lead to enhanced operational efficiency rather than short-term net income, which will contribute to the bank's performance as well. To address such an argument, we examine whether small banks' IT investment impacts the bank's operational efficiency. Besides following the definitions of Interest expense and Noninterest expense in Evanoff & Ors (2008) and Casu et al. (2013), we also construct the proxy of non-interest expense to Total revenues to measure how much of a bank's revenue is consumed by operating expenses that are not related to interest, aiming to investigate to which extent the IT investment could improve the operational efficiency. The lower the ratio is, the more operationally efficient the bank will be.

Columns (1) and (2) in Panel B of Table 9 disassembles different expenses, and Column (3) displays the efficiency test result. The findings indicate that increased IT investment in small banks does not significantly raise their interest expenses on deposits, nor does it lead to a substantial increase in noninterest expenses relative to total assets. However, it is noteworthy that more IT investment reduces efficiency marginally. In conclusion, the empirical results presented in Panel B reveal that small banks' IT investment seems to diminish overall operational efficiency.

Lastly, we examine if small banks' IT investment will improve the bank's capital structure and asset quality. We use proxies of Tier 1 and Tier 2 capital and total capital to total assets, respectively, to measure banks' capital structure., and Non-Performing Loan (NPL) to evaluate the asset quality. The result in Column (2), Panel C of Table 9 shows a negative impact of small banks' IT investment on capital structure, while the insignificant coefficient of IT investment in Column (3) shows that such investment is not related to banks' asset quality.

7. Conclusion

This study examines the small banks' anticipatory response, the IT investment specifically, to the state's privacy legislation in the U.S. We exploit the dynamic effect of privacy legislation and the factors driving small banks' such responses and investment decisions. We find that U.S. small banks, on

average, increased IT investment by 27.5% in the year following the announcement of the privacy regulation proposals. The anticipatory response starts from the coinstantaneous time, boosting small banks' IT investment by 16.8%, and lasts to the end of the second year following the announcement. We strengthen the evidence for the causal effect of privacy legislation on small banks' IT investments through robustness checks, employing staggered Difference-in-Difference regression models, and conducting space and time placebo tests.

In addition to examining banks' anticipatory responses to proposed privacy regulations, we explore factors that explain the heterogeneity in banks' reactions. Through mechanism analysis, we find that banks with higher local market competitiveness, and stricter regulatory oversight are more likely to increase IT investment following the announcement of privacy regulation proposals. The increased IT investment in response to the announcement among banks facing more competitive pressures indicates their anticipation of the benefits of IT investment and the potential negative impacts of security incidents. Furthermore, we observe a more pronounced response in banks headquartered closer to their regulators, suggesting a local informational advantage in bank monitoring.

While the small banks respond to proposals anticipated, the increased IT investment would not bring economic benefits directly. Banks headquartered in states without prior successful cyberattacks against small banks, or appraised as having higher cybersecurity risk exposures, are inclined to invest more in IT as a response to privacy legislation. This suggests these banks believe that IT investment will bolster their protection against security incidents. Increased IT investment, on the contrary, will decrease the bank's profitability, reduce operational efficiency, and make the capital structure worse than before. Additionally, more IT investment could not increase the market share or improve the asset quality. Therefore, the increased IT investment in response to the privacy regulation proposals functions as defensive initiatives rather than measures to seek more profits, as failing to comply with the regulation may bring a severe negative impact on small banks.

Overall, our results are the first to document the small banks' anticipatory responses to the ongoing privacy protection campaign. The main innovation is to focus on the small banks' pre-cautionary actions, why such actions occur, and the consequences of these responsive actions. Our study holds significant practical implications. Banks should strategically assess their IT investment responses to privacy

legislation, evaluating the broader impact of these investments on their financial health and operational efficiency. This insight is valuable for policymakers, prompting a re-evaluation of the regulatory burdens on small banks compared to their larger counterparts and the advantages that FinTech lenders hold in compliance. We also highlight the nature of increased IT investment in these institutions, which seems to serve more as a defensive strategy rather than yielding substantial benefits. Future research could delve further into the more efficient responses of small banks to privacy legislation and investigate the broader consequences of their IT investments.

Reference

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks in the financial sector. *SSRN Electronic Journal*.

Baker, A. C., Larcker, D. F., & Wang, C. C. Y. (2022). How much should we trust staggered difference-in-differences estimates? *Journal of Financial Economics*, *144*(2), 370–395.

Berninger, M., Kiesel, F., & Schiereck, D. (2018). When your regulator becomes your new neighbor: Bank regulation and the relocation of EBA and EMA. *Economics Letters*, *167*, 108–111.

Bessembinder, H., Jacobsen, S., Maxwell, W., & Venkataraman, K. (2018). Capital Commitment and Illiquidity in Corporate Bonds. *The Journal of Finance*, *73*(4), 1615–1661.

Bofondi, M., & Lotti, F. (2006). Innovation in the Retail Banking Industry: The Diffusion of Credit Scoring. *Review of Industrial Organization*, *28*(4), 343–358.

Bord, V. M., Ivashina, V., & Taliaferro, R. D. (2021). Large banks and small firm lending. *Journal of Financial Intermediation*, 48, 100924.

Borusyak, K., Jaravel, X., & Spiess, J. (2021). Revisiting event study designs: Robust and efficient estimation. *arXiv preprint arXiv:2108.12419*.

Callaway, B., & Sant'Anna, P. H. C. (2021). Difference-in-Differences with multiple periods. *Journal of Econometrics*, *225*(2), 200–230.

Casu, B., Clare, A., Sarkisyan, A., & Thomas, S. (2013). Securitization and Bank Performance. *Journal of Money, Credit and Banking*, *45*(8), 1617–1658.

Chai, S., Kim, M. and Rao, H.R., 2011. Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, *50*(4), pp.651-661.

Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D. and Yu, I., 2021. Achieving privacy: Costs of compliance and enforcement of Data Protection Regulation. *Policy Research Working Paper*, 9594.

Chang, S., Kalmenovitz, J., & Lopez-Lira, A. (2023). Follow the Pipeline: Anticipatory Effects of Proposed Regulations. *SSRN Electronic Journal*.

Charoenwong, B., Kowaleski, Z.T., Kwan, A. and Sutherland, A.G., 2024. RegTech: Technology-driven compliance and its effects on profitability, operations, and market structure. *Journal of Financial Economics*, 154, p.103792.

Chen, S., Doerr, S., Frost, J., Gambacorta, L., & Shin, H. S. (2023). The fintech gender gap. *Journal of Financial Intermediation*, *54*, 101026.

Crouzet, N., Gupta, A. and Mezzanotti, F., 2023. Shocks and technology adoption: Evidence from electronic payment systems. *Journal of Political Economy*, *131*(11), pp.3003-3065.

Dahlander, L., Gann, D.M. and Wallin, M.W., (2021). How open is innovation? A retrospective and ideas forward. *Research Policy*.

Dang, V. A., De Cesari, A., & Phan, H. V. (2021). Employment protection and share repurchases: Evidence from wrongful discharge laws. *Journal of Corporate Finance*, 69.

David Hirshleifer, Po-Hsuan Hsu, Dongmei Li, Innovative Originality, Profitability, and Stock Returns, *Review of Financial Studies*, Volume 31, Issue 7, July 2018, Pages 2553–2605, https://doi.org/10.1093/rfs/hhx101

Degryse, H., Laeven, L., & Ongena, S. (2009). The Impact of Organizational Structure and Lending Technology on Banking Competition. *Review of Finance,* 13(2), 225–259.

Delis, M.D. and Staikouras, P.K., 2011. Supervisory effectiveness and bank risk. *Review of Finance*, 15(3), pp.511-543.

Deloitte. (2023). RegTech universe 2023: take a closer look at who is orbiting in the RegTech space. Available at: https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html (Accessed March 26, 2024).

Evanoff, D. D., & Ors, E. (2008). The Competitive Dynamics of Geographic Deregulation in Banking: Implications for Productive Efficiency. *Journal of Money, Credit and Banking*, *40*(5), 897–928.

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2022). Cybersecurity Risk. *The Review of Financial Studies*, *36*(1), 351–407.

Fu, J., Mishra, M., 2022. Fintech in the time of COVID−19: Technological adoption during crises. *Journal of Financial Intermediation* 50, 100945.

Fuster, A., Plosser, M., Schnabl, P., & Vickery, J. (2019). The Role of Technology in Mortgage Lending. *The Review of Financial Studies*, *32*(5), 1854–1899.
Goetz, M. R., Laeven, L., & Levine, R. (2013). Identifying the Valuation Effects and Agency Costs of Corporate Diversification: Evidence from the Geographic Diversification of U.S. Banks. *The Review of Financial Studies*, *26*(7), 1787–1823.
Gupta, M., McGowan, D., & Ongena, S. R. G. (2023). The Cost of Privacy. The Impact of the California Consumer Protection Act on Mortgage Markets. *SSRN Electronic Journal*.
Hannan, T. H., & McDowell, J. M. (1984). The Determinants of Technology Adoption: The Case of the Banking Firm. *The RAND Journal of Economics*, *15*(3), 328.
He, Z., Huang, J., & Zhou, J. (2023). Open Banking: Credit Market Competition When Borrowers Own the Data. *Journal of Financial Economics*.
Helfat, C.E. and Raubitschek, R.S., (2018). Dynamic and integrative capabilities for profiting from innovation in digital platform-based ecosystems. *Research Policy*.
Hendricks, B. E., Neilson, J. J., Shakespeare, C., & Williams, C. D. (2023). Anticipatory Effects around Proposed Regulation: Evidence from Basel III. *The Accounting Review*, *98*(1), 285–315.
Hernando, I., & Nieto, M. J. (2007). Is the Internet delivery channel changing banks' performance? The case of Spanish banks. *Journal of Banking & Finance*, *31*(4), 1083–1099.
Hirtle, B., Kovner, A., & Plosser, M. (2020). The Impact of Supervision on Bank Performance. *The Journal of Finance*, *75*(5), 2765–2808. https://doi.org/10.1111/jofi.12964
Hoberg, G., & Phillips, G. (2016). Text-Based Network Industries and Endogenous Product Differentiation. *Journal of Political Economy*, *124*(5), 1423–1465.
Hoberg, G., Phillips, G., & Prabhala, N. (2014). Product Market Threats, Payouts, and Financial Flexibility. *Journal of Finance*, *69*(1), 293–324.
Kalmenovitz, J., 2023. Regulatory intensity and firm-specific exposure. *The Review of Financial Studies*, 36(8), pp.3311-3347.
Kobarg, S., Stumpf-Wollersheim, J. and Welpe, I.M., (2018). More is not always better: Effects of collaboration breadth and depth on radical and incremental innovation performance at the project level. *Research Policy*.
Kovner, A., Vickery, J., & Zhou, L. (2014). Do big banks have lower operating costs? *Economic Policy Review*, *Dec*, 1–27.
Lewellen, S., & Williams, E. (2021). Did technology contribute to the housing boom? Evidence from MERS. *Journal of Financial Economics*, 141(3), 1244-1261.
Li, X., Huang, S.S. and Song, C., 2017. China's outward foreign direct investment in tourism. *Tourism Management*, *59*, pp.1-6.
Lim, I., & Armitage, S. (2016). Does Distance Impede Regulatory Monitoring? Evidence from the Banking Industry. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2807421
Modi, K., Pierri, N., Timmer, Y., and Peria, M.S.M. 2022. The Anatomy of Banks' IT investments: drivers and implications. IMF Working Papers, 2022(244). Parlour, C. A., Rajan, U., & Zhu, H. (2022). When FinTech Competes for Payment Flows. *Review of Financial Studies*. https://doi.org/10.2139/ssrn.3544981
Pennacchi, G. G., & Santos, J. A. C. (2018). Why Do Banks Target ROE? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3199909
Sarathy, R. and Robertson, C.J., 2003. Strategic and ethical considerations in managing digital privacy. *Journal of Business ethics*, 46, pp.111-126.
Srivastav, A., & Vallascas, F. (2022). Small Business Lending and Regulation for Small Banks. *Management Science*, *68*(10), 7742–7760. https://doi.org/10.1287/mnsc.2021.4176
Sun, L., & Abraham, S. (2021). Estimating dynamic treatment effects in event studies with heterogeneous treatment effects. *Journal of Econometrics*, *225*(2), 175–199. https://doi.org/10.1016/j.jeconom.2020.09.006
Teece, D.J., (1986). Profiting from technological innovation: implications for integration, collaboration, licensing, and public policy. *Research Policy*, 15(6), pp.285-305.
Trebbi, F., & Xiao, K. (2019). Regulation and Market Liquidity. *Management Science*, *67(5)*, 1949–1968.
Voss, W.G. and Houser, K.A., 2019. Personal data and the GDPR: providing a competitive advantage for US companies. *American Business Law Journal*, 56(2), pp.287-344.

West, J., Salter, A., Vanhaverbeke, W., Chesbrough, H., (2014). Open innovation: The next decade. *Research Policy*.
Yannelis, C., & Zhang, A. L. (2021). Competition and Selection in Credit Markets. *National Bureau of Economic Research*. https://doi.org/10.3386/w29169

Figures and Tables

Figure 1: Four staggered DID estimators

This figure presents the results of the event study, covering event study plots constructed using four different estimators: Borusyak, Jaravel, and Spiess (2021) (orange circle markers); the dynamic version of the TWFE model with OLS estimation (purple with triangle markers); Sun and Abraham (2021) (blue diamond markers) and Callaway and Sant'Anna (2021) (red cross markers). Results from the event study constructed with these four different estimators all indicate estimates consistent with the parallel trends assumption. The dependent variable is IT investment. The time variable $D_{i,t,s}^{k}$ capture periods preceding and following the legislation event, and δ_k is the parameter of interest in the event study analysis. More specifically, we decompose the periods before and after the event into eight bins: (i) If the state where a commercial bank is located is expected to propose or enact privacy protection legislation in the next 5 years, 4 years, 3 years, 2 years, or 1 year, the indicators are equal to 1 (*period=-5*, *-4*, *-3*, *-2*, *-1*); (ii) if the state proposes or enacts privacy protection legislation in the current year, the indicator is equal to 1 (*period=0*); (iii) if the state proposed or enacted privacy protection legislation 1 year, 2 years, or 3 years ago, the indicators are equal to 1 (*period=1*, *2*, *3*). In the TWFE model and Callaway and Sant'Anna (2022) method, we included all control variables consistent with the baseline model. Due to the model setup, we did not include control variables in Borusyak, Jaravel, and Spiess (2021) and Sun and Abraham (2021) methods, but we controlled all the bank, year, and state fixed effects. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). The bar chart represents a 95% confidence interval.

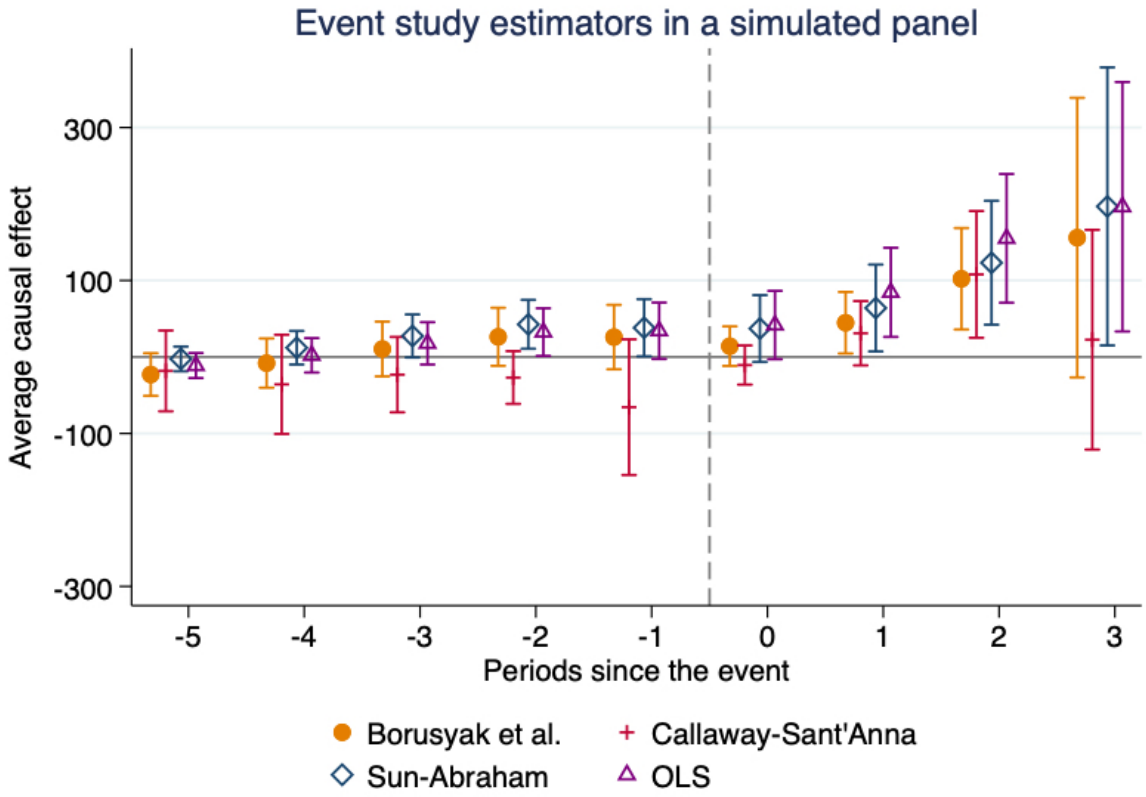

Figure 2: Distribution of estimated coefficients from placebo test

This figure displays the probability density of the estimated coefficients for the impact of privacy legislation on IT investment and expenditure during placebo tests. In each iteration, the true distribution of the event year is retained, while the untreated states are randomly assigned to each year without replacement. The vertical line represents the actual probability density of estimated coefficients from the placebo tests regression and the horizontal line is the estimated coefficients.

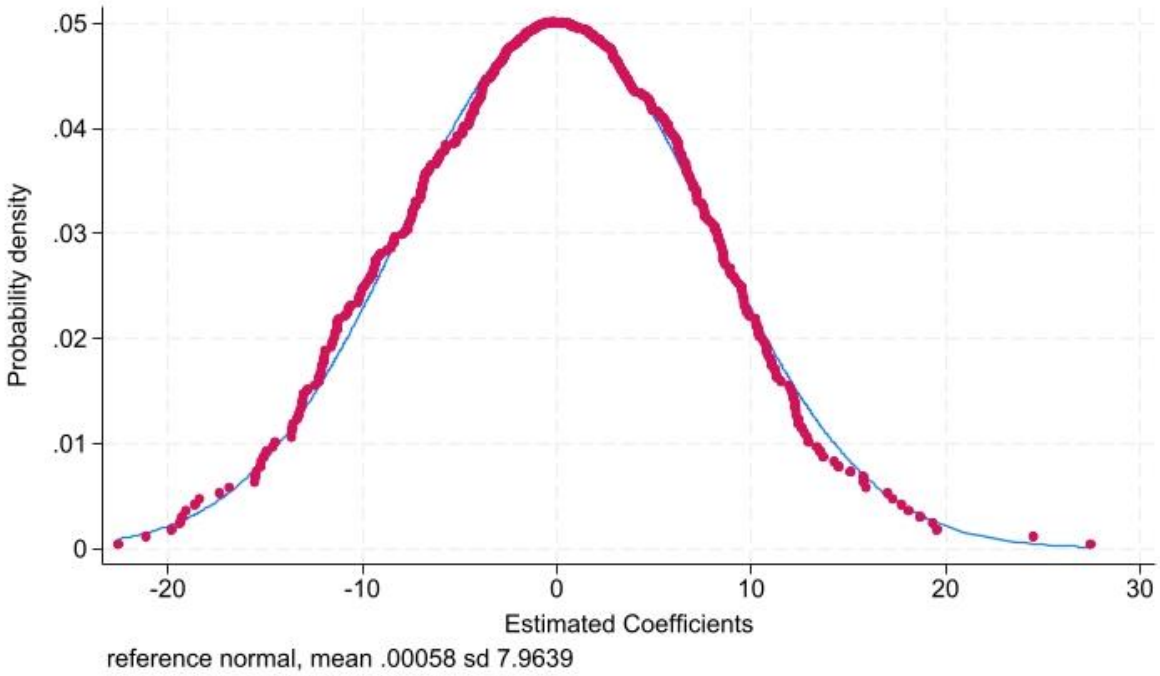

Table 1: Regulation Statistics

This table presents a detailed account of the progress of state-level privacy legislation in the United States since 2018, showcasing the specifics of state privacy initiatives from 2018 to 2022. For states not displayed, this indicates that they have not enacted or implemented relevant state-level privacy legislation.
In the U.S. privacy protection legislation, the abbreviations before each bill number represent different types of legislative proposals or enacted laws, facilitating tracking and reference throughout the legislative process. Specifically, "H" stands for House, indicating a proposal in the House of Representatives; "HB" is an abbreviation for House Bill, denoting a proposal in the House; "HF" stands for House File, referring to a House document; "HR" means House Resolution, a resolution passed by the House; "HCR" represents House Concurrent Resolution, a joint resolution of the House; "LB" is short for Legislative Bill, indicating a legislative proposal; "LD" stands for Legislative Document; "S" abbreviates Senate Bill, denoting a Senate proposal; "SB" is also an abbreviation for Senate Bill, referring to a legislative proposal introduced in the U.S. Senate; "SD" stands for Senate Draft, a draft bill in the Senate; and "SF" signifies Senate File, referring to a Senate document.

State	2018	2019	2020	2021	2022
Alabama				HB 216	
Alaska				SB 116	HB 222; HB 159; SB116
Arizona			SB 1614; HB 2729	HB 2865	HB 2790
California	CCPA		Proposition 24		
Colorado				SB 190	
Connecticut		RB 1108		SB 893	SB 6
Florida			H 963/SB1670	SB 1734; HB 969	SB 1864; HB 9
Georgia					SB 394
Hawaii		HCR 225; SB 418	HB 2572		HB 2051; SB 2428; SB 2797; HB 2341
Illinois		SB 2263	SB 2330; HB 5603	HB 3910	
Indiana					SB 358; HB 1261
Iowa			SF 2351		HF 2506; SF 2208
Kentucky				HB 408	SB 15; HB 586
Louisiana		HR 249			HB 987
Maine					LD 1982
Maryland			HB 249; HB 784; HB 1656	SB 0930	SB 11

(continued next page)

Table 1: Regulation Statistics (cont'd)

State	2018	2019	2020	2021	2022
Massachusetts		S 120		SD 1726	S 2687; H 4514; H 142; H 136; S 46
Michigan					HB 5989
Minnesota			HF 3936	HF 1492; HF 36	HF 1492
Mississippi		HB 1253		SB 2612	SB 2330
Nebraska			LB 746		LB 1188
New Hampshire			HB 1680; HB 1236		
New Jersey	S 2834		A 2188; A 3255		A 505; S 332; A 1971
New Mexico		SB 176			
New York		S 224; S 5642		A 680; A 6042; S 6701; S 567	A 680; S 6701; A 6042; S 567; A 3709
North Carolina				S 569	S 569
North Dakota			HB 1485	HB 1330	
Ohio				HB 376	HB 376
Oklahoma				HB 1602	HB 1602; HB 3447; HB 2969
Pennsylvania		HB 1049		HB 1126	HB1126; HB 2202; HB 2257
Rhode Island		S 0234			HB 7917
South Carolina		H 4812	H 4812		
Texas		HB 4390; HB 4518		HB 3741	
Utah				SB 200	SB 227
Vermont					H 570; H 160
Virginia			HB 473	SB 1392	
Washington		WPA	SB 6281	SB 5062; HB 1433	HB 1433; SB 5062; HB 1850; SB 5813
West Virginia				HF 3159	HB 4454
Wisconsin			AB 870; AB 871; AB 872		AB 957; SB 957; AB 1050; SB 977

Table 2: Descriptive Statistics

The table reports descriptive statistics for all variables in our main empirical analysis. The sample consists of U.S. small BHC commercial banks from 2010 to 2022 with assets of less than 10 billion. The sample used for baseline results includes 70,758 company-year observations. For detailed information on the definition and construction of all variables, please refer to the online Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles.

Variable	N	Mean	SD	1st Perc.	Median	99th Perc.
IT_invest	70,758	190.788	2050.409	0.000	0.000	3852
PrivacyAct	70,758	0.118	0.322	0.000	0.000	1.000
Count_current_year	63,171	0.077	0.350	0	0	2
Dummy_current_year	63,171	0.055	0.227	0	0	1
Count_cummulative	63,171	0.114	0.450	0	0	3
Status	63,171	0.118	0.595	0	0	1
Status2	63,171	0.083	0.313	0	0	2
HHI	70,758	0.116	0.138	0.009	0.070	0.719
Ln_Population	70,758	15.692	0.901	13.436	15.616	17.485
Unemployment	70,758	0.066	0.024	0.029	0.061	0.128
EPU	70,758	90.874	73.649	28.325	68.835	428.462
ROA	70,758	0.009	0.138	-0.031	0.009	0.062
ROE	70,656	0.064	0.820	-0.418	0.078	0.280
Loan_Ratio	70,758	0.617	0.179	0.000	0.647	0.904
Ln_asset	70,758	12.229	1.242	9.502	12.144	15.578
Deposit_Ratio	70,758	0.685	0.142	0.000	0.693	0.915
Leverage	70,758	0.876	0.098	0.169	0.894	0.950
Efficiency	70,772	1.403	146.583	-13.758	1.674	17.534
Market_Share	70,750	0.255	1.185	0.002	0.081	2.739
NIE	70,794	0.040	0.172	0.010	0.028	0.354
Distance	69,830	422.386	366.520	3.209	345.359	1555.207
Interest_Expense	61,829	0.008	0.172	0.001	0.005	0.019
Liquidity	61,829	0.888	14.995	0.113	0.766	1.246
Tier1_2	33,648	0.014	0.029	0.005	0.014	0.031
Capital_Ratio	33,648	0.252	2.154	0.061	0.162	1.773
NPL	29,575	0.001	0.005	0.000	0.000	0.021
Fluidity	13,790	8.330	3.832	1.292	7.957	17.665
Similarity	13,790	27.297	25.980	1.000	18.413	79.269
Cybersecurity[25]	19,431	66658.26	62296.57	1526	30736	187164

[25] Due to the indicators on market competition provided by the Hoberg and Phillips database and the Cybersecurity variable utilized by Florackis et al. (2023), which primarily capture information on publicly listed companies, our sample includes a substantial number of BHC private firms. Consequently, in our subsample analysis, we only include observations with available values for this variable.

Table 3: Baseline Regressions

The table reports ordinary least squares (OLS) regression results and t-statistics (in parentheses) for the impact of privacy legislation proposals on small commercial banks' IT investment and expenditure from 2010 to 2022. The dependent variable is *IT_Invest* which captures the IT-related investment and expenditure. The variable *PrivacyAct* is a dummy variable equal to 1 if the bank's headquarters state has enacted or proposed privacy legislation in or before that year, and 0 otherwise. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). In Panel A, we examine the impact of privacy legislation in the current year on the IT expenditure of small commercial banks in the following year. In Panel B, we examine the influence of privacy legislation on the IT spending of banks, analyzing effects in the year of enactment, the subsequent year, and the year following that. Columns (1)-(3) are all U.S. bank holding companies, while columns (4)-(6) represent the small banks.*, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

Panel A: Baseline regression of privacy legislation

	F. IT_Invest					
	All Banks			Small Banks		
VARIABLES	(1)	(2)	(3)	(4)	(5)	(6)
PrivacyAct	71.392***	69.172***	64.878***	60.672***	55.319***	52.448***
	(3.29)	(3.03)	(3.00)	(3.40)	(3.06)	(2.96)
HHI		-107.271	-137.816		135.286*	75.847
		(-0.75)	(-1.03)		(1.74)	(0.97)
Ln_Population		63.187	102.456		10.280	39.168
		(0.98)	(1.16)		(0.17)	(0.48)
Unemployment		-1,973.951***	-968.958		-1,065.386***	-165.470
		(-3.51)	(-1.06)		(-2.58)	(-0.23)
EPU		-0.013	-0.010		-0.103	-0.077
		(-0.11)	(-0.08)		(-1.01)	(-0.76)
ROA		-1,095.331	-1,267.802*		-1,392.392**	-1,413.486**
		(-1.62)	(-1.82)		(-2.32)	(-2.33)
Loan_ratio		106.922*	88.004		131.677**	118.699**
		(1.78)	(1.43)		(2.47)	(2.22)
Ln(asset)		273.206***	268.408***		257.873***	253.154***
		(5.88)	(5.73)		(6.20)	(6.11)
Deposit_ratio		-96.249	-98.449		-75.047	-56.155
		(-1.48)	(-1.41)		(-1.33)	(-1.00)
Leverage		-1,127.977***	-1,078.954***		-1,245.903***	-1,205.403***
		(-3.04)	(-3.02)		(-3.49)	(-3.59)
Constant	203.502***	-3,005.418***	-3,654.426**	151.336***	-2,017.944*	-2,508.917*
	(125.48)	(-2.63)	(-2.48)	(116.14)	(-1.90)	(-1.88)
Year FE	Y	Y	Y	Y	Y	Y
Bank FE	Y	Y	Y	Y	Y	Y
State FE	Y	N	Y	Y	N	Y
Observations	65,065	64,519	64,519	63,637	63,179	63,179
R-squared	0.767	0.766	0.768	0.729	0.733	0.734

(continued next page)

Table 3: Baseline Regressions (cont'd)

Panel B: Dynamic effects of privacy legislation						
	All Banks			Small Banks		
	IT_Invest	F2.IT_Invest	F3.IT_Invest	IT_Invest	F2.IT_Invest	F3.IT_Invest
VARIABLES	(1)	(2)	(3)	(4)	(5)	(6)
PrivacyAct	33.992*	72.101***	73.041	32.241**	60.241**	-24.456
	(1.83)	(2.62)	(0.89)	(2.10)	(2.47)	(-0.41)
HHI	46.702	-233.697	-95.303	134.222**	-14.857	146.820
	(0.55)	(-1.49)	(-0.57)	(2.33)	(-0.13)	(1.07)
Ln_Population	138.773	37.782	317.125	127.416	-42.540	98.422
	(1.58)	(0.30)	(1.03)	(1.28)	(-0.38)	(0.59)
Unemployment	-763.351	-969.457	-1,065.050	55.246	-26.413	-110.952
	(-0.88)	(-1.15)	(-1.30)	(0.08)	(-0.04)	(-0.16)
EPU	-0.043	-0.411*	-0.088	-0.039	-0.170	-0.005
	(-0.39)	(-1.71)	(-0.34)	(-0.44)	(-1.07)	(-0.03)
ROA	-1,423.486**	-827.785	42.414	-1,389.255**	-504.071	43.811
	(-2.26)	(-1.30)	(0.05)	(-2.34)	(-0.95)	(0.06)
Loan_ratio	75.384	91.383	125.310*	110.541**	103.812*	129.951**
	(1.29)	(1.41)	(1.69)	(2.07)	(1.91)	(2.19)
Ln(asset)	233.942***	278.926***	259.651***	219.567***	258.842***	235.041***
	(5.67)	(5.53)	(4.98)	(5.99)	(5.74)	(5.10)
Deposit_ratio	-55.813	-131.086*	-53.629	-63.200	-60.706	-34.123
	(-0.93)	(-1.73)	(-0.65)	(-1.17)	(-1.14)	(-0.60)
Leverage	-927.203***	-1,048.491***	-1,056.176***	-1,001.785***	-1,040.917***	-835.220***
	(-2.99)	(-2.69)	(-3.06)	(-3.54)	(-2.78)	(-2.68)
Constant	-4,004.212***	-2,716.454	-6,944.479	-3,690.356**	-1,412.096	-3,560.172
	(-2.79)	(-1.28)	(-1.46)	(-2.33)	(-0.75)	(-1.37)
Year FE	Y	Y	Y	Y	Y	Y
Bank FE	Y	Y	Y	Y	Y	Y
State FE	Y	Y	Y	Y	Y	Y
Observations	72,110	57,129	50,038	70,758	55,888	48,902
R-Square	0.738	0.794	0.816	0.703	0.763	0.785

Table 4: Robustness Time Placebo Test

The table reports robust results and t-statistics (in parentheses) for the impact of privacy legislation proposals on small commercial banks' IT investment from 2010 to 2022. The dependent variable is *IT_Invest*. The variable "PrivacyAct" is an indicator variable equal to 1 if the bank's headquarters state has enacted or proposed a privacy protection bill in or before that year, and 0 otherwise. We explore the effects of privacy legislation four years post-enactment on the information technology expenditures of commercial banks in the current year, the following year, and the ensuing two years. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

	(1)	(2)	(3)
VARIABLES	IT_Invest	F.IT_Invest	F2.IT_Invest
F4. PrivacyAct	-1.405	10.153	11.200
	(-0.12)	(0.91)	(1.04)
Controls	Y	Y	Y
Year FE	Y	Y	Y
Bank FE	Y	Y	Y
State FE	Y	Y	Y
Observations	68,053	61,654	55,275
R-squared	0.703	0.734	0.763

Table 5: Regulation Proposal Counts

The table reports ordinary least squares (OLS) regression results and t-statistics (in parentheses) for the impact of privacy legislation proposals on small commercial banks' IT investment and expenditure from 2010 to 2022. The dependent variable is *IT_Invest* which captures the IT-related investment and expenditure. We extend the explanatory variables to a series of regulation proposal count proxies. The variable *Count_current_year* is the number of total privacy protection proposals announced in the current year, *Dummy_current_year* is a dummy taking 1 if the state announced proposals in the current year, *Count_cummulative* denotes the cumulative number of proposals, and *Status* and *Status2* represent the proposal status, with ranges being [0, 3] and [0, 7], respectively. These ranges indicate the varying degrees of a proposal's progress through the legislative framework. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). In Panel A, we examine the impact of privacy legislation in the current year on the IT expenditure of commercial banks in the following year. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

	(1)	(2)	(3)	(4)	(5)
VARIABLES	F. IT_Invest				
Count_current_year	19.455**				
	(2.33)				
Dummy_current_year		26.248**			
		(2.29)			
Count_cummulative			29.931***		
			(2.93)		
Status				32.281*	
				(1.86)	
Status2					4.966
					(0.50)
Controls	Y	Y	Y	Y	Y
Year FE	Y	Y	Y	Y	Y
Bank FE	Y	Y	Y	Y	Y
State FE	Y	Y	Y	Y	Y
Observations	63,171	63,171	63,171	63,171	63,171
R-squared	0.733	0.733	0.734	0.734	0.733

Table 6: Mechanism- Market Competition Pressure

This table reports the results and t-statistics (in parentheses) on the potential mechanisms behind the impact of the proposal of privacy legislation on the IT expenditure of small commercial banks from 2010 to 2022, across different competitive environments. The dependent variable is *IT_Invest*. The variable 'PrivacyAct' is a binary indicator set to 1 if the state, where a bank's headquarters is located, has enacted or proposed privacy legislation in that year or earlier, and 0 otherwise. Columns (1) and (2) present the data split into two groups based on the product similarity index for banks, constructed by Hoberg and Phillips (2016). Columns (3) and (4) categorize banks into high or low-competition groups depending on whether their competition index, developed by Hoberg and Phillips (2014), is above or below the median for the sample year. We test for differences in the 'PrivacyAct' coefficient across the respective subsample divisions. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

	F. IT_Invest			
VARIABLES	Product Fluidity High	Product Fluidity Low	Product Similarity High	Product Similarity Low
	(1)	(2)	(3)	(4)
PrivacyAct	261.935***	-5.646	240.723***	69.074
	(3.39)	(-0.13)	(2.74)	(1.16)
P-value of coefficients difference	0.00		0.04	
Controls	Y	Y	Y	Y
Year FE	Y	Y	Y	Y
Bank FE	Y	Y	Y	Y
State FE	Y	Y	Y	Y
Observations	6,049	5,692	5,998	6,147
R-squared	0.778	0.860	0.801	0.775

Table 7: Mechanism- Regulatory Intensity (Distance)

This table reports the results and -statistics (in parentheses) on potential mechanisms behind the differences in responses to the proposal of privacy legislation on the IT expenditure of small commercial banks from 2010 to 2022, considering varying intensities of regulatory scrutiny. The dependent variable is *IT_Invest*. 'PrivacyAct' is a binary variable set to 1 if the state where the bank's headquarters are located has enacted or proposed privacy legislation in that year or prior, and 0 otherwise. We capture and measure the costs associated with regulatory enforcement based on the driving distance (in kilometers) between the bank's headquarters and its primary regulatory authority (i.e., OCC, FDIC, and Fed), with the assumption that enforcement costs increase with distance from the primary regulator. Banks are categorized into two groups based on their distance from the main regulatory body, banks regulated by the FDIC, banks regulated by the Federal Reserve, and banks regulated by the OCC. Columns (1), (3), (5), and (7) display results for distances above the median within the sample, while columns (2), (4), (6), and (8) present results for distances below the sample median. We test for differences in the 'PrivacyAct' coefficient across the respective subsample divisions. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. *L* refers to longer-distance and *S* represents shorter distance. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

	F. IT_Invest							
	Distance Long	Distance Short	FDIC Long	FDIC Short	FED Long	FED Short	OCC Long	OCC Short
VARIABLES	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
PrivacyAct	22.887	77.571***	25.857	50.909*	20.088	163.564*	73.716**	52.894
	(0.94)	(3.03)	(0.92)	(1.94)	(0.18)	(1.95)	(2.00)	(0.74)
P-value of coefficients difference	0.10		0.27		0.07		0.37	
Controls	Y	Y	Y	Y	Y	Y	Y	Y
Year FE	Y	Y	Y	Y	Y	Y	Y	Y
Bank FE	Y	Y	Y	Y	Y	Y	Y	Y
State FE	Y	Y	Y	Y	Y	Y	Y	Y
Observations	32,069	31,109	20,538	20,466	4,756	4,740	6,024	5,930
R-squared	0.685	0.763	0.706	0.780	0.655	0.793	0.757	0.744

Table 8: Successful Cyberattack after the Financial Crisis

This table reports the results and t-statistics (in parentheses) of potential mechanisms behind the impact of privacy legislation proposals on the IT expenditure of small commercial banks from 2010 to 2022, about different levels of cybersecurity exposure risk. The dependent variable is *IT_Invest*. 'PrivacyAct' is a binary variable that is set to 1 if the state where a bank's headquarters is located has enacted or proposed privacy legislation in that year or earlier, and 0 otherwise. Columns (1) and (2) utilize a cybersecurity risk exposure index developed by Florackis et al. (2023), dividing banks into high or low-cybersecurity risk exposure groups depending on whether their exposure index is above or below the median for the sample year. We test for differences in the 'PrivacyAct' coefficient between these subsample divisions. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

VARIABLES	F. IT_Invest	
	Cybersecurity High	Cybersecurity Low
	(1)	(2)
PrivacyAct	169.882***	67.027
	(2.80)	(1.39)
P-value of coefficients difference	0.06	
Controls	Y	Y
Year FE	Y	Y
Bank FE	Y	Y
State FE	Y	Y
Observations	8,152	8,061
R-squared	0.784	0.792

Table 9: Compliance effect of IT investment

This table reports additional results and t-statistics (in parentheses) on whether IT investment would prevent cyber attacks. The independent variable is *IT_Invest* one year lagged in Columns (1) and (3), and the total IT investment in the last two years in Column (2). Our variables of interest are the number of successful cyber attacks in each year on each bank. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). We also include the same control variables and bank, year, and state fixed effect matrices as the baseline to control for these time-invariant factors. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

	Poisson		OLS
	(1)	(2)	(3)
VARIABLES	#Cyber attack	#Cyber attack	#Cyber attack
L.IT_Invest(/1000)	-0.082		0.000
	(-0.67)		(0.39)
Cum_IT_Invest(/1000)		-0.023	
		(-0.38)	
Controls	Y	Y	Y
Year FE	Y	Y	Y
Bank FE	N	N	Y
State FE	Y	Y	Y
Observations	37,927	37,927	63,212
R-squared			0.096

Table 10: Proactive effect of IT investment

This table reports additional results and t-statistics (in parentheses) on the impact of banks' IT expenditure on bank performance. The independent variable is *IT_Invest*. Our variables of interest are the bank's competitiveness, efficiency, and asset quality. Panel A investigates whether IT investments have enhanced their profitability (ROE) and competitiveness (Market Share), using the ratio of a bank's total deposits to the sum of all banks' deposits within a state. Panel B examines the impact of IT investments on their operational conditions, employing Interest expense, Non-Interest Expense (NIE), and Efficiency to measure related performance. In Panel C, we assess whether IT investments by small banks improve the bank's capital structure and asset quality. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). We also include the same control variables and bank, year, and state fixed effect matrices as the baseline to control for these time-invariant factors. *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

Panel A. IT investment on bank's profitability and competitiveness

	(1)	(2)
VARIABLES	ROE	Market share
IT_Invest	-0.002***	0.007
	(-2.69)	(1.41)
Controls	Y	Y
Year FE	Y	Y
Bank FE	Y	Y
State FE	Y	Y
Observations	67,706	70,087
R-squared	0.650	0.851

Panel B. IT investment on bank's expense and efficiency

	(1)	(2)	(3)
VARIABLES	Interest expense	NIE	Efficiency
IT_Invest	-0.000	0.000	0.029*
	(-0.40)	(1.55)	(1.82)
Controls	Y	Y	Y
Year FE	Y	Y	Y
Bank FE	Y	Y	Y
State FE	Y	Y	Y
Observations	60,561	70,794	70,772
R-squared	0.829	0.943	0.248

Panel C. IT investment on bank's asset quality and structure

	(1)	(2)	(3)
VARIABLES	Tier1_2	Capital_ratio	NPL
IT_Invest	-0.000	-0.004**	0.000
	(-0.26)	(-2.19)	(1.44)
Controls	Y	Y	Y
Year FE	Y	Y	Y
Bank FE	Y	Y	Y
State FE	Y	Y	Y
Observations	25,667	25,667	29,128
R-squared	0.854	0.979	0.548

Appendix

Table A1: Variable Definition

	Definition	Source
IT_Invest	Text analysis to classify IT-related expenses in financial reports' non-interest expenses as "IT expenses" such as "software" "computer" or "Internet"	Pierri database (Modi et al., 2022)
PrivacyAct	Whether the state has issued and passed privacy legislation [0,1]	IAPP
Count_current_year	The number of total proposals announced in the current year	IAPP
Dummy_current_year	Whether the state announced the proposal in the current year [0,1]	IAPP
Count_cummulative	The number of cumulative proposals up to the current year	IAPP
Status	0=no proposal, 1=proposal announcement, 2=proposal signed into law, 3=regulation enforcement (up to the current year)	IAPP
Status2	0=no proposal, 1=proposal announcement, 2=proposal in committee, 3=proposal in cross chamber, 4=proposal in cross committee, 5=proposal voting passed, 6=proposal signed by the governor, 7=regulation enforcement	IAPP
HHI	Deposit-based Herfindahl-Hirschman Index	FDIC
Ln_Population	The logarithm of the total population in each state	Census
Unemployment	Unemployment rate in each state	Census
EPU	Average of monthly policy uncertainty index in each state	
ROA	Bank's net income over total assets	Bank regulatory
ROE	Bank's net income over total common equity	Bank regulatory
Loan_Ratio	Bank's total loans over total assets	Bank regulatory
Ln_asset	Bank's logarithm of total assets	Bank regulatory
Deposit_Ratio	Bank's total deposits over total assets	Bank regulatory
Leverage	Bank's total debts to total assets	Bank regulatory
Similarity	The pairwise product similarities for each bank with competitor firms in 10-k filings.	Hoberg and Phillips Database
Fluidity	The overlap between the product descriptions of firms and corresponding rivals.	Hoberg and Phillips Database
Distance	The time for driving between two locations	Google-API
Internet_Access	The number of households with internet access to the total number of households in each state	ACS
Tier1_2	Tier 1 and 2 capitals over total risk-weighted assets	Bank regulatory
Capital_Ratio	Total risk-based capital over total risk-weighted assets	Bank regulatory
NPL	Total loans due over 90 days over total loans	Bank regulatory
Interest_Expense	Total Interest_Expense over total deposits	Bank regulatory
NIE	Total Non-Interest_Expense over total assets	Bank regulatory
Efficiency	Non-Interest_Expenses to the total revenues	Bank regulatory
Market_Share	Each bank's total deposits over the total deposits in each state	FDIC

Table A2: Robustness: Remove observations have been successfully implemented

The table reports robustness regression results and t-statistics (in parentheses) for the impact of privacy legislation proposals on small commercial banks' IT expenditure from 2010 to 2022. We drop the observations of California, Virginia, Colorado, Connecticut, and Utah, due to their privacy legislation having been enacted in 2023. The dependent variable is *IT_Invest* in columns (1) and (2), and *IT_Invest* scaled by *Non-interest Expense* in Column (3). The variable *PrivacyAct* is a dummy variable equal to 1 if the bank's headquarters state has enacted or proposed privacy legislation in or before that year, and 0 otherwise. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

	F. IT_Invest		F. IT_Invest/NIE
VARIABLES	(1)	(2)	(3)
PrivacyAct	58.662***	50.749***	0.867*
	(3.14)	(2.77)	(1.73)
Controls	N	Y	Y
Year FE	Y	Y	Y
Bank FE	Y	Y	Y
State FE	Y	Y	Y
Observations	59,162	58,725	63,179
R-squared	0.718	0.724	0.584

Table A3: Robustness: Large and Tiny banks

The table reports robustness regression results and t-statistics (in parentheses) for the impact of privacy legislation proposals on small commercial banks' IT expenditure from 2010 to 2022. The dependent variable is *F.IT_Invest* in columns (1) - (2). The variable *PrivacyAct* is a dummy variable equal to 1 if the bank's headquarters state has enacted or proposed privacy legislation in or before that year, and 0 otherwise. In our paper, we define "tiny banks" as those whose total assets are in the lowest 10% of all U.S. commercial banks in our sample. We include big banks and small banks but exclude tiny banks in column (1) and only small banks and exclude very small banks in column (2). For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

VARIABLES	F. IT_Invest		
	Large and small banks (exclude tiny)	Small banks (exclude tiny)	Narrow obs to banks with IT investment
	(1)	(2)	(3)
PrivacyAct	69.053***	54.575***	146.006***
	(2.96)	(2.86)	(2.79)
Controls	Y	Y	Y
Year FE	Y	Y	Y
Bank FE	Y	Y	Y
State FE	Y	Y	Y
Observations	57,589	56,252	20,416
R-squared	0.769	0.736	0.722

Table A4: Robustness: Exclude Covid-19 period

The table reports robustness regression results and t-statistics (in parentheses) for the impact of privacy legislation proposals on small commercial banks' IT expenditure. The dependent variable is *IT_Invest* in columns (1) and (2). The variable *PrivacyAct* is a dummy variable equal to 1 if the bank's headquarters state has enacted or proposed privacy legislation in or before that year, and 0 otherwise. We exclude the COVID-19 period in column (1) and only keep observations from 2015-2020 in column (2). For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

	F. IT_Invest		IT_Invest	F. IT_Invest
VARIABLES	2010-2020	2015-2020	Exclude 2020	Exclude 2020
	(1)	(2)	(3)	(4)
PrivacyAct	64.637**	44.776**	34.451**	50.745**
	(2.47)	(2.10)	(1.99)	(2.26)
Controls	Y	Y	Y	Y
Year FE	Y	Y	Y	Y
Bank FE	Y	Y	Y	Y
State FE	Y	Y	Y	Y
Observations	59,657	26,978	65,871	58,506
R-squared	0.784	0.888	0.707	0.759

Table A5: Robustness: Overall trend of IT investment

The table reports robustness regression results and t-statistics (in parentheses) for the impact of privacy legislation proposals on small commercial banks' IT expenditure. The dependent variable is *IT_Invest* in columns (1) and (2), and the anomaly of IT investment above the median of all samples within each year. The variable *PrivacyAct* is a dummy variable equal to 1 if the bank's headquarters state has enacted or proposed privacy legislation in or before that year, and 0 otherwise, and Internet_Access is the ratio of households with internet access over total households in each state for each year. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

	F. IT_Invest		F. IT_Invest_Anomoly
VARIABLES	2010-2020	2015-2020	
	(1)	(2)	(3)
PrivacyAct	48.136**	49.768**	0.062**
	(2.33)	(2.39)	(2.39)
Internet_Access	-64.037	-371.831	-0.463
	(-0.14)	(-0.80)	(-0.80)
Controls	Y	Y	Y
Year FE	Y	Y	Y
Bank FE	Y	Y	Y
State FE	N	Y	Y
Observations	44,041	44,039	44,039
R-squared	0.813	0.815	0.815

Table A6: Robustness: Potential influence of IT investment zero inflation issues

This table presents the robustness regression results and t-statistics (in parentheses) for the impact of privacy legislation proposals on IT expenditures of small commercial banks from 2010 to 2022. We employed both the ordinary Poisson model and the zero-inflated Poisson model. Column (1) displays the results from the ordinary Poisson regression, while Column (2) and (3) respectively show the first and second stages of the zero-inflated Poisson regression results. Then we limited our analysis to banks that made IT investments during our sample period (2010-2022), excluding those that no longer invest in IT in column (4). The dependent variable, *IT_Invest*, is featured in columns (1)-(4). The variable *PrivacyAct* is a dummy variable that equals 1 if the state where the bank's headquarters are located enacted or proposed privacy legislation in that year or earlier, otherwise it is 0. Detailed information on the definitions and constructions of all control variables can be found in Appendix Table A1. Continuous variables, excluding macroeconomic variables, are winsorized at the 1st and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). The significance levels * , ** , and *** indicate significance at the 10%, 5%, and 1% levels, respectively.

	F. IT_Invest			
	Poisson	ZIP 1st stage	ZIP 2nd stage	Investment in IT ever
	(1)	(2)	(3)	(4)
PrivacyAct	0.158*		0.144***	146.006***
	(1.91)		(110.91)	(2.79)
Non-Interest Expense		-0.000***		
		(-13.44)		
Controls	Y	Y	Y	Y
Year FE	Y	Y	Y	Y
Bank FE	Y	Y	Y	Y
State FE	Y	Y	Y	Y
Observations	19,559	63,488	63,488	20,416

Table A7: Proposal Heterogeneity

This table reports the results and t-statistics (in parentheses) of the proposal heterogeneity. The dependent variable is *IT_Invest*. 'PrivacyAct' is a binary variable that is set to 1 if the state where a bank's headquarters is located has enacted or proposed privacy legislation in that year or earlier, and 0 otherwise. Columns (1) reports the baseline regression results with the subsamples that announce proposals with granted customer lawsuit right and (2) is the result based on other samples. For detailed information on the definition and construction of all control variables, please refer to Appendix Table A1. Continuous variables, except macroeconomic variables, are weighted at the first and 99th percentiles. Standard errors are clustered at the bank level (statistics in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

VARIABLES	(1) Customer lawsuit right=Y	(2) Customer lawsuit right=N
PrivacyAct	43.407*	69.429***
	(1.74)	(2.68)
P-value of coefficients difference	0.204	
Controls	Y	Y
Year FE	Y	Y
Bank FE	Y	Y
State FE	Y	Y
Observations	18,836	44,340
R-squared	0.783	0.713