Government Data Breaches, Internal Controls, and Municipal Borrowing Costs *

Sean Cao† Anya Nakhmurina‡ Tianchen (Hugo) Zhao§

November 5, 2026

Abstract

We investigate the role of internal controls in the financial consequences of data breaches for U.S. local governments. Using a stacked difference-in-differences design, we find that breached municipalities experience an increase in municipal bond yield spreads. The effect is concentrated in municipalities with pre-existing weaknesses in internal controls, including both general and information system-specific controls, suggesting that well-maintained internal controls may mitigate the spread increase associated with a data breach. Nonetheless, we find little evidence of internal control improvements in breached municipalities. Instead, municipalities with control weaknesses cut total and administrative expenditures, which include internal control spending. Overall, our results raise concerns that data breaches leave municipalities more vulnerable to future incidents and the associated erosion of public services.

*For helpful comments, we thank DuckKi Cho (discussant), Jess Cornaggia, Teodor Duevski (discussant), Yun Feng (discussant), Marcin Kacperczyk, Renping Li (discussant), Vojislav Maksimovic, Roxana Mihet (discussant), Pablo Slutzky, Laura Starks, Kate Volkova, David Wang (discussant), Chenqi Zhu (discussant), and conference and seminar participants at the Australasian Finance and Banking Conference 2024, the Inter-Finance PhD Seminar 2024, the Sydney Banking and Financial Stability Conference 2024, the Eastern Finance Association Annual Meeting 2025, the SGF 2025, the Transatlantic Doctoral Conference 2025, the FARS Midyear Meeting 2026, the University of Macau, and the University of Maryland. Sean Cao acknowledges support from the AI Initiative for Capital Market Research at the University of Maryland. We used ChatGPT and Claude to copyedit the paper.

†Robert H. Smith School of Business, The University of Maryland. *Email:* scao824@umd.edu

‡Yale School of Management, Yale University. *Email:* anya.nakhmurina@yale.edu

§Robert H. Smith School of Business, The University of Maryland. *Email:* tzhao97@umd.edu

1. Introduction

Data breaches cause serious disruption and have become a growing concern for local governments and the public. For example, an external cyberattack forced Foster City, California, to suspend most city services (Johns, 2026). Yet breaches do not require a sophisticated external attacker, as has been illustrated repeatedly, including the recent cases in which Shasta County, California, and Citrus County, Florida, exposed health records and Social Security numbers, respectively, simply by mishandling responses to public records requests (Shasta County, 2026; Security Magazine, 2026). Meanwhile, federal support for local cybersecurity is shrinking. Federal funding for the cybersecurity information-sharing center for state and local governments ended in 2025 (Wood, 2025), and the federal cybersecurity grant program for state and local governments has yet to be reauthorized (National Association of Counties, 2026).

Compromised municipal data systems can expose residents' private information, undermine trust in local institutions, and disrupt essential public services. Unlike consumers, who can take their business elsewhere after a corporate breach, residents have little choice but to entrust their local government with their most sensitive data, from Social Security numbers to financial records (Funk et al., 2019). Beyond immediate remediation expenses, which recent estimates put at $2.55 million for the average public-sector incident (IBM Security, 2024), breaches can suspend critical government functions. They can also reveal negative information about governance practices and internal controls, which may affect borrowing costs in the municipal bond market.

A breach can expose control weaknesses because effective data security depends on internal control quality (OCCM, 2025). Internal controls are the procedures used to safeguard assets, produce reliable records, and comply with laws and regulations (COSO, 2013). The sensitive data that residents entrust to their local government is one of the assets these procedures protect. In practice, internal controls determine who can access residents' records, how user activity is monitored, and how devices holding data are physically

secured (ONYSC, 2016).

Yet internal control deficiencies are not uncommon (Wallace, 1981; GAO, 2007; Gore et al., 2023). Even where auditors document no internal control weaknesses, these procedures are often maintained with minimal resources because municipalities favor public-facing roles over operational staff (Deloitte, 2020). Few cities have the dedicated IT budgets, with only 17% being highly engaged in internal systems protection, and 67% lacking the funds to do so (Funk et al., 2019).[1] Audits can also miss problems (Hobson et al., 2017). It is therefore unclear whether the absence of reported weaknesses reflects internal controls strong enough to limit the financial consequences of a breach. Audited reports can instead give investors a false sense of security (Li and Venkatachalam, 2025).

Evidence from the corporate sector offers limited guidance on this question, because local governments differ from firms in how their controls are resourced, overseen, and audited. They operate under tighter budgets, answer to voters rather than shareholders, and struggle to compete with the private sector for skilled cybersecurity professionals (Deloitte, 2020). Moreover, whereas auditors of large public firms must attest to whether internal control over financial reporting is effective (AICPA, 2020a), Single Audits report the weaknesses auditors identify without offering an opinion on whether controls are effective (OMB, 2014f). However, even with these limitations, Single Audits appear to discipline management, at least in nonprofit hospitals (Ruan et al., 2025). We therefore study how municipal borrowing costs respond to data breaches, whether breaches are less costly for municipalities with stronger internal controls, and whether breached municipalities subsequently strengthen their controls.

We begin by examining the impact of data breaches on offering yield spreads in the primary municipal bond market, a critical source of financing for local governments in the U.S. In the primary market, price-setting demand comes from sophisticated institutional investors and underwriters, who routinely track issuer-specific credit news (Cuny et al.,

[1]The average municipality in our sample reported annual expenditures exceeding revenues, suggesting breach costs can be financially material (at least to the average local government).

2026). If these investors view a breach as a signal of higher credit risk, they should demand higher yields on the municipality's new bonds, increasing its borrowing costs.

We use a stacked difference-in-differences specification to estimate the impact of publicly reported data breaches on U.S. municipalities from 2007 to 2017. In each breach cohort, we compare bonds issued by the breached municipality with bonds issued by never-breached municipalities, before and after the breach is reported. Offering yield spreads of breached municipalities increase by approximately 7 basis points (30% of the sample mean) within one year after a breach announcement. The financing effects materialize only after breach announcements and remain robust in a sample of municipalities matched on their ex-ante breach probability, suggesting that investors perceive breached municipalities as bearing greater credit risk.

Next, we explore heterogeneity across different types of data breaches to identify which incidents impose higher costs on municipalities. While the literature has primarily focused on cyberattacks (Curti et al., 2024; Andreadis et al., 2024), cyberattacks and breaches of unknown type account for only 24% of breaches in our sample. The remaining 76% involve insiders: 60% stem from insider carelessness (unintentional leakage resulting from employee errors or oversight), and 16% from insider offenses (deliberate theft or misuse of data by authorized individuals). Among these categories, insider offenses are associated with the largest increase in municipal bond spreads (34% to 48% of the sample mean), and insider carelessness with an increase of 26% to 31%. The estimates for external cyberattacks are not statistically significant. These findings suggest that investors view insider-related breaches, whether intentional or not, as more financially consequential. One explanation is that insider breaches reveal more about the quality of a municipality's internal controls, and investors adjust their risk perceptions accordingly.

To test this explanation, we examine whether the absence of pre-existing general internal control issues is associated with less severe capital market consequences. We use auditor assessments from annual Single Audits (SA) reports, in which external auditors

evaluate the appropriateness of the design and the operational effectiveness of municipalities' internal controls, including their information security protocols (AICPA, 2020b). Ex ante, the relationship between auditor-assessed control quality and market reactions to data breaches is unclear. Investors may view municipalities without identified weaknesses as fundamentally sound and treat breaches as isolated events. Alternatively, breaches may expose hidden deficiencies, prompting investors to reassess municipalities that auditors previously deemed sound. We find that the increase in offering yield spreads is concentrated in municipalities with internal control weaknesses identified in the year preceding the breach. By contrast, municipalities without previously flagged weaknesses do not experience a statistically significant increase in spreads.

Next, we examine whether municipalities' hiring demand for IT professionals, a proxy for information system control quality (ONYSC, 2016), is associated with smaller increases in borrowing costs after data breaches. Recruiting IT personnel may signal that a municipality takes breach threats seriously and invests in prevention. Consistent with this hypothesis, we observe no statistically or economically significant change in bond spreads among municipalities that sought to recruit IT professionals in the year before a breach. In contrast, municipalities without such hiring efforts experience notably larger increases in bond spreads, suggesting that investors view the absence of dedicated IT resources as indicative of weaker preparedness.

Given the evidence that relatively stronger internal controls are associated with lower costs from data breaches, we investigate whether local governments address weaknesses in their control systems after breaches. Surprisingly, we find no reduction in the likelihood of auditor-identified internal control weaknesses in breached municipalities. We also find no robust evidence of increased IT hiring after breaches. Together, these results suggest that breached municipalities generally *do not* strengthen their internal control systems.

To better understand why local governments do not resolve their internal control weaknesses, we examine their expenditures following breaches. We find that municipalities

with pre-existing internal control weaknesses reduce their total expenditures relative to total revenues after breaches. Specifically, the decline is concentrated in spending on central staff and financial administration, categories directly related to internal control functions. This decline suggests that municipalities already struggling with weaker controls become more financially constrained following breaches, prompting them to reduce operational expenditures rather than invest in improved governance. Consequently, such cuts may further expose them to future breaches, higher borrowing costs, and lower-quality public service provision.

We acknowledge that establishing a causal link between internal control quality and the consequences of data breaches is difficult in our setting, because both may reflect underlying (and unobservable) governance issues. Nonetheless, documenting this association is important, particularly given our evidence that municipalities generally fail to strengthen internal controls following breaches despite incurring significant costs.

This paper contributes to the emerging literature on the consequences of municipal data breaches. Curti et al. (2024) demonstrate that municipal bond markets price in cyberattacks across governmental entities. Andreadis et al. (2024) focus on spillover effects, showing that cyberattacks targeting either municipalities or firms within a county increase debt costs for all municipal issuers in that area. Osborne (2025) finds that cyberattacks also increase the borrowing costs of county governments. Our work complements and extends these findings in three dimensions.

First, these studies focus on external cyberattacks, whereas insiders are responsible for most municipal breaches in our sample. We find that the market response to internal data breaches is more significant than to cyberattacks. This suggests that while external threats are a significant risk (Curti et al., 2024; Andreadis et al., 2024; Osborne, 2025), internal vulnerabilities can also incur substantial costs. Second, we show that municipalities without pre-existing internal control weaknesses experience muted market response following breaches, consistent with disciplined control systems being associated with

lower breach costs. Third, we contribute evidence to the debate on the real consequences of data breaches. Andreadis et al. (2024) find that municipal spending, aggregated at the county level, decreases with the cumulative number of cyberattacks on either firms or municipalities within the county. Osborne (2025) finds no change in the total expenditures of hacked counties but documents a reallocation away from public services such as policing and water. In contrast, Curti et al. (2024) find that municipalities directly experiencing cyberattacks increase their total expenditures during the breach year before returning to normal levels. We document a more nuanced pattern. Municipalities with prior internal control weaknesses, where breach-related financing costs are concentrated, reduce their total expenditures relative to revenues not immediately but two years after a breach. This lag is consistent with the municipal budget cycle, in which budgets are adopted months before the fiscal year begins (Morgan et al., 2017). The decline is concentrated in spending on central staff and financial administration, categories directly related to internal control functions.

We also contribute to the literature on internal controls, both on how markets price control weaknesses and on whether organizations remediate them after breaches. Ogneva et al. (2007) find no meaningful association between internal control weaknesses and firms' cost of capital after controlling for standard firm characteristics. Gore et al. (2023) document that municipal bond markups are higher when issuers have material weaknesses in internal control. Material weaknesses are also associated with higher municipal borrowing costs, particularly when accompanied by other adverse audit outcomes (Park et al., 2017; Edmonds et al., 2023). Our findings suggest that investors also consider the quality of pre-existing internal controls when assessing the credit risk implications of data breaches. Existing research also finds that firms hire cybersecurity workers after breaches (Bana et al., 2025) and, in some samples, improve their internal controls (Zhou and Huang, 2024), that peer breaches prompt firms to remediate control weaknesses (Ashraf, 2022), and

that financial statement audits reduce clients' breach risk (Liu, 2025).[2] By contrast, we find no evidence that breached municipalities reduce auditor-identified internal control weaknesses. Relatedly, we argue that tightened financial constraints after breaches may explain why some municipalities struggle to address internal control weaknesses.

More broadly, our paper contributes to an emerging literature on municipal debt pricing and government spending policies. Cheng et al. (2023) show that state-level legalization of medical marijuana increases states' borrowing costs in the primary municipal bond market and induces states to increase expenditures toward public welfare programs. Li et al. (2024) document that state mandates requiring employers to verify workers' legal status lower local governments' borrowing costs and reduce fiscal deficits. Kim et al. (2026) show that strengthening public access to government records lowers municipal borrowing costs. Dambra et al. (2023) show that mandated disclosure of previously unrecognized pension liabilities leads counties to update their information sets and adjust fiscal spending. Our paper highlights municipal data security as another factor that affects local government financing costs and is associated with reductions in total expenditures.[3]

The remainder of the paper is structured as follows: Section 2 describes the institutional background and develops our hypotheses. Section 3 describes the data and sample construction. Section 4 introduces the empirical methodology and summary statistics. Section 5 estimates the impact of data breaches on local governments' costs of debt. Section 6 examines how the increase in borrowing costs varies with pre-breach internal controls. Section 7 analyzes local governments' responses to data breaches. Section 8 concludes.

[2]Relatedly, auditors respond to data breaches by raising audit fees and hiring specialized personnel (Lawrence et al., 2018; Li et al., 2026), and some firms purchase voluntary cybersecurity audits (Schoenfeld, 2024).

[3]Related recent work documents that factors such as credit ratings (Cornaggia et al., 2018, 2023; Zhang, 2024), ESG risks (Dougal et al., 2019; Painter, 2020; Chordia et al., 2022; Goldsmith-Pinkham et al., 2023; Lu and Ye, 2023), information disclosure (Cuny, 2018; Cuny et al., 2025), political alignment (Dagostino and Nakhmurina, 2026b), and fiscal subsidy policies (Gao et al., 2019) influence municipal financing.

2. Institutional Background and Hypothesis Development

2.1. Data Breaches at Local Governments

To collect taxes, run utilities, pay employees, and administer public programs, local governments store large amounts of sensitive information about their residents and employees. These records include Social Security numbers, bank account details, employment records, and medical histories. A data breach occurs when such information is lost, stolen, or exposed to unauthorized parties. Breaches typically become public through notifications to affected individuals, reports to state authorities, and media coverage.[4]

Breaches differ in how the data are compromised. In an external cyberattack, outsiders gain access to municipal systems, for example through phishing emails, malicious software, or unpatched vulnerabilities. Insider breaches originate with the government's employees or contractors. They include carelessness, such as a lost laptop holding unencrypted records or sensitive documents mailed or posted online in error. They also include offenses, in which employees deliberately steal or misuse data. For example, an employee of the New York City Police Pension Fund was arrested for taking backup tapes containing the Social Security numbers and bank account information of about 80,000 current and retired police officers.[5] Insider incidents account for 76% of the breaches in our sample (Section 5.4).

Breaches impose direct costs on the affected government. The government must notify affected individuals, investigate the incident, restore its systems, and respond to legal claims. After a 2023 ransomware attack exposed the personal information of current and former employees, for example, Dallas approved $8.5 million to notify affected individuals, provide them with identity theft and fraud protection, and hire outside cybersecurity firms to restore the city's systems (Arghire, 2023). Attacks that disable systems can also suspend services and revenue collection. Baltimore, for example, lost or delayed an estimated $8.2

[4]These are also the sources from which the Privacy Rights Clearinghouse compiles our breach data (Section 3.1).

[5]Vijayan (2009) describes the case.

million in revenue from property taxes, real estate fees, and fines after its 2019 ransomware attack (Baltimore Sun, 2019). Legal claims add to these costs. In 2026, Clark County, Washington, agreed to pay $800,000 to settle a class action over a 2023 breach of residents' information (Phiel, 2026). These costs compete with debt service and public services for the same operating budget.[6]

2.2. *Internal Controls and Single Audits*

The internal controls that protect data, known as information system controls, restrict access to authorized users, monitor user activity, secure data and software, and physically safeguard equipment (ONYSC, 2016). Each type of breach can be traced to the failure of one of these controls. A lost unencrypted laptop points to failed physical and data safeguards. An employee who sells residents' records points to failed access restrictions and monitoring. A successful cyberattack can point to weaknesses in software security, access restrictions, or monitoring. It is a noisier signal of control quality, however, because sophisticated attackers can also breach well-designed controls.

Unlike public firms, local governments are not subject to the internal control reporting requirements of the Sarbanes-Oxley Act. The primary standardized source of information about their controls is the Single Audit. Under the Single Audit Act of 1984, a local government that expends federal awards above a threshold must undergo an annual audit of its financial statements and its major federal programs. The threshold was $500,000 for fiscal years ending after December 31, 2003, and $750,000 for fiscal years beginning on or after December 26, 2014 (OMB, 2003, 2014b).

Single Audits also examine controls over a government's information systems. Beyond the procedures required by auditing standards, the auditor must obtain an understanding of internal control over federal programs and test the controls over compliance for each major

[6]Insurance may cover part of these costs, but cyber insurance has spread among local governments only recently. According to Moody's Investors Service (2023), the share of U.S. local governments with cybersecurity insurance increased from 54% to 92% over the five years before 2023.

program (OMB, 2014e). Federal guidance for these audits lists computer controls among the control activities that support compliance, including access controls and computer general and security controls (OMB, 2013).[7] Audit reports can therefore include findings on information system controls. The 2020 Single Audit of the City of Avalon, California, for example, found that the city had no documented policies on IT logical security and that its password settings allowed passwords to go unchanged for up to a year (City of Avalon, California, 2020).

Auditors must report significant deficiencies and material weaknesses in internal control, material noncompliance with program requirements, and questioned costs (OMB, 2014g). For each finding, the government must prepare a corrective action plan and report the finding's status in subsequent audits (OMB, 2014c).[8] Single Audits, however, provide less assurance than audits of large public firms. Auditors report the weaknesses they find but do not express an opinion on whether internal control is effective (AICPA, 2020a; OMB, 2014f). The Government Accountability Office has also found persistent problems with the quality of Single Audits (GAO, 2007).

2.3. *Hypothesis Development*

2.3.1. *Data breaches and municipal borrowing costs*

A data breach can increase a municipality's borrowing costs because bondholders bear the downside of municipal finances but share little of the upside. When news increases default risk, which accounts for most of the yield spread on municipal bonds (Schwert, 2017), they demand higher yields on new issues (Baber et al., 2013). A breach can have this effect through two channels, one operating through default risk and the other through information risk (Huang and Wang, 2021). Under the default risk channel, a breach imposes costs that the budget did not anticipate. The costs of notifying residents and restoring

[7]Since 2014, the internal controls required of federal award recipients have also explicitly included reasonable measures to safeguard personally identifiable information (OMB, 2014a).

[8]The Federal Audit Clearinghouse makes these reports available to the public (OMB, 2014d).

systems, lost revenue, and legal settlements reduce the funds available for debt service, especially in governments with little fiscal slack (Section 2.1).

Under the information risk channel, a breach reveals weaknesses in internal controls that investors could not otherwise observe. These weaknesses are unlikely to be isolated. Because access controls and system software support control activities throughout an organization, a weakness that permits a breach is likely to affect other operations as well, including financial reporting (Lawrence et al., 2018). Investors may therefore expect further breaches and other control failures, such as misappropriated funds or misstated reports (Huang and Wang, 2021).[9]

2.3.2. *Pre-breach internal controls and the cost of a breach*

How much a breach raises borrowing costs is likely to depend on the strength of the municipality's internal controls before the breach. Investors cannot observe these controls directly and rely instead on noisy signals, the most systematic of which are Single Audit findings (Section 2.2). A report without findings can reflect either stronger controls or weaknesses that the audit did not detect. These findings can therefore shape the market's response to a breach in two opposite ways.

On the one hand, weaker controls can amplify the consequences of a breach. A government with weaker controls may be slower to detect and contain a breach and to restore its systems, which raises the cost of the breach. Many local governments lack the capacity to respond, commonly citing too few cybersecurity staff and an inability to pay

[9]There are also reasons to expect little or no effect. Municipal defaults are rare, and general obligation bonds are secured by the issuer's ability to raise taxes. Investors may also miss breach news, because municipal bond ownership is fragmented and breaches are not always covered in the news. Existing evidence on the consequences of breaches is mixed. Among firms, breach announcements reduce equity values only modestly on average (Richardson et al., 2019), but the losses are substantial when attacks compromise personal financial information or were initially withheld (Amir et al., 2018; Kamiya et al., 2021). Breached firms also lose customers (Akey et al., 2026), experience lower sales growth (Kamiya et al., 2021), and borrow on less favorable terms (Huang and Wang, 2021). Among local governments, Curti et al. (2024) and Osborne (2025) find that cyberattacks increase borrowing costs, and Andreadis et al. (2024) find the same, but only for attacks with media coverage. By contrast, Jensen and Paine (2023) find that borrowing costs decrease after ransomware attacks. In addition to the ambiguity about the sign of the effect, it is unclear whether findings based on cyberattacks extend to other breach categories.

competitive salaries as barriers to cybersecurity (Funk et al., 2019). For a municipality with Single Audit findings, a breach also signals that its control weaknesses may extend beyond grant compliance and financial reporting. For a municipality without findings, the same breach is more likely to look like an isolated incident. Consistent with this view, firms with control weaknesses manage their inventories less efficiently (Feng et al., 2015) and make worse acquisitions (Harp and Barnes, 2018), and municipalities with material weaknesses have higher borrowing costs (Park et al., 2017).

On the other hand, a breach may be a larger surprise when a municipality's controls appeared sound. Investors who relied on an audit report learn from the breach that weaknesses existed but went undetected. They may then revise their assessment of the municipality more sharply and place less weight on the audit's assurance about its other controls. Banks appear to update their assessments in this way. Huang and Wang (2021) find that banks respond more harshly to breaches at firms with a strong IT reputation, for which a breach is unexpected, but no more harshly to breaches at firms with previously reported control weaknesses. If bond investors behave similarly, a breach should raise borrowing costs at least as much for municipalities without Single Audit findings as for those with findings.

Information system controls require specialized expertise to design and monitor. State guidance for local officials notes that most managers "will need the help of a qualified IT professional to adequately assess the risks, design and monitor controls in a digital environment" (Office of the New York State Comptroller, 2016, p. 16). Because the Single Audit data classify findings only broadly and do not identify weaknesses in information system controls separately, we examine the staffing of IT professionals instead.

Because IT professionals identify vulnerabilities, monitor systems, and lead the response when an incident occurs, municipalities with IT staff should be better able to prevent breaches and limit their cost. Beyond strengthening these controls, recruiting IT professionals may signal to investors that a municipality takes data security seriously. We

therefore expect municipalities that posted IT job openings before a breach to experience smaller increases in borrowing costs.

2.3.3. *Do municipalities strengthen their controls after a breach?*

Municipalities have strong incentives to improve their internal controls after a breach. Once a breach has exposed control weaknesses to auditors and residents, officials can no longer claim to be unaware of them, and a subsequent breach would be harder to excuse. Remediation can also pay off in the bond market, because municipalities borrow repeatedly and investors may price future breaches less harshly once controls have been strengthened. Consistent with this logic, prior studies show that firms improve their internal controls after breaches and benefit from doing so. They post more job openings for cybersecurity workers (Bana et al., 2025), strengthen their governance even after breaches at peer firms (Ashraf, 2022), and remediate control weaknesses, which is followed by a lower cost of equity (Ashbaugh-Skaife et al., 2009) and more favorable loan terms (Huang and Wang, 2021).

There are several reasons why municipalities may not improve their internal controls. First, the costs of a breach and any increase in borrowing costs drain the funds a municipality would need to remediate. Remediation must then compete with public services for the remaining funds, and residents and elected officials tend to favor spending on public services. When discussing cybersecurity-related improvements, Moody's Investors Service (2023) warns that "expensive initiatives that require a shift in resources away from core services can become a credit challenge."

Second, local officials face little pressure to invest in controls. Residents have weak incentives to monitor officials, because they face collective-action and free-rider problems and often lack the time or expertise to interpret government financial statements (Zimmerman, 1977; Dagostino and Nakhmurina, 2026a). Officials, in turn, gain little from investing in controls. The benefits of stronger controls are hard to observe, and a subsequent breach

may not occur until after current officials have left office. Third, even municipalities that want to improve their controls may be unable to staff the effort. Local governments report that they cannot pay competitive salaries for cybersecurity personnel and lack trained staff, which makes it difficult to recruit the IT professionals that remediation requires (Funk et al., 2019). If these frictions outweigh the incentives to remediate, internal controls may not improve after a breach.

3. Data

We use several data sources in our analyses. The data breach sample comes from the Privacy Rights Clearinghouse (PRC). The primary market municipal bond characteristics are collected from the Mergent Municipal Bond Database (Mergent). We obtain municipality-level demographic characteristics and financial information from the Atlas Investment Research (Muni Atlas) and the Government Finance Database (GFD). Finally, we use Single Audit data from the Federal Audit Clearinghouse (FAC) to measure auditor-identified internal control weaknesses, and job postings data from Lightcast to measure municipalities' demand for IT professionals.

3.1. Data Breaches

We obtain a list of data breaches in the United States from Privacy Rights Clearinghouse (PRC), a nonprofit organization that aims to promote data privacy awareness.[10] PRC maintains a database of breach incidents that target businesses, educational institutions, government agencies, medical providers, and non-profit organizations. One important feature of this dataset is its focus on breaches that are publicly reported by media outlets, state authorities (e.g., Attorney Generals), and local government entities. While our sample may not contain a complete set of municipal breaches that have ever occurred, it concentrates

[10]For more information regarding PRC, see https://privacyrights.org/. For previous studies that also make use of PRC data, see, e.g., Florackis et al. (2023) and Liu (2025).

on large-scale, well-publicized breaches that are likely to influence municipal debt pricing and spending decisions.

For each breach incident, the PRC provides information on the name of the targeted entity, geographic location, the reported date (the date when the incident was first made public, which we also refer to as the breach announcement), breach type, an estimate of the total number of records affected, and a brief description of the incident.

We take several steps to clean the PRC data and identify breached municipalities. We outline these steps in the Online Appendix Table OA1. First, we obtain a comprehensive raw dataset from PRC, which has 29,176 breaches. We then filter the data to include only breaches affecting governmental organizations (as categorized by PRC) and remove duplicate entries. Using fuzzy matching and manual review, we identify breaches of municipalities in our Muni Atlas database, excluding federal, state, university, and special district entities. During this process, we discover and remove additional duplicates caused by misspellings of municipality names.

Focusing on the 2007–2017 period, our cleaned PRC sample has a total of 201 municipal data breaches across 39 states in the U.S. Among these breaches, about 42.8% took place in county governments, 46.3% in cities, and 10.9% in towns and villages.[11] Figure 1 plots the geographic distribution of municipal data breaches in the U.S. Breaches occur throughout the country, with clusters in large states such as California and New York. In Section 5.3, we discuss municipality-level characteristics that are correlated with the presence of data breaches.

To obtain the appropriate sample for the municipal bond analyses, we restrict the sample to issuers that had issued bonds in both the year preceding and the year following the reported breach, resulting in 87 breaches (Table OA2). This restriction ensures that we

[11]We limit our final sample to 2007-2017 for two reasons. First, although our version of PRC sample also includes municipal data breaches in 2018, we are concerned about data quality. The reported number of breaches in 2018 is much lower than previous years, and it does not cover large-scale cyberattacks, such as the one that happened in Atlanta. Second, our data on municipality-level characteristics from Muni Atlas ends in 2017 (see Section 3.3).

observe the borrowing costs of each breached municipality both before and after its breach. Our estimates therefore reflect changes in each municipality's own borrowing costs. A shift in which municipalities issue bonds after a breach cannot explain them. The one-year window on each side of the breach also limits the scope for unrelated events to drive these changes. This restriction allows us to attribute changes in borrowing costs more cleanly to the breach.

3.2. Municipal Bonds

Using data from Mergent Municipal, we focus on the primary municipal bond market, where price-setting demand comes from sophisticated investors who track issuer-specific credit news (Cuny et al., 2026). We focus on fixed-coupon and tax-exempt bonds issued between 2006 and 2018. This sample covers longer periods than the PRC sample (2007–2017) to ensure our ability to implement a stacked difference-in-differences design and use a window of [-1,1] years around each event (breach).[12] For each bond issued, we retain a variety of characteristics, such as the bond CUSIP, offering yield, offering amount, times to maturity, coupon rate, General Obligation (GO) status, callable status, insured status, and average bond credit ratings (converted to numerical ratings) from three rating providers: Moody's, Fitch, and S&P.

To compute municipal bond spreads, we obtain the Municipal Market Advisors (MMA) yield curve data from Bloomberg. For specific maturities where the MMA yield is not available, we estimate the MMA yield using linear interpolation. We then calculate bond spreads as the difference between the offering yields and the maturity-matched par yield from the MMA AAA-rated curve as of the dated date of issuance.

[12] See Section 4.1 for details.

3.3. *Municipality Demographics and Financial Information*

We obtain each municipality's name and 6-digit CUSIP from Muni Atlas, along with its annual demographic and economic characteristics: population, per capita income, per capita debt, poverty rate, unemployment rate, median age, and the share of residents without a high school education.

Additionally, we collect detailed data on municipalities' revenues and expenditures from the Government Finance Database (GFD), which cleans and processes data directly from the U.S. Census Bureau (Pierson et al., 2015).[13] GFD keeps track of detailed amounts that local governments receive from their revenue sources (e.g., property taxes, utility revenues, interest revenues), as well as the amounts that they spend on various functions (e.g. public safety, public welfare, utilities, etc). GFD covers 2007 to 2017, but Muni Atlas begins in 2008. To align the coverage periods, we linearly extrapolate the Muni Atlas characteristics to 2007. Following the Census survey methodology, GFD reports values only every five years for most municipalities, which tend to be small. To avoid sampling biases, we linearly interpolate the GFD data.[14] GFD also records zero expenditures for some municipality-years. A zero can reflect missing data rather than actual zero spending. Some services, such as education, may also be funded by special districts, such as school districts, rather than by general-purpose governments. In our analysis of expenditures, we therefore include only observations with positive spending.

We take several steps to process and combine the data samples. After matching the names of entities in PRC with the issuer names in Muni Atlas, we obtain the corresponding 6-digit issuer CUSIPs. To get a sample of municipal bonds issued by local governments, we merge with the Mergent bond sample using the 6-digit CUSIPs. Next, to obtain a municipality-by-year panel of characteristics, we merge the Muni Atlas sample with the

[13] For more information regarding GFD, see https://willamette.edu/mba/research-impact/public-datasets/index.html.

[14] For most municipalities, GFD data are available in 2007, 2012, and 2017. Therefore, we linearly interpolate values for the rest of the years within this period.

GFD sample by issuer names. Finally, the sample of bonds issued by local governments is merged with the sample of municipality-by-year characteristics using issuer names.

3.4. Single Audits

We use Single Audit (SA) reports from the Federal Audit Clearinghouse (FAC). We manually match entity names in the SA data with the list of local governments in our sample. Each report indicates whether the auditor identified significant deficiencies or material weaknesses in internal control, material noncompliance with program requirements, or questioned costs. We classify a municipality as having Single Audit findings in a year if any of its reports for that year contains any of these findings. Because the SA data do not have a separate variable for weaknesses in information system controls, we refer to these findings as general internal control weaknesses. Tables 5 and OA2 label municipalities with and without findings as having weaker and stronger general internal controls.

3.5. Job Postings

Because the SA data do not identify weaknesses in information system controls separately, we measure these controls through municipalities' demand for IT professionals (Section 2.3.2), using job postings data from Lightcast (previously Burning Glass). We focus on postings by local government agencies, because our goal is to measure demand for staff who can protect and manage the government's data. We use a combination of fuzzy matching and manual inspection to identify postings in Lightcast made by our sample local governments. We classify a posting as an IT posting if Lightcast assigns it to 1) the broad category (variable name "bgtcareerareaname") of "Information Technology," and 2) the sub-category (variable name "bgtoccgroupname") of any one of the following: "Database Specialists," "IT managers," "Network and System Engineering," "Network and Systems Support," or "Software Development". For each year, we code a municipality as having IT hiring demand if it posted at least one IT job. When we split municipalities by IT hiring,

we include only municipalities that posted at least one job of any kind in Lightcast during the sample period (Section 6.2).

4. Empirical Methodology

In this section, we describe our empirical approach and explain how we estimate the effect of data breaches on municipal borrowing costs. We then present summary statistics of key variables used in our main sample.

4.1. Stacked Difference-in-Differences

The data breaches in our sample occur at different times (i.e., municipalities are "treated" on a staggered schedule) throughout the sample period. To examine the implications of these breaches on municipal costs of debt, we employ a stacked difference-in-differences estimation, following the methodology of Gormley and Matsa (2011). A key advantage of this approach is that it treats each cohort as a separate sub-experiment and ensures that only municipalities that are "never-treated" serve as control units. This design helps avoid biases caused by heterogeneous treatment effects in traditional TWFE models (Baker et al., 2022). In our setting, the control units in each cohort are municipalities that issue bonds within the specified event window but never experience any data breaches during the sample period.

Specifically, we consider an event window of two years (one year before the reported date of each breach and one year after) and estimate the following regression:

$$Y_{c,i,j,t} = \alpha + \beta * Treated_{c,i} \times Post_{c,t} + \gamma * Controls + \lambda_{c,i} + \delta_{c,t} + \eta_{j,r} + \epsilon_{c,i,j,t} \qquad (1)$$

where c is cohort, i is municipality, j is bond, t is the offering year, and r is each level of the average bond rating. The dependent variable in the baseline analysis is municipal

bonds' offering yield spreads. $Treated_{c,i}$ equals 1 if the bonds are issued by the breached municipality in each cohort, and 0 if otherwise. $Post_{c,t}$ equals 1 for any bonds that are issued within 1 year after the reported date of the data breach in each cohort, and 0 if otherwise.

To further sharpen our identification, we control for several bond-level and municipality-level characteristics. At the bond level, we include a bond's coupon rate, the natural logarithm of issuance size, maturity, and indicators for whether the bond is callable, general obligation (GO), and insured. At the municipality level, we control for the natural logarithm of population and the natural logarithm of income per capita. $\lambda_{c,i}$ is the cohort-by-municipality fixed effects, which removes time-invariant municipality characteristics within each cohort. $\delta_{c,t}$ is the cohort-by-offering year fixed effects, which accounts for common time trends. $\eta_{j,r}$ is the average bond credit rating fixed effects, which allows us to compare bonds with the same rating levels. Following Cengiz et al. (2019), we cluster standard errors at the cohort $\times$ municipality level.

Effectively, for each cohort, we estimate the treatment effect by comparing the changes in yield spreads of the bonds issued by breached versus never-breached municipalities, before and after the breach is reported. We then aggregate the treatment effects from cohorts to arrive at the overall treatment effect, which is captured by β in Equation (1). β measures the impact of data breaches on municipalities' costs of debt. A positive and statistically significant β would indicate that data breaches raise affected municipalities' borrowing costs in the primary bond market.

4.2. Summary Statistics

After constructing valid cohorts for our stacked difference-in-differences framework, our final sample consists of 429,776 unique bonds issued by 7,761 unique local governments between 2006 and 2018.

Table 1 Panel A reports the summary statistics of the main variables used in our

baseline specifications. The average bond has an offering yield of 2.652% and a yield spread of 0.232%. On average, it pays a coupon rate of 3.337%, features an issuance size of $0.398 million, and has a maturity of 8.762 years. Approximately 75% of sample bonds are GO bonds, 41% are callable, and 21% are insured. The average issuing municipality in our sample has a population of 32,468 and an income per capita of $27,778.

5. Data Breaches and Municipal Costs of Debt

In this section, we first examine the impact of data breaches on the financing costs of local governments in the primary municipal bond market. Next, we estimate the dynamic treatment effects and perform a series of robustness tests. Lastly, we examine whether the effect differs between external cyberattacks and insider breaches.

5.1. Baseline Results

We begin by examining the relationship between data breaches and municipal borrowing costs, as measured by offering yield spreads.

Table 2 reports the results from estimating Equation (1), with offering yield spreads as the dependent variable. Across specifications (with different control variables and fixed effects), the offering yield spreads of bonds issued by breached municipalities increase, on average, by 5.2 to 7.4 basis points within one year after a breach is reported, relative to comparable bonds from never-breached municipalities. This increase is economically large, amounting to 22% to 32% of the average offering yield spread of 23.2 basis points in the full stacked sample (Table 1, Panel A).

5.2. *Dynamic Treatment Effects*

To examine the timing of the effect, we estimate the following dynamic specification:

$$Y_{c,i,j,t} = \alpha + \sum_{s=-3,\, s\neq 0}^{4} \beta_s (Treated_{c,i} \times \rho_s) + \gamma * Controls + \lambda_{c,i} + \delta_{c,t} + \eta_{j,r} + \epsilon_{c,i,j,t}, \qquad (2)$$

where each ρ_s is an indicator variable that equals 1 for a specific quarter within the two-year event window. We use the most recent quarter before the data breach reported date as the benchmark period $(s = 0)$.[15]

Figure 2 illustrates the coefficients of interest, β_s. Before the reported date of data breaches, the yield spreads of newly issued bonds are statistically indistinguishable between breached and never-breached municipalities, consistent with parallel trends before the breach. However, starting from the second quarter after news of the breach becomes public, municipalities subject to data breaches experience a significant rise in yield spreads, which remains elevated for at least two quarters. The increase in borrowing costs thus emerges only after the breach becomes public.

5.3. *Robustness*

We conduct two analyses to check the robustness of our baseline results. First, we examine whether our results depend on how we measure borrowing costs. Our baseline measure, the yield spread, depends on the MMA benchmark curve, which we interpolate for maturities that MMA does not report (Section 3.2). Offering yields measure borrowing costs directly, without a benchmark. We re-estimate Equation (1) with offering yields as the dependent variable. Our results are robust to this alternative measure. Offering yields

[15] Muni Atlas data begin in 2008, and we extrapolate them by only one year, to 2007, to align them with the other data sources (Section 3.3). Including municipality-level characteristics as controls therefore drops bonds issued in 2006, which is why columns 4 and 5 of Table 2 have fewer observations than columns 1 to 3. The baseline estimate changes little when we add these controls. In untabulated tests, we also extrapolate log population and log per capita income to 2006 and include them as controls. Our results remain robust. We therefore include only bond-level controls in this specification and in all later analyses of yield spreads.

of breached municipalities increase by 5.0 to 11.0 basis points relative to never-breached municipalities, comparable to the baseline increase in spreads (Table OA3).

Second, we address the concern that breaches do not occur randomly across municipalities. If certain municipal characteristics make breaches more likely, these characteristics, rather than the breaches themselves, could drive the increase in borrowing costs. Table 3 compares breached and never-breached municipalities along observable socio-economic characteristics. On average, breached municipalities have larger populations, higher per capita income, higher poverty and unemployment rates, and younger and less educated residents. They also have higher per capita debt, although their per capita deficits are similar to those of never-breached municipalities.

To account for these differences, we use propensity score matching (PSM). We estimate the probability of a breach from all characteristics in Table 3 and match each breached municipality with 30 never-breached municipalities based on this probability. We then re-estimate Equation (1) on the matched sample. Offering yield spreads of breached municipalities increase by 4.9 to 8.4 basis points, similar to the baseline estimates (Table OA4). Breached municipalities thus pay higher borrowing costs even when compared with otherwise similar municipalities.

5.4. Types of Breaches

We next test whether the effect of a breach on borrowing costs differs across the breach types described in Section 2.1. Insiders are responsible for 76% of the breaches in our sample: 60% stem from insider carelessness and 16% from insider offenses (Table OA2). Cyberattacks by outsiders and breaches of unknown type account for the remaining 24%.

We re-estimate Equation (1) separately for each breach type in both the full sample and the PSM sample. The results are shown in Table 4. In both samples, insider offenses are associated with the largest increase in offering yield spreads, of 8.0 to 11.1 basis points (34% to 48% of the sample mean). Insider carelessness is associated with an increase of

6.0 to 7.1 basis points (26% to 31%). The estimates for cyberattacks are positive but not statistically significant in either sample.[16] The concentration of the effect in insider breaches is consistent with the information risk channel. Lost devices, misdirected records, and employee misconduct point to failures of routine controls. A successful cyberattack is a noisier signal of control quality, because sophisticated attackers can also breach well-designed controls (Section 2.2).

6. Pre-Breach Internal Controls and the Cost of a Breach

In this section, we examine whether the increase in borrowing costs documented in Section 5 varies with the strength of a municipality's internal controls before the breach. We measure control strength in two ways, through Single Audit findings and through demand for IT professionals (Section 3).

6.1. General Internal Controls

Under the information risk channel, the cost of a breach should depend on the strength of a municipality's internal controls before the breach. Weaker controls can amplify the cost, because the government is slower to contain the breach and the breach suggests broader weaknesses. Alternatively, a breach can be more costly for a municipality whose audits revealed no weaknesses, because investors did not expect it.

We re-estimate Equation (1) separately for municipalities with and without Single Audit findings in the year before the breach (Section 3.4). Table 5 presents the results. Among municipalities with findings, offering yield spreads increase by 8.6 basis points after a breach, or 37% of the sample mean (column 2). Among municipalities without findings, the estimate is close to zero and not statistically significant (column 1). The

[16] Our estimate for cyberattacks differs from the increases in borrowing costs found by other studies (Curti et al., 2024; Andreadis et al., 2024; Osborne, 2025). These papers focus exclusively on cyberattacks, feature a larger sample of cyberattacks, and use different empirical approaches. We attribute the difference to these factors.

difference between the two estimates is not statistically significant at conventional levels (Wald test $p = 0.107$).

The pattern favors the first prediction, that weaker controls amplify the cost of a breach, although the difference between the two groups is imprecisely estimated. It also suggests that investors find a Single Audit without findings informative, because a breach at such a municipality is not associated with higher borrowing costs. This result differs from the corporate evidence in Huang and Wang (2021), who find that banks respond more harshly to breaches at firms with a strong IT reputation. In the municipal setting, the result is consistent with evidence that bonds are more costly for issuers with material weaknesses in internal control, through higher markups (Gore et al., 2023) and higher borrowing costs (Park et al., 2017; Edmonds et al., 2023).

6.2. Information System Internal Controls

Single Audit data do not have a separate variable for weaknesses in information system controls. We therefore measure the quality of these controls through municipalities' demand for IT professionals. Municipalities that recruit IT professionals should be better prepared to detect and contain a breach. We expect breaches to increase their borrowing costs by less.

We re-estimate Equation (1) separately for municipalities with and without IT job postings in the year before the breach. Table 6 presents the results. Among municipalities without IT postings, offering yield spreads increase by 20.8 basis points after a breach, or 90% of the sample mean (column 2). Among municipalities with IT postings, the estimate is close to zero and not statistically significant (column 1). The difference between the two estimates is statistically significant at the 10% level (Wald test $p = 0.070$). These results suggest that investors view municipalities that recruit IT professionals as better prepared to contain a breach.

7. Data Breaches and Municipalities' Responses

In this section, we examine how local governments respond to data breaches by assessing changes in their internal controls and spending. We first test whether breached municipalities strengthen their controls. We then examine whether breaches tighten the budgets of municipalities with weaker controls, one of the frictions that can prevent them from strengthening their controls (Section 2.3).

7.1. Data Breaches and Internal Controls Quality

The increase in borrowing costs after a breach is concentrated in municipalities with weaker internal controls. These municipalities therefore have strong incentives to strengthen their controls. Several frictions, however, may prevent them from doing so (Section 2.3). If breached municipalities strengthen their controls, we should observe fewer Single Audit findings and more IT job postings after the breach.

To test this, we estimate the following regression, using an event window of four years before and after the year in which the breach is reported:

$$Y_{c,i,t} = \alpha + \beta * Treated_{c,i} \times Post_{c,t} + \gamma * Controls + \lambda_{c,i} + \delta_{c,t} + \epsilon_{c,i,t}, \tag{3}$$

where c denotes cohort, i denotes municipality, and t denotes year. We consider two dependent variables: an indicator for Single Audit findings and an indicator for IT hiring demand (Section 3). $Treated_{c,i}$ equals 1 for the breached municipality in cohort c and 0 otherwise. $Post_{c,t}$ equals 1 for observations up to four years after the breach is reported and 0 otherwise. We control for the natural logarithms of population, per capita income, per capita debt, and total revenues, as well as the poverty rate. $\lambda_{c,i}$ denotes cohort-by-municipality fixed effects, which absorb time-invariant municipality characteristics within each cohort. $\delta_{c,t}$ denotes cohort-by-year fixed effects, which absorb common shocks. We cluster standard errors at the cohort $\times$ municipality level.

Table 7 presents the results. Perhaps surprisingly, we find no evidence that breached municipalities strengthen their internal controls, despite their incentives to do so. The probability of Single Audit findings does not decrease after a breach (column 1). There is weak evidence of an increase in the demand for IT professionals (column 2). However, the dynamic estimates in Figure 3 show an upward trend in IT hiring demand that begins before the breach, and this trend likely had little to do with data breaches. None of the estimates after the breach is statistically significant. Together, the two measures suggest that breached municipalities strengthen neither their general internal controls nor their information system controls.[17]

7.2. Data Breaches and Municipal Expenditures

A breach can strain a municipality's finances. Beyond the direct costs of responding to the incident, breached municipalities with weaker internal controls face higher borrowing costs (Section 6). Tighter budgets may leave these municipalities without the funds needed to strengthen their controls. If so, they should reduce their spending after a breach.

To test this prediction, we build a stacked sample of municipalities with Single Audit findings in the year before a data breach, because these municipalities experience the largest increase in borrowing costs (Table 5). Our event window spans one year before and four years after each breach, which allows us to capture any longer-horizon shifts in expenditure decisions. Specifically, we estimate Equation (3) with the dependent variables defined as $100 \times$ (expenditures / total revenues) in a given year, so that the coefficients can be interpreted as percentage point changes.[18]

Table 8 displays the results. After a breach, the ratio of total expenditures to total

[17] In our analysis, we define the treatment year as the year in which the breach is first publicly reported. Municipalities may, however, become aware of an incident prior to disclosure and begin adjusting internal and information system controls in advance. To assess this possibility, Figure OA1 shifts the treatment year one year earlier (using the year before the reported breach as the benchmark). The results remain robust to this alternative timing assumption.

[18] Our results are robust if we use logs of $1 +$ the ratios as the dependent variables.

revenues of municipalities with Single Audit findings decreases by 3.6 percentage points (column 1).[19] This decrease is consistent with breaches tightening municipal budgets. Panel A of Figure 4 presents the dynamic estimates for total expenditures. These estimates turn negative two years after the breach, consistent with the municipal budget cycle, in which budgets are adopted months before the fiscal year begins (Morgan et al., 2017).[20]

Tighter budgets can explain why internal controls do not improve only if the cuts reach the offices that perform these controls. We therefore examine the two Census expenditure categories that record spending on these offices at the government-wide level (U.S. Census Bureau, 2006). The first, financial administration, covers the offices of the auditor, comptroller, and treasurer, along with central accounting and central data processing. This category spans both types of controls we study: accounting and auditing for general internal controls, and central data processing for information system controls. The second, central staff services, covers the office of the chief executive and central personnel administration. These offices perform government-wide executive and administrative functions, including recruiting the municipality's staff. Spending on both categories decreases after a breach (Table 8). The ratio of spending on financial administration to total revenues decreases by 0.145 percentage points (column 3). The corresponding ratio for central staff services decreases by 0.161 percentage points (column 2). These decreases equal 5.8% and 4.6% of the respective sample means (Table 1, Panel B). Panels B and C of Figure 4 show the same timing as total spending. The pre-breach estimates for both categories are not statistically significant. The estimates turn negative two years after the breach and are statistically significant in the third and fourth years.

The decline in spending on administrative functions suggests that tighter budgets may explain why the internal controls of these municipalities do not improve after a breach.

[19] Because the outcomes are scaled by total revenues, a decline can also reflect an increase in revenues.

[20] In Figure OA2, we again address the concern that municipalities may learn of an incident prior to public disclosure and begin responding immediately by adjusting expenditures. We increase the event window to [-2,4] and shift the treatment year one year earlier (using the year before the reported breach as the benchmark). The results remain robust to this alternative window and timing specification.

8. Conclusion

Residents have little choice but to entrust their most sensitive data to their local governments. Understanding the costs of data breaches is therefore a fundamental question for local governments and their residents. The question is especially timely now that federal support for local cybersecurity is shrinking. This paper examines how a breach affects a municipality's borrowing costs and how this effect depends on the strength of its internal controls. Within a year of a breach, offering yield spreads on the municipality's new bonds increase by 5.2 to 7.4 basis points, or 22% to 32% of the sample mean, relative to comparable bonds of never-breached municipalities.

The increase is largest after insider breaches, which point to failures of internal controls. Borrowing costs increase more for municipalities whose internal controls were weaker before the breach, whether we measure control quality by Single Audit findings or by the absence of IT job postings. Despite these costs, breached municipalities do not appear to strengthen their internal controls afterward. Instead, those with pre-existing internal control weaknesses reduce their spending, including spending on financial administration and central staff services. One interpretation is that financial constraints keep these municipalities from investing in better controls.

Municipalities with weaker controls may thus be caught in a downward spiral. A breach increases their borrowing costs and strains their budgets. Tighter budgets, in turn, make it harder to fund the controls that could prevent the next breach. As a result, these municipalities remain exposed to future breaches and to further increases in their borrowing costs.

These findings suggest a role for outside support, particularly as federal funding recedes. Programs that help municipalities with weaker controls fund internal controls and data security could relieve the budget pressure that appears to hold such investments back. We caution, however, that our evidence is associational. Future research could examine whether stronger controls reduce the cost of a breach and which forms of support are most

effective.

References

AICPA, 2020a. PCAOB Standards and Related Rules: 2019. John Wiley & Sons.

AICPA, 2020b. Single audit fundamental series part 3: Understanding and testing compliance requirements and internal control over compliance.

Akey, P., Lewellen, S., Liskovich, I., Schiller, C., 2026. Hacking corporate reputations. Review of Finance 30, 795–862.

Amir, E., Levi, S., Livne, T., 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. Review of Accounting Studies 23, 1177–1206.

Andreadis, L., Kalotychou, E., Louca, C., Lundblad, C. T., Makridis, C., 2024. From bits to bonds: The economic ripple of local cyberattacks on municipalities. Kenan Institute of Private Enterprise Research Paper .

Arghire, I., 2023. City of Dallas details ransomware attack impact, costs. SecurityWeek, September 25 https://www.securityweek.com/city-of-dallas-details-ransomware-attack-impact-costs/.

Ashbaugh-Skaife, H., Collins, D. W., Kinney Jr., W. R., LaFond, R., 2009. The effect of SOX internal control deficiencies on firm risk and cost of equity. Journal of Accounting Research 47, 1–43.

Ashraf, M., 2022. The role of peer events in corporate governance: Evidence from data breaches. The Accounting Review 97, 1–24.

Baber, W. R., Gore, A. K., Rich, K. T., Zhang, J. X., 2013. Accounting restatements, governance and municipal debt financing. Journal of Accounting and Economics 56, 212–227.

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

Baltimore Sun, 2019. Estimates put Baltimore's ransomware recovery at $18.2M. Government Technology, May 30 https://www.govtech.com/security/estimates-put-baltimores-ransomware-recovery-at-18-2-m.html.

Bana, S., Brynjolfsson, E., Jin, W., Steffen, S., Wang, X., 2025. Human capital acquisition in response to data breaches. MIS Quarterly 49, 367–388.

Cengiz, D., Dube, A., Lindner, A., Zipperer, B., 2019. The effect of minimum wages on low-wage jobs. The Quarterly Journal of Economics 134, 1405–1454.

Cheng, S. F., De Franco, G., Lin, P., 2023. Marijuana liberalization and public finance: A capital market perspective on the passage of medical use laws. Journal of Accounting and Economics 75, 101516.

Chordia, T., Jeung, J., Pati, A., 2022. Biased expectations and default risk in the municipal bond market. Available at SSRN .

City of Avalon, California, 2020. Single audit report for the fiscal year ended June 30, 2020.

Cornaggia, J., Cornaggia, K. J., Israelsen, R., 2023. Rating agency fees: pay to play in public finance? The Review of Financial Studies 36, 2004–2045.

Cornaggia, J., Cornaggia, K. J., Israelsen, R. D., 2018. Credit ratings and the cost of municipal financing. The Review of Financial Studies 31, 2038–2079.

COSO, 2013. Internal control – integrated framework. Tech. rep., Committee of Sponsoring Organizations of the Treadway Commission.

Cuny, C., 2018. When knowledge is power: Evidence from the municipal bond market. Journal of Accounting and Economics 65, 109–128.

Cuny, C., Duguay, R., Li, K., Nakhmurina, A., Watts, E. M., 2026. Tipped off: Information leakage in the municipal securities market. Available at SSRN 7541603 .

Cuny, C., Li, K., Nakhmurina, A., Watts, E. M., 2025. Muni disclosure: All talk and no trade? Journal of Accounting and Economics p. 101797.

Curti, F., Ivanov, I., Macchiavelli, M., Zimmermann, T., 2024. City hall has been hacked! The financial costs of lax cybersecurity. Available at SSRN 4465071 .

Dagostino, R., Nakhmurina, A., 2026a. Monitoring public promises: Municipal debt and retirement security. Working paper, Pension Research Council, The Wharton School, University of Pennsylvania.

Dagostino, R., Nakhmurina, A., 2026b. Partisan cities: How state–local political alignment shapes credit risk and information processing in the municipal bond market. Journal of Accounting Research 64, 1733–1770.

Dambra, M., Even-Tov, O., Naughton, J. P., 2023. The economic consequences of gasb financial statement disclosure. Journal of Accounting and Economics 75, 101555.

Deloitte, 2020. Nascio: State of state it.

Dougal, C., Gao, P., Mayew, W. J., Parsons, C. A., 2019. What's in a (school) name? racial discrimination in higher education bond markets. Journal of Financial Economics 134, 570–590.

Edmonds, C. T., Leece, R. D., Vermeer, B. Y., Vermeer, T. E., 2023. The role of adverse outcomes in municipal debt costs. Advances in Accounting 63, 100671.

Feng, M., Li, C., McVay, S. E., Skaife, H., 2015. Does ineffective internal control over financial reporting affect a firm's operations? evidence from firms' inventory management. The Accounting Review 90, 529–557.

Florackis, C., Louca, C., Michaely, R., Weber, M., 2023. Cybersecurity risk. The Review of Financial Studies 36, 351–407.

Funk, K., Martin, C., DuPuis, N., Shark, A., Bowen, D., 2019. Protecting our data: What cities should know about cybersecurity. National League of Cities pp. 2019–10.

GAO, 2007. Single audit quality: Actions needed to address persistent audit quality problems. Tech. rep., Government Accountability Office.

Gao, P., Lee, C., Murphy, D., 2019. Municipal borrowing costs and state policies for distressed municipalities. Journal of Financial Economics 132, 404–426.

Goldsmith-Pinkham, P., Gustafson, M. T., Lewis, R. C., Schwert, M., 2023. Sea-level rise exposure and municipal bond yields. The Review of Financial Studies 36, 4588–4635.

Gore, A. K., Henderson, B. J., Ji, Y., 2023. Do municipal bond prices reflect internal control quality? Available at SSRN 2772605 .

Gormley, T. A., Matsa, D. A., 2011. Growing out of trouble? corporate responses to liability risk. The Review of Financial Studies 24, 2781–2821.

Harp, N. L., Barnes, B. G., 2018. Internal control weaknesses and acquisition performance. The Accounting Review 93, 235–258.

Hobson, J. L., Mayew, W. J., Peecher, M. E., Venkatachalam, M., 2017. Improving experienced auditors' detection of deception in CEO narratives. Journal of Accounting Research 55, 1137–1166.

Huang, H. H., Wang, C., 2021. Do banks price firms' data breaches? The Accounting Review 96, 261–286.

IBM Security, 2024. Cost of a data breach report.

Jensen, J., Paine, F., 2023. Municipal cyber risk.

Johns, T., 2026. Foster City declares emergency after cyberattack forces city computer system offline for days. ABC7 News, March 24 https://abc7news.com/post/foster-city-declares-emergency-cyberattack-forces-computer-system-offline-days/18759516/.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., Stulz, R. M., 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics 139, 719–749.

Kim, Y., Su, L., Zhang, M., Zhang, V., 2026. Local government transparency and financing costs. Working paper .

Lawrence, A., Minutti-Meza, M., Vyas, D., 2018. Is operational control risk informative of financial reporting deficiencies? AUDITING: A Journal of Practice & Theory 37, 139–165.

Li, B., Li, Y., Pittman, J., Wang, W., 2026. Auditors' response to clients' cyber breaches: A human-capital perspective. Contemporary Accounting Research Forthcoming.

Li, B., Venkatachalam, M., 2025. Do audited financial reports mitigate (or exacerbate) stock market crashes? Available at SSRN 5812662 .

Li, L., Weng, L., Su, L. N., Zeng, C. C., 2024. Documenting the undocumented: The impact of employment verification mandates on government borrowing costs. Northeastern U. D'Amore-McKim School of Business Research Paper .

Liu, L. Y., 2025. Financial statement audits and data breaches. Management Science 71, 6340–6366.

Lu, R., Ye, Z., 2023. Roe v. rates: Reproductive healthcare and public financing costs. SocArXiv. September 1.

Moody's Investors Service, 2023. Evolving cyber landscape challenges municipalities to keep up with risk. Sector in-depth, local government – US, Moody's Investors Service.

Morgan, D., Robinson, K. S., Strachota, D., Hough, J. A., 2017. Budgeting for Local Governments and Communities. Routledge.

National Association of Counties, 2026. Reauthorize the State and Local Cybersecurity Grant Program. NACo, July 17 https://www.naco.org/resource/reauthorize-state-and-local-cybersecurity-grant-program.

OCCM, 2025. Office of the comptroller commonwealth of massachusetts: Cybersecurity responsibilities. https://www.macomptroller.org/ctr-cyber/cybersecurity-responsibilities/ .

Office of the New York State Comptroller, 2016. Local government management guide: Management's responsibility for internal controls.

Ogneva, M., Subramanyam, K. R., Raghunandan, K., 2007. Internal control weakness and cost of equity: Evidence from sox section 404 disclosures. The Accounting Review 82, 1255–1297.

OMB, 2003. Revision to OMB circular A-133, "audits of states, local governments, and non-profit organizations".

OMB, 2013. OMB circular A-133 compliance supplement, part 6: Internal control.

OMB, 2014a. Uniform administrative requirements, cost principles, and audit requirements for federal awards, 2 CFR 200.303: Internal controls.

OMB, 2014b. Uniform administrative requirements, cost principles, and audit requirements for federal awards, 2 CFR 200.501: Audit requirements.

OMB, 2014c. Uniform administrative requirements, cost principles, and audit requirements for federal awards, 2 CFR 200.511: Audit findings follow-up.

OMB, 2014d. Uniform administrative requirements, cost principles, and audit requirements for federal awards, 2 CFR 200.512: Report submission.

OMB, 2014e. Uniform administrative requirements, cost principles, and audit requirements for federal awards, 2 CFR 200.514: Scope of audit.

OMB, 2014f. Uniform administrative requirements, cost principles, and audit requirements for federal awards, 2 CFR 200.515: Audit reporting.

OMB, 2014g. Uniform administrative requirements, cost principles, and audit requirements for federal awards, 2 CFR 200.516: Audit findings.

ONYSC, 2016. Local government guide: The practice of internal controls. Office of the New York State Comptroller .

Osborne, B. N., 2025. The Financial and Societal Costs of Institutional Data Breaches: Evidence from Government and Hospital Breaches. Ph.D. thesis, University of Tennessee.

Painter, M., 2020. An inconvenient cost: The effects of climate change on municipal bonds. Journal of Financial Economics 135, 468–482.

Park, Y. J., Matkin, D. S. T., Marlowe, J., 2017. Internal control deficiencies and municipal borrowing costs. Public Budgeting & Finance 37, 88–111.

Phiel, S., 2026. Clark County will pay for data breach. The Columbian, April 2 https://www.camaspostrecord.com/news/2026/apr/02/clark-county-will-pay-for-data-breach/.

Pierson, K., Hand, M. L., Thompson, F., 2015. The government finance database: A common resource for quantitative research in public financial analysis. PloS one 10, e0130119.

Richardson, V. J., Smith, R. E., Watson, M. W., 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. Journal of Information Systems 33, 227–265.

Ruan, Z., Venkatachalam, M., Xie, X., Zhang, V., 2025. Externalities from forcing hospitals to audit: Evidence from the Single Audit Act. Available at SSRN 5222877 .

Schoenfeld, J., 2024. Cyber risk and voluntary service organization control (soc) audits. Review of Accounting Studies 29, 580–620.

Schwert, M., 2017. Municipal bond liquidity and default risk. The Journal of Finance 72, 1683–1722.

Security Magazine, 2026. Taxpayers may pay up to $25,000 to address county data breach. Security Magazine, October 26 https://www.securitymagazine.com/articles/102692-taxpayers-may-pay-up-to-25-000-to-address-county-data-breach.

Shasta County, 2026. Private data breach notification. Shasta County, July https://www.shastacounty.gov/county-administrative-office/page/private-data-breach-notification-july-2026.

U.S. Census Bureau, 2006. Government finance and employment classification manual.

Vijayan, J., 2009. NYPD faces ID theft risk after data stolen from pension fund. Computerworld, March 5 https://www.computerworld.com/article/1559749/nypd-faces-id-theft-risk-after-data-stolen-from-pension-fund.html.

Wallace, W. A., 1981. Internal control reporting practices in the municipal sector. The Accounting Review 56, 666–689.

Wood, C., 2025. CISA confirms it's ending MS-ISAC support. StateScoop, September 29 https://statescoop.com/cisa-confirms-its-ending-ms-isac-support/.

Zhang, V., 2024. Municipal bond credit rating access and retail investors' transaction costs. The Accounting Review 99, 427–453.

Zhou, F., Huang, J., 2024. Cybersecurity data breaches and internal control. International Review of Financial Analysis 93, 103174.

Zimmerman, J. L., 1977. The municipal accounting maze: An analysis of political incentives. Journal of Accounting Research 15, 107–144.

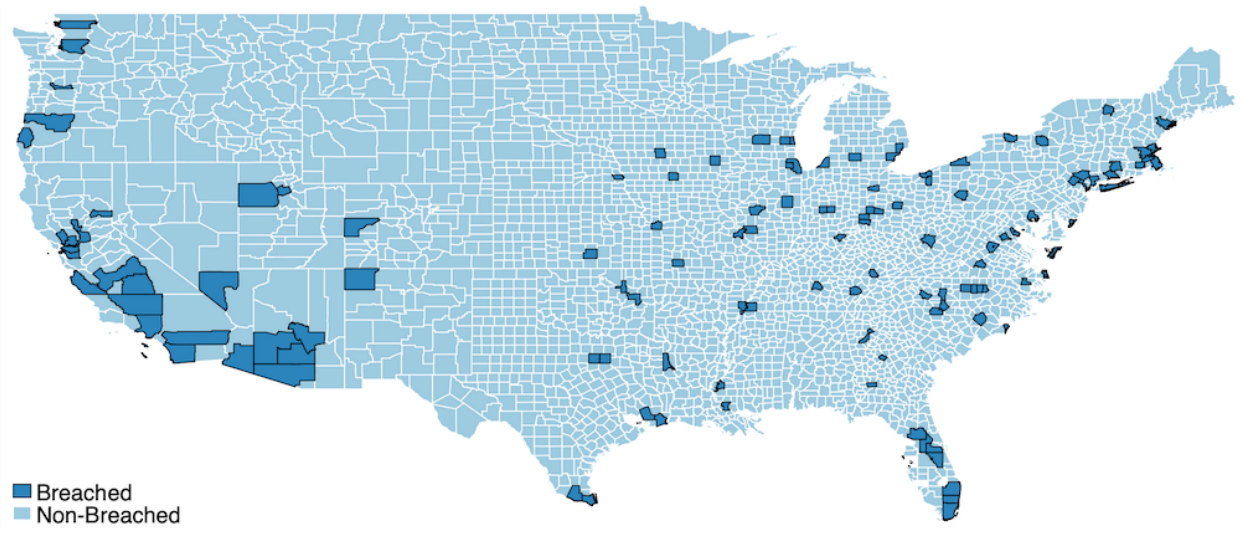


Fig. 1 Municipal Data Breaches by Geographic Location. This figure presents the geographic distribution of municipal data breaches in our cleaned PRC sample. The sample period is 2007–2017. Darker blue marks counties in which at least one municipality experienced a data breach during the sample period.

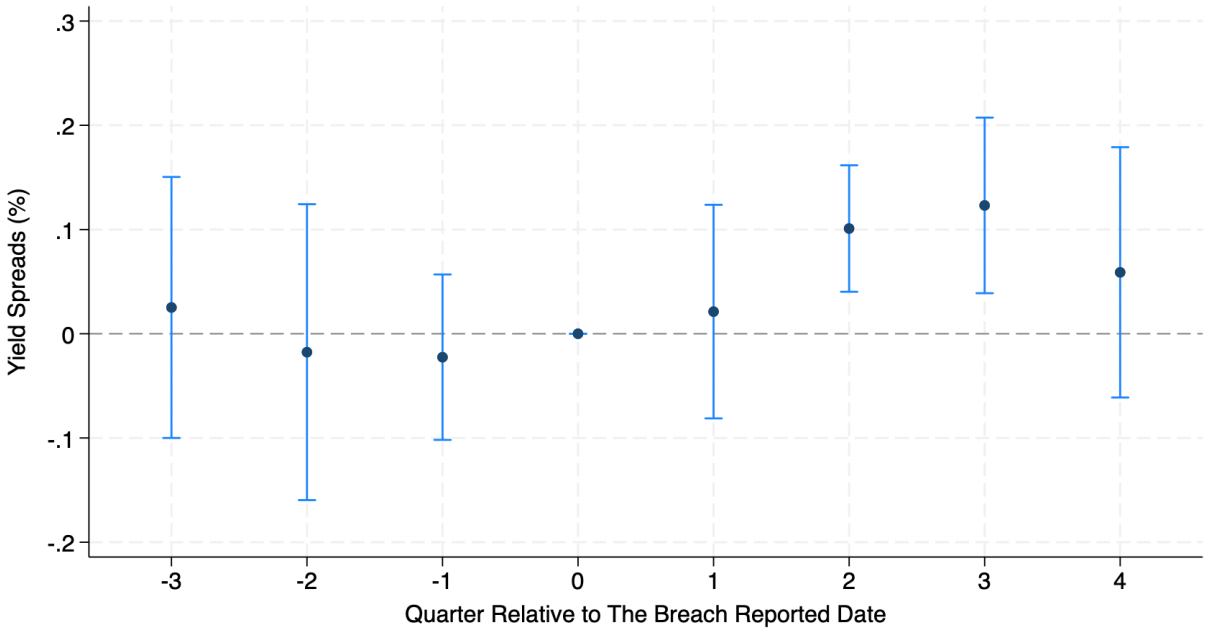
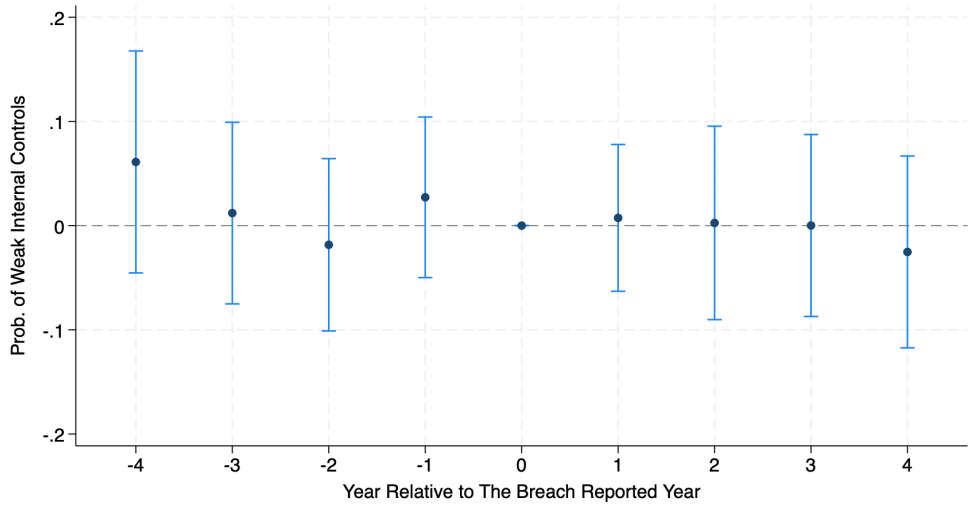
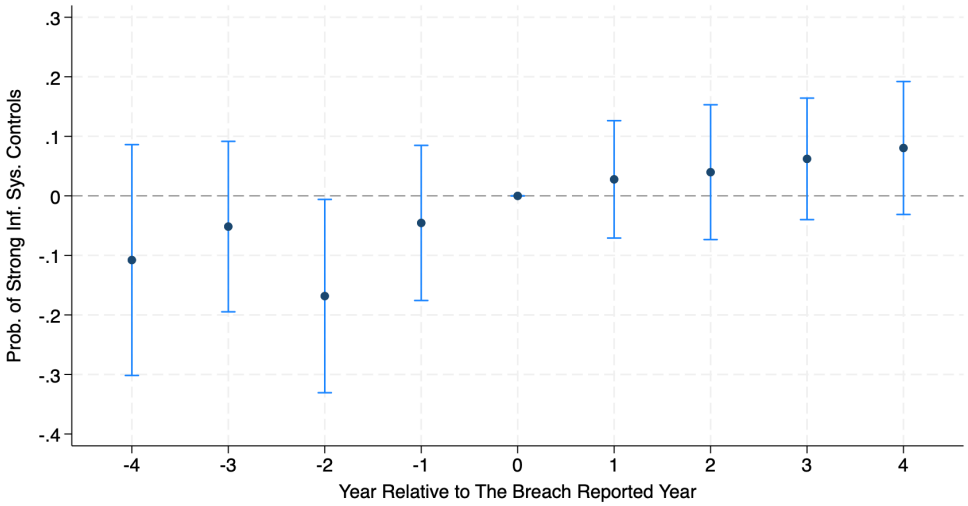


Fig. 2 Dynamic Treatment Effects of Municipal Data Breaches on Municipal Bond Offering Yield Spreads. This figure presents the dynamic treatment effects of municipal data breaches on municipal bond offering yield spreads. Breaches are reported in 2007–2017, and bonds are issued in 2006–2018. Each cohort contains bonds issued by the breached (treated) municipality and never-breached (control) municipalities within $[-1, 1]$ years around the reported date of the data breach. Each dot is the β_s coefficient estimate from Equation (2). The bar around each dot indicates the 95% confidence interval. Quarters are periods of roughly 90 days relative to the reported date of the data breach. Quarter 0 covers the 90 days before the reported date and serves as the benchmark. Quarter 1 covers the first 90 days after it.

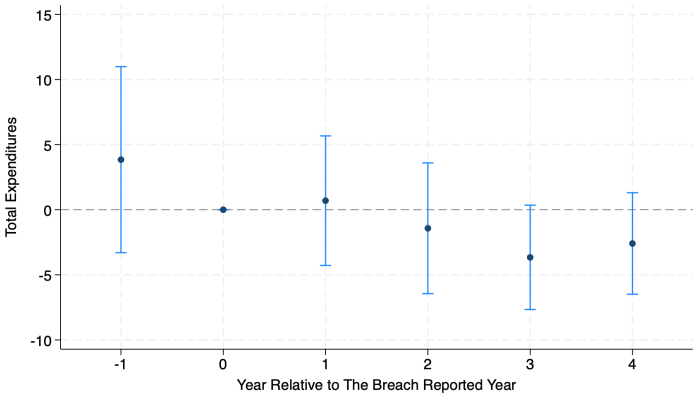


(**a**) Probability of Weaker General Internal Controls

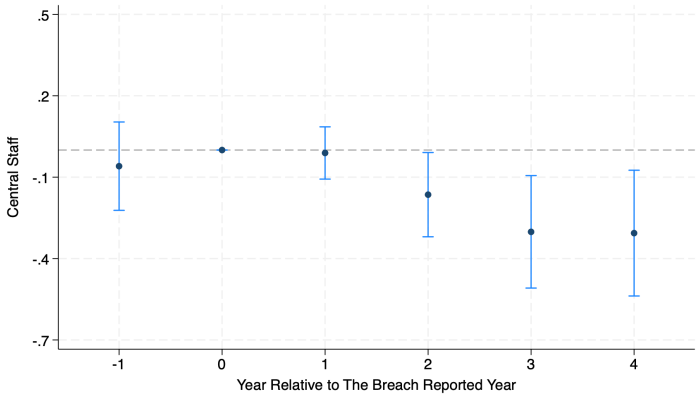


(**b**) Probability of Stronger Information System Controls

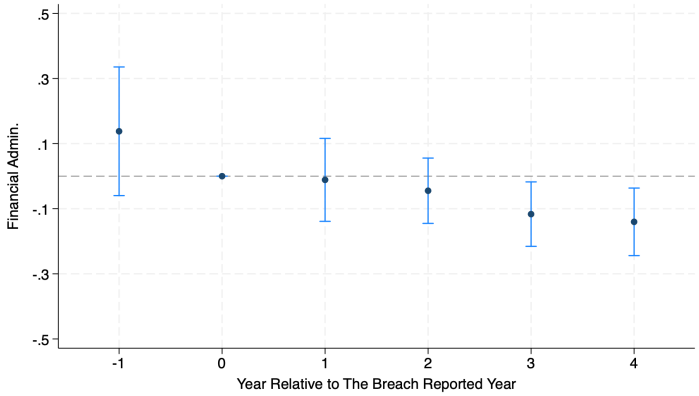
Fig. 3 Dynamic Treatment Effects of Municipal Data Breaches on Internal Control Quality. This figure presents the dynamic treatment effects of municipal data breaches on the quality of municipal internal controls and information system controls. The sample period is 2007–2017. The event window is $[-4, 4]$ years around the reported year of the data breach. In (a), the dependent variable is an indicator variable that equals 1 if the municipality has general internal control weaknesses identified in its Single Audit (SA) reports in a given year, and 0 otherwise. In (b), the dependent variable is an indicator variable that equals 1 if the municipality has at least one job posting related to IT in a given year, and 0 otherwise. The bar around each dot indicates the 95% confidence interval. The coefficient estimate for the reported year of the data breach is used as the benchmark.



(**a**) Total Expenditures



(**b**) Central Staff Services



(**c**) Financial Administration

Fig. 4 Dynamic Treatment Effects of Municipal Data Breaches on Municipalities' Expenditures. This figure presents the dynamic treatment effects of municipal data breaches on municipalities' expenditures. Breaches are reported in 2008–2016. The sample consists of municipalities with general internal control weaknesses identified in their Single Audit (SA) reports prior to the breach. The event window is $[-1, 4]$ years around the reported year of the data breach. Each dependent variable is 100 $\times$ the corresponding expenditures scaled by total revenues. The bar around each dot indicates the 95% confidence interval. The coefficient estimate for the reported year of the data breach is used as the benchmark.

Table 1
Summary Statistics of Key Variables

Panel A: Full Bond Sample

Variable	Obs	Mean	Std. Dev.	P25	P50	P75
Spread (%)	4,268,454	0.232	0.371	-0.010	0.160	0.400
Offering Yield (%)	4,268,454	2.652	1.232	1.600	2.700	3.700
GO	4,268,454	0.749	0.434	0.000	1.000	1.000
Coupon Rate (%)	4,268,454	3.337	1.079	2.500	3.400	4.000
Log (Offering Amount)	4,268,454	12.893	1.251	12.101	12.848	13.688
Maturity (Years)	4,268,454	8.762	5.517	4.236	7.973	12.277
Callable	4,268,454	0.416	0.493	0.000	0.000	1.000
Insured	4,268,454	0.210	0.408	0.000	0.000	0.000
Average Bond Rating	4,268,454	13.704	8.234	0.000	18.000	19.000
Log (Population)	3,980,025	10.388	1.677	9.291	10.321	11.459
Log (Per Capita Income)	3,980,025	10.232	0.344	9.996	10.188	10.436

Panel B: Municipalities with Weaker General Internal Controls

Variable	Obs	Mean	Std. Dev.	P25	P50	P75
Total Revenues ($000)	798,718	124,055	242,836	17,809	45,815	114,816
Total Expenditures ($000)	798,718	128,922	250,215	19,198	48,743	119,472
Central Staff Services (%)	785,986	3.483	3.560	1.101	2.269	4.494
Financial Administration (%)	756,347	2.498	2.084	1.106	1.850	3.224

This table reports summary statistics of bond- and municipality-level characteristics. Panel A focuses on the full stacked bond sample, which includes bonds issued in 2006–2018 around breaches reported in 2007–2017. Panel B focuses on the stacked sample consisting of municipalities with general internal control weaknesses identified in their Single Audit (SA) reports prior to breaches reported in 2008–2016. In Panel B, "Central Staff Services" and "Financial Administration" are the corresponding expenditures as a percentage of total revenues. "Average Bond Rating" is the average of the available numerical ratings from Moody's, Fitch, and S&P, which range from 1 (C or D) to 21 (AAA). Unrated bonds are coded 0. All continuous variables are winsorized at the 1st and 99th percentiles.

Table 2
Data Breaches and Municipal Bond Offering Yield Spreads

	(1) Spread	(2) Spread	(3) Spread	(4) Spread	(5) Spread
Treated × Post	0.052*	0.061**	0.074***	0.061**	0.072***
	[0.0266]	[0.0246]	[0.0236]	[0.0294]	[0.0271]
GO		-0.144***	-0.120***	-0.150***	-0.123***
		[0.0024]	[0.0021]	[0.0025]	[0.0022]
Coupon Rate		0.014***	0.012***	0.014***	0.012***
		[0.0006]	[0.0006]	[0.0006]	[0.0006]
Log (Offering Amount)		-0.014***	-0.011***	-0.013***	-0.011***
		[0.0004]	[0.0004]	[0.0004]	[0.0004]
Maturity		0.005***	0.005***	0.005***	0.005***
		[0.0001]	[0.0001]	[0.0001]	[0.0001]
Callable		-0.023***	-0.023***	-0.026***	-0.026***
		[0.0006]	[0.0006]	[0.0007]	[0.0006]
Insured		-0.084***	-0.116***	-0.072***	-0.108***
		[0.0031]	[0.0029]	[0.0035]	[0.0033]
Log (Population)				-0.070***	-0.056**
				[0.0270]	[0.0258]
Log (Per Capita Income)				-0.145***	-0.127***
				[0.0270]	[0.0257]
Cohort-Year FE	Yes	Yes	Yes	Yes	Yes
Cohort-Municipality FE	Yes	Yes	Yes	Yes	Yes
Bond Rating FE	No	No	Yes	No	Yes
Observations	4,268,454	4,268,454	4,268,454	3,979,829	3,979,829
Adjusted R^2	0.724	0.737	0.749	0.739	0.752

This table reports the impact of municipal data breaches on municipal bond offering yield spreads in the full sample. Breaches are reported in 2007–2017, and bonds are issued in 2006–2018. Each cohort contains bonds issued by the breached (treated) municipality and never-breached (control) municipalities within $[-1, 1]$ years around the reported date of the data breach. The dependent variable is the municipal bond offering yield spread, in percentage points. See Sections 3 and 4 for details on variable definitions and sample construction. In all specifications, cohort-by-year and cohort-by-municipality fixed effects are included. Standard errors, reported in brackets, are clustered at the cohort-by-municipality level. Levels of significance are presented as follows: *p<0.1; **p<0.05; ***p<0.01.

Table 3
Summary Statistics: Breached vs. Never-Breached Municipalities

	(1) Never-Breached	(2) Breached	(3) Difference	(4) T-stat
Log (Population)	9.120	12.162	-3.042***	-30.124
Log (Per Capita Income)	10.125	10.171	-0.046**	-2.085
Poverty Rate (%)	12.785	16.635	-3.849***	-6.917
Unemployment Rate (%)	6.401	7.483	-1.082***	-4.393
Median Age	38.955	35.639	3.316***	11.721
Below High School Rate (%)	10.055	13.478	-3.423***	-6.569
Log (Per Capita Debt)	8.735	8.960	-0.225***	-5.098
Deficit Per Capita ($)	99.966	95.918	4.048	0.122

This table reports the mean values of municipality-level characteristics for breached (treated) and never-breached (control) municipality-year observations. Column (3) reports the difference between the means in columns (1) and (2), and column (4) reports the t-statistic for the test that this difference is zero. The sample period is 2007–2017. Municipality-level characteristics are collected from Muni Atlas and the Government Finance Database (GFD). Levels of significance are presented as follows: *p<0.1; **p<0.05; ***p<0.01.

Table 4
Data Breaches and Municipal Bond Offering Yield Spreads: Breach Types

Dep. Var: Yield Spread	(1) Full Sample	(2) PSM Sample
Cyberattacks	0.012	0.064
Insider Offense	0.111***	0.080***
Insider Carelessness	0.071***	0.060**

This table reports the impact of municipal data breaches on municipal bond offering yield spreads by breach type. Breaches are reported in 2007–2017, and bonds are issued in 2006–2018. The dependent variable is the municipal bond offering yield spread. Each cell reports the coefficient β on "Treated $\times$ Post" from a separate estimation of Equation (1) for one breach type. Column (1) uses the full sample, and column (2) uses the PSM sample (Section 5.3). Bond-level characteristics are included as control variables, together with cohort-by-year, cohort-by-municipality, and bond rating fixed effects. "Cyberattacks" refers to incidents in which local government agencies are hacked by an outside party or infected by malware. "Insider Offense" refers to incidents in which employees or contractors within local government agencies deliberately steal or misuse sensitive data. "Insider Carelessness" refers to incidents in which employees within local government agencies lose physical devices or accidentally disclose sensitive data. Breaches of unknown type are excluded. Levels of significance are presented as follows: *p<0.1; **p<0.05; ***p<0.01.

Table 5
Data Breaches and Municipal Bond Offering Yield Spreads: General Internal Controls

Dep. Var: Yield Spread	(1) Stronger General Internal Controls		(2) Weaker General Internal Controls
Treated × Post	-0.010		0.086***
	[0.0540]		[0.0233]
Bond Controls	Yes		Yes
Cohort-Year FE	Yes		Yes
Cohort-Municipality FE	Yes		Yes
Bond Rating FE	Yes		Yes
Wald test p-value		0.107	
Observations	1,317,064		1,280,568
Adjusted R^2	0.734		0.745

This table reports the results of subsample analyses based on general internal control quality. Breaches are reported in 2007–2017, and bonds are issued in 2006–2018. The dependent variable is the municipal bond offering yield spread. The "Stronger General Internal Controls" sample includes bonds issued by municipalities that had no internal control weaknesses in their Single Audit (SA) reports in the year prior to the breach. The "Weaker General Internal Controls" sample includes bonds issued by municipalities that had internal control weaknesses in their SA reports in the year prior to the breach. Municipalities without an SA report in that year are excluded. In all specifications, bond-level characteristics are included as control variables. Cohort-by-year, cohort-by-municipality, and bond rating fixed effects are included. The p-value of the Wald test on the difference between the subsample coefficients is reported. Standard errors, reported in brackets, are clustered at the cohort-by-municipality level. Levels of significance are presented as follows: *p<0.1; **p<0.05; ***p<0.01.

Table 6
Data Breaches and Municipal Bond Offering Yield Spreads: IS Internal Controls

Dep. Var: Yield Spread	(1) Stronger IS Internal Controls		(2) Weaker IS Internal Controls
Treated × Post	0.001		0.208**
	[0.0412]		[0.1042]
Bond Controls	Yes		Yes
Cohort-Year FE	Yes		Yes
Cohort-Municipality FE	Yes		Yes
Bond Rating FE	Yes		Yes
Wald test p-value		0.070	
Observations	465,753		1,654,196
Adjusted R^2	0.730		0.730

This table reports the results of subsample analyses based on information system (IS) internal control quality. The sample period is 2007–2017. The dependent variable is the municipal bond offering yield spread. The "Stronger IS Internal Controls" sample includes bonds issued by municipalities that had at least one job posting related to IT in the year prior to the breach. The "Weaker IS Internal Controls" sample includes bonds issued by municipalities that had no job posting related to IT in the year prior to the breach. Both samples include only municipalities that posted at least one job of any kind in Lightcast during the sample period. In all specifications, bond-level characteristics are included as control variables. Cohort-by-year, cohort-by-municipality, and bond rating fixed effects are included. The p-value of the Wald test on the difference between the subsample coefficients is reported. Standard errors, reported in brackets, are clustered at the cohort-by-municipality level. Levels of significance are presented as follows: *p<0.1; **p<0.05; ***p<0.01.

Table 7
Data Breaches and Internal Control Quality

Dep. Var:	(1) Prob. of Weaker General Internal Controls	(2) Prob. of Stronger IS Internal Controls
Treated × Post	-0.015	0.104**
	[0.0302]	[0.0424]
Controls	Yes	Yes
Cohort-Year FE	Yes	Yes
Cohort-Municipality FE	Yes	Yes
Observations	3,544,517	1,038,059
Adjusted R^2	0.503	0.399

This table reports the impact of municipal data breaches on the quality of internal controls. The sample period is 2007–2017. The event window is $[-4, 4]$ years around the reported year of the data breach. In column (1), the dependent variable is an indicator variable that equals 1 if the municipality has general internal control weaknesses identified in its Single Audit (SA) reports in a given year, and 0 otherwise. In column (2), the dependent variable is an indicator variable that equals 1 if the municipality has at least one job posting related to IT in a given year, and 0 otherwise. In all specifications, municipality-level characteristics are included as control variables. Cohort-by-year and cohort-by-municipality fixed effects are included. Standard errors, reported in brackets, are clustered at the cohort-by-municipality level. Levels of significance are presented as follows: *p<0.1; **p<0.05; ***p<0.01.

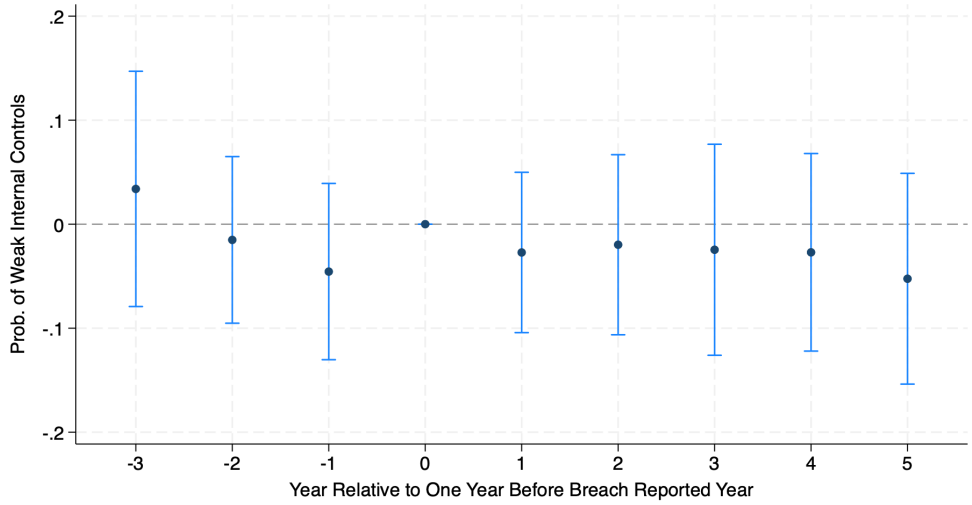
Table 8
Data Breaches and Municipalities' Expenditures: Weaker General Internal Controls Sample

Dep. Var:	(1) Total Expenditures	(2) Central Staff Services	(3) Financial Administration
Treated × Post	-3.606**	-0.161**	-0.145**
	[1.5706]	[0.0711]	[0.0595]
Controls	Yes	Yes	Yes
Cohort-Year FE	Yes	Yes	Yes
Cohort-Municipality FE	Yes	Yes	Yes
Observations	798,718	785,986	756,347
Adjusted R^2	0.550	0.842	0.858

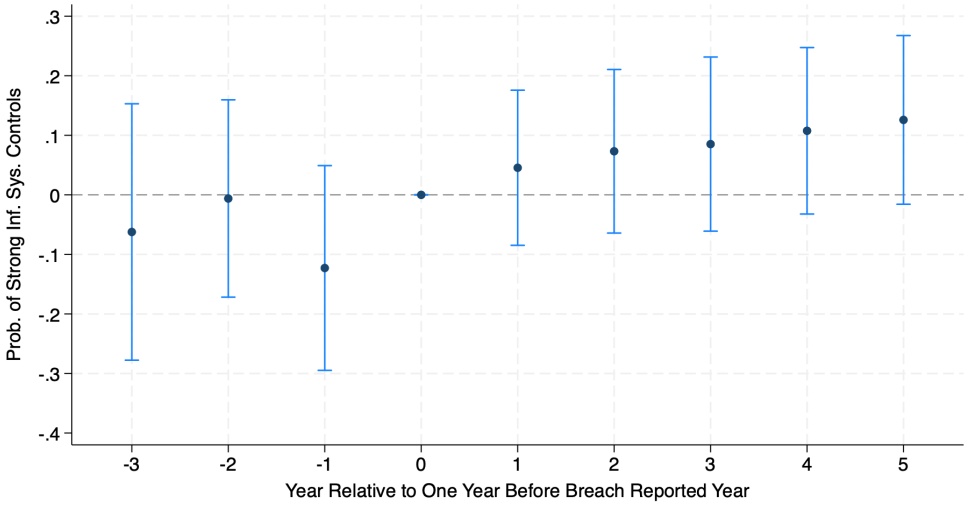
This table reports the impact of municipal data breaches on municipalities' expenditures. Breaches are reported in 2008–2016. The sample consists of municipalities with general internal control weaknesses identified in their Single Audit (SA) reports prior to the breach. The event window is $[-1, 4]$ years around the reported year of each data breach. The dependent variables are 100 × expenditures scaled by total revenues. Each specification includes only observations in which the corresponding dependent variable is positive, and controls for municipality-level characteristics as well as cohort-by-year and cohort-by-municipality fixed effects. Standard errors, reported in brackets, are clustered at the cohort-by-municipality level. Levels of significance are presented as follows: *p<0.1; **p<0.05; ***p<0.01.

Online Appendix to

Government Data Breaches, Internal Controls, and Municipal Borrowing Costs

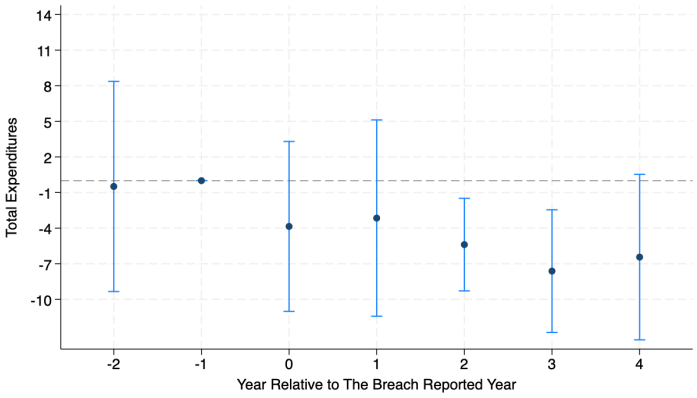


(**a**) Probability of Weaker General Internal Controls

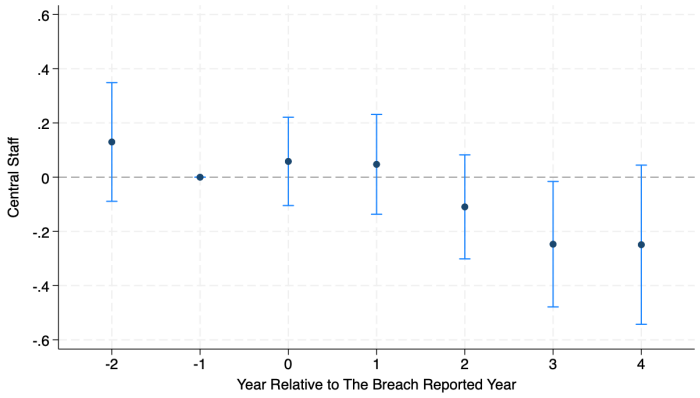


(**b**) Probability of Stronger Information System Controls

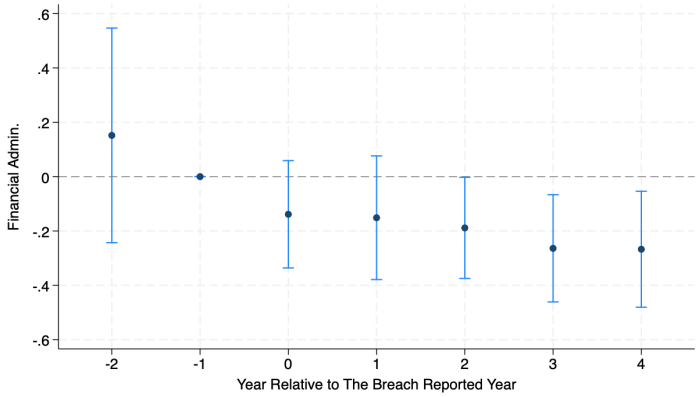
Fig. OA1 Dynamic Treatment Effects of Municipal Data Breaches on Internal Control Quality (Different Benchmark Period) This figure presents the dynamic treatment effects of municipal data breaches on the quality of municipal internal controls and information system controls. The sample period is 2007-2017. The event window is [-4,4] years around the reported year of the data breach. In (a), the dependent variable is an indicator variable that equals 1 if municipalities have general internal control weaknesses (as identified in SA reports), 0 if otherwise. In (b), the dependent variable is an indicator variable that equals 1 if municipalities have at least one job posting related to IT, 0 if otherwise. The bar around each dot indicates the 95% confidence interval. The coefficient estimate for the year preceding the reported year of the data breach is used as the benchmark.



(**a**) Total Expenditures



(**b**) Central Staff Services



(**c**) Financial Administration

Fig. OA2 Dynamic Treatment Effects of Municipal Data Breaches on Municipalities' Expenditures (Different Window and Benchmark Period). This figure presents the dynamic treatment effects of municipal data breaches on municipalities' expenditures. The sample period is 2007-2017. The sample consists of municipalities with internal control weaknesses prior to the breach (as identified in SA reports). The event window is [-2,4] years around the reported year of the data breach. Each dependent variable is 100 $\times$ the corresponding expenditures scaled by the total revenues. The bar around each dot indicates the 95% confidence interval. The coefficient estimate for the year preceding the reported year of the data breach is used as the benchmark.

Table OA1
Data Breach Sample Construction

Step	(1) Procedure	(2) # of Data Breaches
1	PRC raw samples	29,176
2	Keep breaches related to local government entities, remove duplicated breaches, and fuzzy match with Muni Atlas data	339
3	Keep breaches that were reported between 2007 and 2017	201
4	Keep breaches that occurred in local governments with valid municipal bond issuance data within one year around the reported date	87

This table reports the procedures taken to clean and construct the municipal data breach sample. For each step, column (1) contains a short description of the procedure, and column (2) contains the number of data breaches at the end of the corresponding procedure.

Table OA2
Summary Statistics of Data Breaches

Number of Breaches	(1) Full Sample	(2) Stronger General Internal Controls	(3) Weaker General Internal Controls
Cyberattacks	19	3	15
Insider Offense	14	4	10
Insider Carelessness	52	16	35
Unknown	2	0	2
Total	87	23	52

This table reports the number of municipal data breaches by breach type. The sample period is 2007-2017. Column (1) focuses on the full bond sample. Column (2) and Column (3) focus on subsamples of bonds issued by municipalities with stronger and weaker general internal controls in the year prior to the breach (as identified in SA reports). "Cyberattacks" refers to incidents in which local government agencies are hacked by an outside party or infected by malware. "Insider Offense" refers to incidents in which employees or contractors of local government agencies deliberately steal or misuse sensitive data. "Insider Carelessness" refers to incidents in which employees within local government agencies lose physical devices or accidentally disclose sensitive data. "Unknown" refers to incidents in which the nature of data leakage is not clear.

Table OA3
Data Breaches and Municipal Bond Offering Yield

	(1) Offering Yield	(2) Offering Yield	(3) Offering Yield	(4) Offering Yield	(5) Offering Yield
Treated × Post	0.050	0.095**	0.110**	0.078	0.092*
	[0.0550]	[0.0475]	[0.0482]	[0.0485]	[0.0472]
GO		-0.098***	-0.075***	-0.102***	-0.076***
		[0.0028]	[0.0026]	[0.0030]	[0.0028]
Coupon Rate		0.265***	0.262***	0.247***	0.244***
		[0.0012]	[0.0011]	[0.0011]	[0.0011]
Log (Offering Amount)		-0.095***	-0.092***	-0.089***	-0.086***
		[0.0007]	[0.0007]	[0.0007]	[0.0007]
Maturity		0.122***	0.122***	0.129***	0.129***
		[0.0002]	[0.0002]	[0.0002]	[0.0002]
Callable		0.163***	0.161***	0.160***	0.159***
		[0.0013]	[0.0013]	[0.0013]	[0.0013]
Insured		-0.081***	-0.115***	-0.072***	-0.109***
		[0.0036]	[0.0037]	[0.0041]	[0.0041]
Log (Population)				-0.114***	-0.103***
				[0.0291]	[0.0287]
Log (Per Capita Income)				-0.077**	-0.068**
				[0.0320]	[0.0312]
Cohort-Year FE	Yes	Yes	Yes	Yes	Yes
Cohort-Municipality FE	Yes	Yes	Yes	Yes	Yes
Bond Rating FE	No	No	Yes	No	Yes
Observations	4,268,454	4,268,454	4,268,454	3,979,829	3,979,829
Adjusted R^2	0.501	0.904	0.905	0.907	0.908

This table reports the impact of municipal data breaches on municipal bond offering yield in the full sample. The sample period is 2007-2017. Each cohort contains bonds issued by the breached (treated) municipality and never-breached (control) municipalities within [-1,1] years around the reported date of the data breach. The dependent variable is the municipal bond offering yield. See Section 3 and 4 for details on variable definition and sample construction. In all specifications, cohort-by-year and cohort-by-municipality fixed effects are included. The standard errors are clustered at the cohort-by-municipality level. Levels of significance are presented as follows: *p<0.1; **p<0.05; ***p<0.01.

Table OA4
Data Breaches and Municipal Bond Offering Yield Spreads: PSM Sample

	(1) Spread	(2) Spread	(3) Spread	(4) Spread	(5) Spread
Treated × Post	0.049**	0.063***	0.068***	0.075***	0.084***
	[0.0213]	[0.0220]	[0.0183]	[0.0244]	[0.0194]
GO		-0.218***	-0.151***	-0.225***	-0.153***
		[0.0165]	[0.0128]	[0.0166]	[0.0131]
Coupon Rate		0.012***	0.004	0.013***	0.005
		[0.0038]	[0.0036]	[0.0039]	[0.0036]
Log (Offering Amount)		-0.011***	-0.006**	-0.011***	-0.007**
		[0.0030]	[0.0028]	[0.0032]	[0.0029]
Maturity		0.008***	0.008***	0.009***	0.008***
		[0.0008]	[0.0008]	[0.0008]	[0.0007]
Callable		0.018***	0.018***	0.016***	0.017***
		[0.0063]	[0.0059]	[0.0060]	[0.0055]
Insured		-0.070***	-0.109***	-0.052*	-0.099***
		[0.0240]	[0.0182]	[0.0269]	[0.0210]
Log (Population)				1.209***	1.088***
				[0.4120]	[0.3518]
Log (Per Capita Income)				-1.143**	-1.611***
				[0.5517]	[0.4471]
Cohort-Year FE	Yes	Yes	Yes	Yes	Yes
Cohort-Municipality FE	Yes	Yes	Yes	Yes	Yes
Bond Rating FE	No	No	Yes	No	Yes
Observations	97,940	97,940	97,940	91,991	91,991
Adjusted R^2	0.628	0.679	0.737	0.684	0.746

This table reports the impact of municipal data breaches on municipal bond offering yield spreads in a propensity score matching (PSM) sample. The sample period is 2007-2017. For each breached (treated) municipality, we match it with 30 never-breached (control) municipalities based on propensity scores produced using characteristics from Table 3 prior to breaches. Each cohort contains bonds issued by the breached (treated) municipality and matched never-breached (control) municipalities within [-1,1] years around the reported date of the data breach. The dependent variable is the municipal bond offering yield spreads. See Section 3 and 4 for details on variable definition and sample construction. In all specifications, cohort-by-year and cohort-by-municipality fixed effects are included. The standard errors are clustered at the cohort-by-municipality level. Levels of significance are presented as follows: *p<0.1; **p<0.05; ***p<0.01.