Do Banks Price Firms' Data Breaches?

ABSTRACT:

This paper studies the financial consequences of a reported data breach for bank loan terms. Using a staggered difference-in-differences approach with treatment and control samples matched by data breach propensity, we find that firms that have reported data breaches face higher loan spreads and their loans are more likely to require collateral and demand more covenants. The effects are more pronounced when the data breach involves criminal activities or the loss of a large number of records, or when the breached firm belongs to certain industries or has a high IT reputation. Moreover, using the introduction of state mandatory data breach notification laws as an exogenous shock, we find that the negative effect of data breaches on bank loan terms is more significant after these laws took effect. Our evidence also suggests that breached firms that take more remedial actions following the breach incident receive less unfavorable loan terms.

JEL Classifications: G10, G12

Keywords: data breaches; bank loan terms; loan spreads; collateral; covenants.

Do Banks Price Firms' Data Breaches?

I. INTRODUCTION

This paper investigates the effect of data breaches on firms' bank loan terms. In this digital era, big data is continuously reshaping industries. Annually, firms spend $36 billion collecting, storing, and analyzing large amounts of customer data (Columbus 2014). These datasets are highly valuable to firms and give them a competitive edge. However, electronic systems are susceptible to breaches. In the last decade, as customer data grew and became more valuable, the incidence and cost of data breaches have escalated correspondingly (Ponemon Institute 2017). Firms affected by data breaches incur substantial financial costs including direct costs (e.g., costs associated with detection, notification, remedial activities, and legal obligations) and indirect costs (e.g., loss of brand image, customer trust, business, and market share) (Romanosky, Hoffman, and Acquisti 2014; Martin, Borah, and Palmatier 2017; Ponemon Institute 2017; Rosati et al. 2017; Gwebu, Wang, and Wang 2018; SEC 2018).[1]

The reported cost of a data breach typically does not include the increased cost of capital (e.g., Ponemon Institute 2017).[2] However, the present value of the additional capital contracting costs due to data breaches can be substantial for a firm and may dwarf the known direct costs. We explore this issue in the context of bank loans—a major source of corporate financing (Bradley and Roberts 2015). Based on the framework provided by Duffie and Lando (2001), we reason that a data breach can affect a firm's bank loan contracting mainly through two channels: default risk

[1] For instance, Equifax revealed in September 2017 that hackers had breached its database and stolen the personal data of nearly 146 million people. Equifax recognized a one-time charge of $87.5 million related to this data breach. Its earnings were negatively affected because customers were dissatisfied. The company was hit with 240 class-action lawsuits in the US and Canada as a result of the data breach. In July 2019, Equifax reached a settlement with the federal and state regulators to pay affected customers up to $700 million in compensation (LaCroix 2017).

[2] It is possible for firms to purchase insurance to cover potential data breach costs, but the insurance is highly unlikely to cover the indirect costs such as the increase in the cost of capital as illustrated in this paper (Kopp, Kaffenberger, and Jenkinson 2017).

and information risk. First, direct costs and indirect costs (e.g., reputation loss) lead to lower and more volatile earnings, thereby increasing the default risk. Second, increased information risk also leads to unfavorable bank loan terms. Banks, as creditors, rely on information generated by borrowers' internal information system to assess their health and viability (Graham, Li, and Qiu 2008; Drucker and Puri 2009; Costello and Wittenberg-Moerman 2011; Kim, Song, and Stratopoulos 2018). Data breaches could indicate weak operational control risk and a poor internal information system (Lawrence, Minutti-Meza, and Vyas 2018; Smith, Higgs, and Pinsker 2019; Li, No, and Boritz 2020). Consequently, we expect banks to perceive breached firms as having a higher information risk and thus to offer them less favorable loan terms.

Our sample consists of 139 reported data breach events from 2005 to 2014 and 1,081 bank loans of US public firms from 2003 to 2016. We start by examining the effect of these data breach events on bank loan terms. One might argue that any change in bank loan terms following these data breaches was simply driven by a contemporaneous market-wide trend in bank loan terms. In addition, a firm's characteristics can simultaneously determine the likelihood of its becoming a data breach target and its bank loan terms, leading to a spurious association between the two. To mitigate these concerns, we use a difference-in-differences (DID) approach to compare changes in bank loan terms between breached firms and control firms matched using propensity score matching (PSM). Specifically, we use the first-stage Probit regression to generate a control sample with characteristics similar to those of the treatment sample. In the second stage, we employ the staggered DID design (Bertrand and Mullainathan 1999a; 1999b; 2003; Low 2009; Armstrong, Balakrishnan, and Cohen 2012) and control for firm and loan characteristics. We find that breached firms face greater increases in loan spreads than control firms and their loans are more likely to require collateral and demand more loan covenants. Our results also show that breached and non-breached firms exhibit similar trends in bank loan terms before data breaches and thus their prior trends cannot explain their diverging trends after the data breaches. We also find consistent results when using variations of the PSM method and different sample periods. Furthermore, we identify three conditions where data breaches are likely to inflict more harm on firms. Specifically, we find that breaches resulting from criminal attacks, with more records lost, and in certain vulnerable industries experience a higher increase in unfavorable loan terms. These cross-sectional tests indicate that post-breach changes in bank loan terms are driven by the characteristics of the data breaches.

Next, we test whether data breaches bring surprises to banks given a borrower's pre-breach reputation. Firms with a high IT reputation are viewed as having a strong internal information system (Kim et al. 2018), whereas firms with internal control weaknesses (ICWs) have substandard internal control over financial reporting (Kim, Song, and Zhang 2011). We find that, after breaches, firms with a high IT reputation experience more negative adjustments to their loan terms than peer breached firms, but firms with ICWs experience adjustments similar to their peers. This suggests that, consistent with Kim et al. (2018), banks have high expectations for firms with a strong IT reputation and price their loans favorably, so that when the firms are suddenly hit with data breaches (disconfirmatory evidence), the banks are taken by surprise and adjust their loan terms harshly.

Moreover, we use the exogenous shock of the introduction of mandatory data breach notification laws to confirm the effect of data breaches on bank loan terms. These laws impose costs on breached firms (e.g., costs of notification and corresponding remedial activities) and alert the investment community including banks to negative news. Our analyses reveal that data breach incidents lead to more unfavorable terms after these laws became effective in the states in which breached firms are headquartered. In an attempt to further establish a link between reported data breaches and bank loan terms, we also explore channels through which the former affects the latter. Consistent with the proposition that breaches increase default risk and information risk, we find that compared with control firms, breached firms experience significant losses of major customers and market share, decreases in firm performance, and increases in default and information risks. Finally, we investigate whether remedial actions taken by breached firms can mitigate the adverse consequences for loan terms. We manually collect seven variables describing firms' corrective actions following data breaches. We find that firms that take remedial actions more actively experience less unfavorable changes in loan terms.

Our study makes several important contributions. First, we contribute to a more complete understanding of lenders' reactions to data breaches. Banks are an important provider of corporate financing and can adjust various features of their contracting terms in response to adverse events (Graham et al. 2008). We show that data breaches lead to significant increases in the amount of interest payable, the likelihood of collateral requirement, and the number of covenants. Our conclusions are largely consistent with concurrent work (Sheneman 2017). More importantly, we conduct a series of analyses pertaining to cross-sectional variations, regulatory intervention, and remedial action, and perform a channel analysis and another analysis conditional on IT reputation and ICWs. Although our results on cross-sectional variations in breach characteristics are similar to those in Shemenan (2017), our other analyses complement and extend that study's cross-sectional analyses of analysts following, credit rating, and lender competition. Our evidence provides a nuanced and in-depth understanding of the loan contracting consequences of negative data breach information, especially when compared with positive IT reputation information and other types of negative information such as restatements, litigation, and ICWs (Graham et al. 2008; Kim et al. 2011; Deng, Willis, and Xu 2014; Kim et al. 2018).

Second, we advance our understanding of the nature of a data breach. Our analyses indicate that the impact of a data breach depends on the type of breach, the number of records lost, and the type of industry the breached firm belongs to. In addition, we provide evidence on the mechanisms through which data breaches affect firm value (e.g., loss of major customers and higher information risk). Furthermore, we find that the effect of data breaches is conditional on IT reputation. Finally, our evidence suggests that firms can mitigate the negative consequences by taking more remedial actions.

Third, our study explores the regulatory effect on data breaches. The increasing use of big data, mobile devices, social media, artificial intelligence, and cloud computing has exacerbated the issue of security breach and drawn attention from regulators. All US jurisdictions have now adopted some form of data breach mandatory disclosure rule. We show that banks' respond more strongly to data breaches after the introduction of such legislations, suggesting the mandatory disclosures improve market efficiency.

The remainder of the paper is organized as follows. Section II discusses prior research and develops our hypotheses. Section III describes the data source and the sample selection process and presents descriptive statistics. Section IV discusses the results of our main analyses and robustness tests. Section V presents the results of additional analyses. Section VI concludes the study.

II. HYPOTHESIS DEVELOPMENT

Following Duffie and Lando's (2001) framework, we reason that a data breach can affect a firm's bank loan contracting mainly through two channels: default risk and increased information risk. We further argue that a data breach provides incremental information above and beyond IT reputation and SOX 302 ICWs.

Default Risk and Bank Loan Terms

Breached firms incur significant breach-related direct costs leading to a decrease in firm profitability. Ponemon Institute (2017) classifies these costs into three major categories: detection and escalation costs (e.g., forensic and investigative activities, assessment and audit services, and crisis team management), notification costs (e.g., creating contact databases, identifying all regulatory requirements, and postal expenditures), and post-breach costs (e.g., help desk activities, remedial activities, legal expenditures, and identity protection services). These three categories of costs amount to approximately $1.07 million, $0.69 million, and $1.56 million for a breached firm on average and directly reduce the firm's earnings (Ponemon Institute 2017). In Equifax's case, the direct costs of its data breach incident in 2017 exceeded $700 million (LaCroix 2017). In summary, we conjecture that the direct costs following a data breach will lead to lower firm profitability, higher default risk, and unfavorable loan contracting terms.

In addition, breached firms experience significant indirect costs such as reputation costs, which are the larger penalty for a negative corporate event (Karpoff and Lott 1993). A data breach tends to be viewed as a breach of trust and a violation of contract resulting in severe reputation damage for the firm (Janakiraman, Lim, and Rishika 2018; Gwebu et al. 2018; Akey, Lewellen, and Liskovich 2018). First, we argue that a loss of customers leads to lower and more volatile operating profitability. When customers' financial information is compromised in a data breach, their trust in the breached firm is reduced (Martin et al. 2017). In addition, customers may incur psychological loss (e.g., anxiety), recovery cost, and possibly a higher cost of borrowing as a result of having their data stolen (Solove and Citron 2018). Thus, they may leave the breached firms. For example, Ponemon Institute (2017) reports an abnormal customer churn rate of 5.7 percent for breached firms in life science industries. Using a DID approach, Janakiraman et al. (2018) find that customers of breached firms significantly reduce their purchases. Furthermore, data breaches can lead to a loss of major customers, which will cause a large drop in the cash flow of breached firms (Dhaliwal et al. 2016). Less profitable firms are more likely to default on their debt, so they tend to receive worse terms (Berger and Udell 1995; Freixas and Rochet 1997; Graham et al. 2008; Bradley and Roberts 2015).

Second, we conjecture that the reputation fallout from a data breach also negatively affects the firm's relationships with other stakeholders such as suppliers, executives, shareholders, and regulators (Cavusoglu, Mishra, and Raghunathan 2004), leading to higher operational risk. For example, a data breach can negatively affect the careers of top executives as breached firms might try to put the blame on their executives (Fuhrmans 2017; Nordlund 2017; Lending, Minnick, and Schorno 2018; Banker and Feng 2019). To make matters worse, qualified executives may hesitate to join a firm whose reputation has been damaged by a breach, which increases the uncertainty surrounding the firm's future. A data breach often leads to lawsuits from affected stakeholders (Romanosky et al. 2014),[3] which harm defendant firms' reputation by leading to negative media coverage, additional damaging information, difficulty in recruiting managers and directors, and disruption of relationships with suppliers (Johnson, Nelson, and Pritchard 2000; Black, Cheffins, and Klausner 2006; Chava et al. 2010). Finally, regulators are also actively involved post breach further damaging the breached firm's reputation. For example, shortly after Capital One's disclosure of a massive data breach with more than 100 million records compromised, New York

[3] For example, Yahoo's announcement on September 22, 2016, of a data breach involving more than 500 million accounts triggered class-action lawsuits from its users and resulted in a $115 million settlement and a severe loss of brand value. See https://www.reuters.com/article/us-verizon-yahoo/yahoo-in-new-117-5-million-data-breach-settlement-after-earlier-accord-rejected-idUSKCN1RL1H1.

Attorney General Letitia James launched an investigation into the firm's security failures.[4] Consistent with these studies, Murphy, Shrieves, and Tibbs (2009) show that firms with reputation costs subsequently face increased risk and decreased market value and earnings. Deng et al. (2014) suggest that firms whose reputation is damaged by securities lawsuits are seen as having riskier operations. In summary, the reputation loss from being hit with a data breach can lead to an increase in operational risk and default risk, which will in turn induce a higher cost of borrowing.

Information Risk and Bank Loan Terms

We expect banks to perceive breached firms as having high information risk and thus to offer them unfavorable bank loan terms. Dichev and Skinner (2002), Drucker and Puri (2009), Costello and Wittenberg-Moerman (2011), and Kim et al. (2018) propose that creditors such as banks rely on operating and accounting information including insider information obtained directly from the firm to evaluate its health and viability and make loan terms decisions. A data breach indicates that a weakness exists in this system, which can be seen as an operational control risk and may lead others to doubt the reliability of the firm's financial reporting (Lawrence et al. 2018; Smith et al. 2019; Li et al. 2020). Thus, breached firms have higher information risk, which will be negatively reflected in bank loan terms (Rajan and Winton 1995; Kim et al. 2018), given that lenders cannot fully trust the information supplied by these firms (Graham et al. 2008; Costello and Wittenberg-Moerman 2011). For example, Rajan and Winton (1995) suggest that to mitigate information risk, banks will monitor borrowers more vigilantly by demanding collateral and putting more covenants in place. Kim et al. (2018) find that firms with a solid IT reputation enjoy better loan terms partly due to their perceived low information risk. In summary, a data breach incident signals a high level of information risk associated with the firm, leading to unfavorable

[4] https://finance.yahoo.com/news/cost-of-capital-ones-data-breach-could-exceed-300-million-expert-224823227.html

bank loan terms.

However, the effect of a data breach on a firm's information environment is anything but straightforward. A breached firm may quickly improve its information environment and internal control system as a response to the public scrutiny following the data breach. For example, many breached firms take corrective actions (Gwebu et al. 2018), which can include hiring an external data security expert, improving their IT system, revising policies on data security, and providing better employee training. Take HEI Hotels & Resorts for example. After experiencing a data breach of their payment system by malicious software, the company stated the following in their letter to the Office of the Attorney General of New Hampshire:

> "HEI took steps to address and contain this incident promptly after it was discovered, including engaging outside data forensic experts to assist in investigating and remediating the situation and promptly transitioning payment card processing to stand-alone systems that are completely separated from the rest of its network. In addition, HEI has disabled the malware and have reconfigured its point-of-sale and payment card processing systems to enhance the security of these systems." [5]

This piece of anecdotal evidence suggests that a breached firm might be able to improve its information system shortly post-breach through a series of corrective actions, thereby mitigating some of the adverse consequences. In sum, firms with data breaches are viewed as having a weak internal information system. Nevertheless, their post-breach corrective actions might be able to mitigate some of the weaknesses.

The Effects of Data Breaches Are Above and Beyond Those of IT Reputation and ICWs

Data Breaches and IT Reputation

Kim et al. (2018) show that firms with a high IT reputation (being named in InformationWeek 500 for five consecutive years) enjoy better bank loan terms. Hence, to the extent

[5] https://www.doj.nh.gov/consumer/security-breaches/documents/hei-hotels-resorts-20160812.pdf

that IT reputation is inversely related to a data breach incident, we expect the latter to lead to unfavorable bank loan terms. However, it is not clear whether IT reputation is indeed inversely related to the likelihood of a data breach. First, a strong IT reputation suggests that these firms have superior data collection and storage capabilities and thus possess more valuable information repositories (data accessible and usable for decision making) (Wixom and Watson 2001; Piccoli and Ives 2005), which in turn are more likely to attract attacks. Second, IT reputation does not necessarily measure a firm's ability to protect itself from data breaches. For example, many firms prioritize digital, cloud or other IT projects over data security and often they do not have a separate budget for the latter (Florov 2019). Third, IT reputation is a barometer for a firm's IT capability (Stoel and Muhanna 2009). A strong IT capability tends to indicate a large number of IT employees and physical devices, which might actually increase the likelihood of a data breach by insiders and lost or stolen physical devices. Fourth, some research suggests that data breaches are idiosyncratic and impossible to avoid entirely, and there is no guarantee that IT technology can prevent all data breaches (Barton 2015). In sum, the above argument suggests that it is unclear how IT reputation will affect the likelihood of a data breach incident, and thus a data breach will provide banks with incremental information above and beyond the firm's IT reputation.

Data Breaches and Internal Control Weaknesses (ICWs)

Prior literature has shown that ICWs are associated with unfavorable bank loan terms (e.g., Kim et al. 2011). Thus, to the extent that data breach incidents are strongly determined by whether a firm has an ICW, such incidents would not provide significant incremental information to banks above and beyond ICWs. However, while internal controls generally include those over operations, financial reporting, and regulatory compliance (COSO 2013; Lawrence et al. 2018), the ICW assessment mandated by SOX focuses on the effectiveness of controls over financial reporting

(Kim et al. 2011; DeFond and Lennox 2017; McKenna 2018). Therefore, material risk may still exist in the internal control system of a firm without an ICW (Ernst & Young 2006). Consistent with this view, in a ruling for the securities class action filed by Equifax shareholders, the judge stated that SOX applies to accounting-related internal control and a clean managerial assessment of ICWs is not equivalent to a clean assessment of the firm's entire internal control system and its ability to prevent data breaches (LaCroix 2019). In addition, firms with ICWs are not necessarily more likely to experience a data breach (Amir, Levi, and Livne 2018; Westland 2018; Richardson, Smith, and Watson 2019). For example, Westland (2018) shows that an ICW is a poor predictor of various types of data breaches except for credit card breaches. The above argument indicates that the likelihood of a data breach is, to a large extent, independent of a firm's ICW assessment. Thus, data breaches will provide significant incremental information regarding a firm's internal control above and beyond ICWs.

Summary

The above arguments suggest that a data breach leads to higher default risk due to direct costs and reputation loss and might also indicate a high information risk, both of which will lead to unfavorable bank loan terms. In addition, a data breach provides incremental information above and beyond IT reputation and ICWs to banks. We, therefore, propose the following hypothesis (stated in alternative form):

> **Hypothesis 1**: Firms receive less favorable bank loan terms after experiencing a data breach.

III. DATA SOURCES, SAMPLE SELECTION, AND DESCRIPTIVE STATISTICS

Data Sources

We obtain financial data from Compustat, stock return data from CRSP, and bank loan data from DealScan. Appendix A provides detailed definitions of the variables used in our empirical analysis. We obtain data on reported data breach events from 2005 to 2014 from the Privacy Rights Clearinghouse's Chronology of Data Breaches (https://www.privacyrights.org/data-breaches). This Chronology records US data breaches reported by either government agencies or verifiable media sources from 2005 onward for both public and private firms.[6] It defines a data breach as "a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual."[7]

Sample Selection

We test the changes in loan terms from three years before to three years (including the incident year) after the data breach. Our data breach sample spans the period from 2005 to 2014 and our loan sample from 2003 to 2016. Table 1 presents sample development and distribution. As shown in panel A, we start by merging breached firms from 2005 to 2014 in the Chronology with Compustat, resulting in 551 event firms. If event firms had also experienced breaches between 2003 and 2004, banks would have already responded negatively to the breaches. We identify such firms by conducting a search in Factiva, Bloomberg, and Google using a firm's name and keywords (e.g., data breach, cyberattack, and security breach) and excluding all 16 of them from our sample. Following Bertrand and Mullainathan (1999b; 2003), for firms with multiple data breach events from 2005 to 2014, we keep only the most severe one with the highest number of

[6] It is possible that some data breaches were not reported to the Privacy Rights Clearinghouse (Li et al. 2020). Thus, some of our control firms may have experienced unreported data breaches. Nevertheless, any potentially unreported breaches in the control firms will not affect the validity of our results since they work against finding our results (Li et al. 2020). In addition, we conduct a robustness test to mitigate the concern. Specifically, after the enactment of state-level data breach notification laws that require mandatory disclosures of data breaches, firms are more likely to report a breach. We thus limit the event firms to those attacked after the data breach notification laws took effect in their respective states and find that our main results (untabulated) still hold.

[7] https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice

records lost. This procedure removes 70 event firms. Next, we match each event firm with a control firm based on their probability of falling victim to a data breach in the incident year. This step eliminates 252 firms due to the lack of necessary data required for the PSM process. We limit our bank loan sample to those loans extended to firms within three years before (including the incident year) to three years after data breaches. Specifically, we merge the remaining 213 event firms and the corresponding 213 control firms with those in the DealScan database from 2003 to 2016, resulting in 1,428 bank loans for these firms. We exclude 254 observations from the financial services industry (SIC 6000-6999), 55 observations with bridge loans and non-fund-based facilities (e.g., leases and standby letters of credit), and 37 observations with insufficient data to calculate the control variables. Finally, we exclude 1 observation of a control firm that had data breach events from 2003 to 2004. Our final sample consists of 1,081 bank loans from 2003 to 2016 for which all required data are available, and a total of 139 breached firms.[8] In Appendix B, we present a figure showing the change in bank loan terms for two sample firms.

Panel B of Table 1 reports the distribution of breached firms by the Fama-French industry. The business services industry has the highest number of data breaches (28), followed by the retail industry (25), and the restaurants, hotels & motels industry (12). Panel C of Table 1 presents the data breach events by type. Privacy Rights Clearinghouse classifies data breach events into eight types: payment card fraud, hacking or malware, insider, physical loss, portable device, stationary device, unintended disclosure, and unknown. Please refer to Appendix A for definitions of these types of data breach events.

[8] For the treatment firms, there are 312 (275) observations for the pre-breach (post-breach) period. For the control firms, there are 255 (239) observations for the pre-breach (post-breach) period. Not all breached firms have at least one loan in the pre- and post-breach periods, but as indicated in our robustness checks, imposing this requirement yields similar results. In addition, the mean of the treatment sample (i.e., *Data Breach*) is 0.543, which is fairly similar to prior research using the PSM method (e.g., Chen, Hung, and Wang 2018).

Descriptive Statistics

Panel A of Table 2 reports the descriptive statistics for our final sample of 1,081 observations. The first part shows the descriptive statistics for bank loan characteristics. The mean and median of *Loan Spread* are 210.500 and 175.000 basis points, respectively. The mean (median) loan amounts and maturity are $0.954 ($0.500) billion and 55.310 (60.000) months, respectively. The percentage of secured bank loans is 48.5 percent and 42.3 percent of the sample loans have performance pricing provisions. The average number of total, general, and financial covenants are 3.069, 1.966, and 1.104, respectively. The remainder of panel A presents the descriptive statistics for other variables. On average, firm size (natural log of total assets) is 8.779, leverage is 50.3 percent, and *ROA* is 14.4 percent. Panel B of Table 2 presents the correlation analysis. The interaction term of *Data Breach*Post* exhibits significantly positive associations with both *Ln(Loan Spread)* and *Secured*, suggesting a post-breach increase in loan spread and the likelihood of collateral requirement at a univariate analysis level.

IV. METHODOLOGY AND MAIN RESULTS

The Sample Matched by Propensity Score

We conduct a DID analysis to see whether changes in bank loan terms before and after the data breach are significantly different between treatment and control firms. Specifically, in the first-stage Probit regression, we regress the incident of a data breach on lagged firm characteristics for all firms in the Compustat database with available data from 2005 to 2014 and then use the obtained coefficients to estimate a propensity score for each firm-year. We then match each breached firm with a control firm with the closest propensity score in the year of the data breach incident. We employ the following Probit regression model to identify the determinants of a data breach:

$$
\begin{aligned}
\textit{Data Breach Event}_t = {} & \alpha_0 + \alpha_1 \textit{Firm Size}_{t\text{-}1} + \alpha_2 \textit{Leverage}_{t\text{-}1} + \alpha_3 \textit{ROA}_{t\text{-}1} + \alpha_4 \textit{Operational Risk}_{t\text{-}1} \\
& + \alpha_5 \textit{Tangibility}_{t\text{-}1} + \alpha_6 \textit{Z-score}_{t\text{-}1} + \alpha_7 \textit{MB}_{t\text{-}1} + \alpha_8 \textit{IT Expertise}_{t\text{-}1} \\
& + \alpha_9 \textit{IT Reputation}_{t\text{-}1} + \alpha_{10} \textit{Number of Segments}_{t\text{-}1} + \alpha_{11} \textit{ICW}_{t\text{-}1} \\
& + \alpha \textit{Industry} + \alpha \textit{Year} + \varepsilon \qquad (1)
\end{aligned}
$$

Data Breach Event equals 1 if a firm discloses a data breach in a particular year, and 0 otherwise. We include several variables as the determinants of the likelihood of experiencing a data breach. *Firm Size* is the natural log of total assets. Larger firms tend to have larger customer bases and more customer data and thus are more attractive attack targets (Wang, Kannan, and Ulmer 2013). *Leverage* is the sum of current debt and long-term debt scaled by total assets (Li et al. 2020). Cash-constrained firms are less likely to spend on IT technology to protect their customer databases, making them more vulnerable to attacks (Higgs et al. 2016). *ROA* is the EBITDA scaled by total assets. A higher *ROA* suggests that the firm has a superior customer base and hence valuable customer information and thus it is likely to be a target of data breach. *Operational Risk* is the standard deviation of yearly cash flows from operations divided by total assets over the past five fiscal years. A high operational risk might indicate that the firm has an unstable information system, making it susceptible to attacks (Kamiya et al. 2020).[9] *Tangibility* is gross property, plant, and equipment scaled by total assets. Firms with a larger amount of tangible assets are less likely to rely on intangible assets such as the customer database to obtain a competitive advantage and are less vulnerable to data breaches (Kamiya et al. 2020). *Z-score* is the modified Altman (1968) Z-score to capture a firm's likelihood of experiencing financial distress. Similar to high leverage firms, firms that are more likely to experience financial distress are more likely to be attack targets. *MB* is the market-to-book ratio. Growing firms tend to have a higher *MB*, but it is not clear whether such firms have valuable and attractive customer databases. *IT Expertise* is an indicator variable that equals 1 if the firm has at least one chief information officer, chief security officer, or any

[9] Kamiya et al. (2020) use a similar measure (volatility of return) that also captures a firm's risk.

high-ranking officer holding an information- or security-related position, and 0 otherwise. Having in-house IT expertise indicates the firm's desire to protect its data, which in turn suggests that it possesses valuable databases that hackers would find attractive. Meanwhile, having an officer devoted to IT and security might lead to more resources being allocated to database protection. *IT Reputation* is an indicator variable that equals 1 if the firm can be seen on the InformationWeek 500 list for five consecutive years, and 0 otherwise. As discussed previously in Section II, it is not clear how *IT reputation* affects the likelihood of a data breach incident. We include *Number of Segments* to control for a firm's operational complexity. Firms operating in more market segments are more likely to be exposed to operational risk and thus to attract data attacks (Lawrence et al. 2018). *ICW* is an indicator variable that equals 1 if the firm has ICWs under SOX 302, and 0 otherwise.[10] As discussed previously in Section II, the likelihood of a data breach is, to a large extent, independent of a firm's ICW assessment. We include *ICW* to control for its potential association with data breach incidents. *Industry* equals 1 if the firm is operating in a particular Fama-French 48 industry, and 0 otherwise, and *Year* equals 1 if the observation occurs in a particular year, and 0 otherwise (Wang et al. 2013; Sheneman 2017; Li et al. 2020).

Panel A of Table 3 presents the results of this Probit regression analysis. We find that large firms and firms with a high *ROA*, high *Operational Risk*, executive-level IT expertise, and a strong IT reputation (high *MB*) are more (less) likely to fall victim to a data breach. The results seem to suggest that better-performing firms are more attractive targets for data attacks probably due to their possession of valuable customer databases. The area under the receiver operating characteristic curve (AUC) is 0.870, indicating that the first-stage model is reasonably accurate in predicting the likelihood of a data breach. Panel B of Table 3 presents the differences in firm and

[10] Following Lobo et al. (2020), we consider SOX 302 ICWs instead of SOX 404 ICWs.

IT characteristics (i.e., *Firm Size*, *Leverage*, *ROA*, *Operational Risk*, *Tangibility*, *Z-score*, *MB*, *IT Expertise*, *IT Reputation*, *Number of Segments*, and *ICW*) between the 213 treatment firms and the 213 control firms after the PSM. None of the differences is significant, indicating that these two samples have very similar firm and IT characteristics.

Main Results

Different firms experience data breaches at different times. Thus, to capture the effect of the staggered data breaches on bank loans, following Bertrand and Mullainathan (1999a; 1999b; 2003), Low (2009), Armstrong et al. (2012), and Fauver, Hung, and Taboada (2017), we take a staggered difference-in-differences approach and construct the following dynamic treatment effects model:

$$
\begin{aligned}
\mathit{Loan\ Contract\ Terms} = {} & \beta_0 + \beta_1 \mathit{Data\ Breach{*}Year\ {-1}} + \beta_2 \mathit{Data\ Breach{*}Year\ 0} \\
& + \beta_3 \mathit{Data\ Breach{*}Year\ 1} + \beta_4 \mathit{Data\ Breach{*}Year\ 2{+}} + {+}\beta_5 \mathit{Ln(Loan\ Size)} \\
& + \beta_6 \mathit{Ln(Loan\ Maturity)} + \beta_7 \mathit{Performance\ Pricing} + \beta_8 \mathit{Firm\ Size}_{t\text{-}1} \\
& + \beta_9 \mathit{Leverage}_{t\text{-}1} + \beta_{10} \mathit{ROA}_{t\text{-}1} + \beta_{11} \mathit{Operational\ Risk}_{t\text{-}1} + \beta_{12} \mathit{Tangibility}_{t\text{-}1} \\
& + \beta_{13} \mathit{Z\text{-}score}_{t\text{-}1} + \beta_{14} \mathit{MB}_{t\text{-}1} + \beta_{15} \mathit{IT\ Expertise}_{t\text{-}1} + \beta_{16} \mathit{IT\ Reputation}_{t\text{-}1} \\
& + \beta_{17} \mathit{Number\ of\ Segments}_{t\text{-}1} + \beta_{18} \mathit{ICW}_{t\text{-}1} + \beta_{19} \mathit{Credit\ Spread} \\
& + \beta_{20} \mathit{Term\ Spread} + \beta \mathit{Firm} + \beta \mathit{Year} + \varepsilon
\end{aligned} \tag{2}
$$

where *Data Breach* equals 1 if the firm discloses a data breach during 2005-2014, and 0 otherwise. Dummies *Year -1, Year 0*, *Year 1,* and *Year 2+* are indicator variables set to one if the firm-year is one year before, the year of, one year after, and two or more years after the data breach, respectively (with *Year -2* being the benchmark year). Since the model includes the firm and year fixed effects, it need not include the main effects of *Data Breach* and dummies *Year -1, Year 0, Year 1,* and *Year 2+*. The yearly effect of data breaches on bank loan terms, relative to non-breached firms, is captured by the interaction terms of *Data Breach* and dummies *Year -1, Year 0, Year 1*, and *Year 2+*, respectively..

The dependent variable of *Loan Contract Terms* refers to *Ln(Loan Spread)*, *Secured*, or *Number of Total Covenants*. *Ln(Loan Spread)* is the natural logarithm of the interest rate the borrower pays in basis points over LIBOR for each dollar drawn down. *Secured* is an indicator variable that equals 1 if the loan involves collateral, and 0 otherwise. Drawing on prior studies (Graham et al. 2008; Kim et al. 2011; Chen et al. 2016; Huang et al. 2018; Kim et al. 2018), we also control for loan and firm characteristics. We use the natural log of the amount of loan extended by the lender pool (*Ln(Loan Size*)), the natural log of the number of months to maturity (*Ln(Loan Maturity)*), and whether the facility has a performance pricing provision (*Performance Pricing*) to capture other loan characteristics besides spread (Beatty, Ramesh, and Weber 2002; Asquith, Beatty, and Weber 2005).

Equation (2) includes all firm characteristics in Equation (1). Larger firms (*Firm Size*) have more assets and a larger analyst following and thus lower default and information risks. Therefore, we expect larger firms to receive better loan terms. Leverage increases the default risk and firms with high leverage are expected to have less favorable loan terms. Firms with high *ROA* are more profitable and less likely to default on their loan, leading to their receiving more favorable loan terms. Firms with high *Operational Risk* have higher cash flow volatility and are expected to be given unfavorable loan terms. Because creditors can recover tangible assets if the firm defaults on its loan, higher *Tangibility* is expected to be associated with more favorable loan terms. Firms with a higher *Z-score* have a stronger financial position, lower default risk and thus receive better loan terms. *MB* captures a firm's growth opportunity. On one hand, firms with many growth opportunities may have a lower cost of debt given the expected growth in earnings. On the other hand, high growth firms may have volatile earnings and a higher default risk. We thus provide no directional prediction for the effect of *MB* on loan terms. *IT Expertise* captures whether a high-ranking officer is hired to oversee IT. On the one hand, a devoted IT officer suggests that the firm emphasizes IT technology and might have a market competitive advantage (e.g., superior databases) and high profitability. On the other hand, as discussed previously, such firms tend to be in the IT industry and might be growth firms with more volatile earnings. We hence provide no directional prediction for the effect of *IT Expertise* on loan terms. Firms with high *IT Reputation* tend to have higher and less volatile earnings and a better internal information system, suggesting lower default and information risks (Kim et al. 2018). Firms operating in a greater number of market segments have a more diversified operation and their earnings are less likely to be driven by one segment, leading to less volatile earnings, lower default risk, and more favorable loan terms. Firms with ICWs are likely to receive unfavorable loan terms (Kim et al. 2011).

In addition, we control for macroeconomic factors by including the difference in yield between corporate bonds rated BAA- and AAA- (*Credit Spread*) and the difference in yield between two-year and ten-year US Treasury bonds, measured one month before the loan becomes active (*Term Spread*). Finally, we include firm and year fixed effects. The firm fixed effects control for time-invariant omitted firm characteristics.

Table 4 presents the results of the regression analysis based on Equation (2). Both the interaction terms between *Data Breach* and the year dummies of *Year -1* and *Year 0* carry insignificant coefficients across the three dependent variables. On the other hand, both the interaction terms between *Data Breach* and the year dummies after the data breach (i.e., *Year 1* and *Year 2+*) carry significantly positive coefficients across the three dependent variables. Specifically, column 1 exhibits a significantly positive coefficient on *Data Breach***Year* 1 (0.221). Economically, this implies that relative to control firms, breached firms experience a 22.1 percent increase in loan spread in the first year, representing an increase in the cost of borrowing of 39.85

basis points.[11] Given our sample average loan amount of \$0.923 billion for the pre-breach period, the annual increase in interest cost is \$3.68 million (\$0.923 billion×0.003985) for an average loan, confirming that the impact is economically nontrivial. We also compare the economic significance of data breaches with that of other negative events (i.e. ICWs, securities litigation, and financial restatements). Specifically, our finding of a 39.85-basis-point increase in loan spread for breached firms is higher than the 28-basis-point increase due to ICWs (Kim et al. 2011) and the 26-basis-point increase due to securities litigation (Deng et al. 2014), but lower than the increase of 65 basis points due to financial restatements (Graham et al. 2008).

Similarly, in column 2 of Table 4, the coefficient of 0.114 on *Data Breach**Year 1* implies that relative to control firms, the likelihood that loans extended to breached firms require collateral increases by 11.4 percent in the first year after the incident. In column 3, the coefficient on *Data Breach**Year 1* loads significantly and positively (0.783). This indicates that relative to control firms, breached firms experience significant increases in the number of total covenants during the first year. Specifically, the average increase in the number of total covenants is 0.783, which is economically significant given that our sample mean is 2.94 for the pre-breach period.[12] In terms of loan-level control variables, using column 1 as an example, we find *Ln(Loan Size)*, *Performance Pricing*, *ROA*, *Tangibility*, and *Number of Segments* (*Ln(Loan Maturity)*, *Leverage*, *Credit Spread*, and *Term Spread*) to be negatively (positively) correlated with *Ln(Loan Spread).*

The results suggest that before the data breaches, breached and non-breached firms do not exhibit significant differences in bank loan terms. However, after the data breaches, the breached firms have higher loan spreads and a higher likelihood of collateral requirement, and they provide

[11] Following Graham et al. (2008, page 50, footnote 14), since the dependent variable here is in logarithmic form, the coefficient estimates represent the percentage change effects of the independent variables on the dependent variable. Specifically, 0.221*sample mean (pre-breach)=0.221*180.3=39.85 basis points.

[12] This implies an increase of 26.63 percent (0.783/2.94=26.63 percent) after the breach.

more covenants than non-breached firms. This analysis confirms the validity of the parallel trend assumption and demonstrates that data breaches cause breached and non-breached firms to diverge in their bank loan terms.

Robustness Checks

We run Equation (2) with *Data Breach*Post* (instead of the interaction terms of *Data Breach* and year dummies) as the variable of interest and find similar results (untabulated). *Post* is an indicator variable that equals 1 for the three-year period after the firm experiences a data breach, and 0 for the three years prior to the data breach incident including the incident year. Specifically, *Data Breach*Post* is significantly positive under all three dependent variables. We also run several other robustness tests. First, due to the potential issue associated with PSM analysis (Shipman, Swanquist, and Whited 2017), we use the full Compustat sample without matching by the propensity score. Second, we require the closest propensity score to have a caliper of less than 0.001. Third, we require a firm in the final sample to have observations for at least one year in both the pre- and post-data breach periods. Finally, we reduce the sample period to two years before (including the incident year) and two years after the breach year. The results (untabulated) continue to hold in all tests.

V. ADDITIONAL ANALYSES

Cross-Sectional Tests

Cross-sectional analyses can provide additional evidence on whether changes in bank loan terms are due to damage stemming from a data breach. These cross-sectional tests are conducted among breached firms.

Type of Data Breach

We start by examining variations in the type of data breach. As discussed previously, Privacy Rights Clearinghouse classifies data breaches into eight types. We define the indicator variable of *Criminal Data Breach* as being equal to 1 if a data breach involves payment card fraud or hacking (malware), and 0 otherwise. Criminal breaches are the most difficult to detect and contain (taking on average 303 days) and have a higher cost per capita ($244) than other types of breaches (Ponemon Institute 2017). The uncertainty and high cost associated with criminal data breaches lead to higher direct and reputation costs. Criminal breaches (e.g., hacking) also lead to an increase in audit fee, indicating heightened concern over the firm's financial information environment (Li et al. 2020). The above argument suggests that criminal breaches are associated with both higher default and information risks. We replace the interaction terms of *Data Breach* and year dummies by *Criminal Data Breach*Post* in Equation (2). The coefficient on *Criminal Data Breach*Post* represents the difference between criminal data breaches and other types of breaches in terms of changes in loan terms from the three years prior to the three years post the breach incident. Panel A of Table 5 presents the results of the cross-sectional analysis based on the type of data breach.[13] We find significantly positive coefficients on *Criminal Data Breach*Post* when *Ln(Loan Spread)* and *Secured* are the dependent variable (columns 1 and 2), indicating that increases in loan spread and the likelihood of collateral requirement are more pronounced for firms that have experienced criminal attacks.

Number of Records Lost

Next, we examine whether changes in bank loan terms are affected by the number of records lost. When more records are compromised, more customers are affected leading to higher direct and reputation costs and more business lost (Janakiraman et al. 2018). More data

[13] To save space, for the remaining tables, we report only the results for the variable of interest.

compromised also indicates that the breached firms might have a severe internal control deficiency. Therefore, the number of records lost is associated with both higher default risk and higher information risk. We define *More Records* as an indicator variable that equals 1 if the number of records lost exceeds the sample median, and 0 otherwise. We replace the interaction terms of *Data Breach* and year dummies by *More Records*Post* in Equation (2). Panel B of Table 5 presents the results of the cross-sectional analysis based on the number of records lost. *More Records*Post* loads significantly and positively when *Ln(Loan Spread)* and *Secured* are the dependent variables (columns 1 and 2), indicating that firms with more records lost experience greater increases in the loan spread and the likelihood of collateral requirement.

Industry

Finally, we examine whether changes in bank loan terms are affected by industry affiliation. Certain industries (e.g., healthcare) have higher data breach costs because they are highly regulated and their customers are more sensitive to the breach of personal information (Ponemon Institute 2017; Health Sector Cybersecurity Coordination Center 2019). Based on the per capita cost of a data breach by industry (Ponemon Institute 2017, p.10), we define *Vulnerable Industries* as 1 if the breached firm belongs to one of the following industries, and 0 otherwise: health, personal services, business services, computer, electronic equipment, and transportation. In addition, these industries tend to experience a higher abnormal customer churn rate after breaches (Ponemon Institute 2017, p.13). Thus, these industries suffer more from customer loss and incur higher direct costs after breaches and hence face a higher default risk. We replace the interaction terms of *Data Breach* and year dummies by *Vulnerable Industries*Post* in Equation (2). Panel C of Table 5 presents the results of the cross-sectional analysis based on industry affiliation. The coefficients on *Vulnerable Industries*Post* are significantly positive across all three dependent variables.

Effect of Data Breaches Conditional on IT Reputation and ICWs

In this section, we test the effect of data breaches on loan terms conditional on prior beliefs about the breached firm's IT and financial reporting control system. For firms with a high IT reputation, a data breach presents disconfirmatory evidence on their IT capability, which can lead to greater disappointment for banks and a significant erosion of trust in the firms. However, Gwebu et al. (2018) suggest that investors believe firms with a strong reputation traditionally may be able to recover quickly from data breaches and thus the markets may respond less negatively to breaches of strong reputation firms. We empirically test the effect of IT reputation on the association between data breaches and loan terms by limiting the sample to breached firms and replacing the interaction terms of *Data Breach* and year dummies by *IT Reputation**Post* in Equation (2). The results in panel A of Table 6 show that the interaction term of *IT Reputation**Post* is significantly positive when the dependent variables are *Ln(Loan Spread)* and *Secured*, suggesting that the negative effect of data breaches on loan terms is accentuated for breached firms with a strong IT reputation. This is consistent with lenders being surprised by the data breaches as they expect firms with a high IT reputation to be less likely to fall victim to such attacks. Because IT reputation has already been favorably priced in loan terms (Kim et al. 2018), banks will adjust the loan terms harshly after data breaches.

We also examine the opposite case: when a data breach provides confirmatory evidence on the firm's poor reputation. Specifically, we use SOX 302 ICWs to proxy for prior beliefs about a firm's poor financial reporting control system and examine whether it affects the association between data breaches and loan terms. We limit the sample to breached firms and replace the interaction terms of *Data Breach* and year dummies by *ICW**Post* in Equation (2). The results in panel B of Table 6 show that the interaction term of *ICW**Post* is not significant for any of the three dependent variables, suggesting that ICWs do not affect the association between data breaches and loan terms.

In sum, our results suggest that banks respond differently when a data breach is viewed as disconfirmatory evidence (high *IT reputation*) and when it is viewed as confirmatory evidence (*ICW*). While a disconfirmatory data breach leads to a more negative response from banks, a confirmatory data breach does not.

Enactment of Data Breach Notification Laws

We also examine whether the effect of a data breach on bank loan terms is reinforced by the introduction of data breach notification laws. Currently, private or governmental entities in all 50 states and the District of Columbia are required by law to notify individuals of breaches of personally identifiable information. Panel A of Table 7 provides the dates when the data breach notification laws came into effect in these 51 jurisdictions. Breached firms incur mandatory notification costs including the cost of creating contact databases, the cost of complying with regulation, and postal expenditures (Ponemon Institute 2017). Mandatory disclosures also attract attention from banks, which will incorporate the news into their loan terms.[14]

The legislations also provide us with an ideal quasi-experiment setting to investigate whether data breaches affect bank loan terms, because the legislations are largely exogenous to individual firms and banks. We analyze the effect of notification laws in panel B of Table 7. *Post Notification Law* is defined as an indicator variable that equals 1 if a data breach occurs after the

[14] Public firms are required to disclose material information. However, whether a data breach constitutes material information is subject to the firm's interpretation and can lead to underreporting (SEC 2011; 2018). The notification laws typically stipulate the definitions of "personal information" and "data breach", notice requirements (e.g., timing or method of notice and who must be notified), disclosure content (e.g., the nature and status of the breach), and disclosure to government authorities (e.g., State Attorney General and consumer reporting agency). These mandatory disclosure requirements constrain firms' ability to engage in selective disclosure and increase third parties' awareness of the breach (Tom 2010; https://www.govinfo.gov/content/pkg/CRPT-111srpt290/html/CRPT-111srpt290.htm#?).

data breach notification law became effective in the state in which the firm is headquartered, and 0 otherwise. We limit the sample to breached firms and replace the interaction terms of *Data Breach* and year dummies by *Post Notification Law*Post* in Equation (2). Coefficients on *Post Notification Law*Post* are significantly positive when *Ln(Loan Spread)* and *Number of Total Covenants* are the dependent variables (columns 1 and 3), indicating that post-breach increases in loan spread and number of total covenants are more pronounced after the effective dates of data breach notification laws. The results are supportive of the proposition that notification laws exacerbate the negative effect of data breaches on bank loan terms.

Effect of Data Breaches on Reputation Loss, Operational Performance, Default Risk, and Information Risk

We also explore the mechanisms through which data breaches negatively affect bank loan terms. First, we test whether data breaches lead to customer loss. Using the identities of major customers as reported in SFAS 14 and 131 (Bauer, Henderson, and Daniel 2018), we establish an indicator variable, *Loss of Major Customers*, which equals 1 if the firm loses at least one of its major customers, and 0 otherwise. We also use the annual market share growth (*Market Share Growth*) to capture the degree of customer loss. Second, we use *ROA* and cash flow from operation (*CFO*) to capture operational performance. Third, we use *Prob. Bankruptcy* and *Covenant Violation* to proxy for the risk of loan default and covenant violation. Specifically, *Prob. Bankruptcy* is the probability of bankruptcy following Shumway (2001). *Covenant Violation* is an indicator variable that equals 1 if the current ratio is less than the minimum current ratio or the debt-to-EBITDA ratio is greater than the maximum debt-to-EBITDA ratio required by the loan contract, and 0 otherwise. Finally, following prior literature (Amihud 2002; Easley, Hvidkjaer, and O'Hara 2002; Yang, Zhang, and Zhang 2020), we use *Stock Illiquidity* (the natural logarithm of the stock illiquidity measure from Gopalan, Kadan, and Pevzner (2012)) and *Std. Return* (standard deviation of monthly stock return over the next 12 months) to proxy for information risk.[15] Stock illiquidity arises from adverse selection costs and inventory costs, capturing information risk or the disagreement among investors about the available information from the trading volume-based perspective (Amihud 2002; Easley et al. 2002). The standard deviation of stock return is another measure of information risk from the price-based perspective since it reflects information asymmetry among investors (Yang et al. 2020).

We revise Equation (2) by setting the above variables as the dependent variables and excluding bank loan terms and *Z-score* from the list of control variables.[16] Furthermore, we replace the interaction terms between *Data Breach* and year dummies by *Data Breach*Post*. Table 8 shows that, following the data breach incident, breached firms experience (1) more significant losses of major customers and market share (panel A); (2) more significant decreases in *ROA* and *CFO* (panel B); (3) a higher likelihood of declaring bankruptcy and violating the loan covenants (panel C); and (4) higher information risk as indicated by higher stock illiquidity and higher standard deviation of stock returns (panel D).[17] Other papers have also examined the effect of data breaches on variables such as future sales changes, *ROA*, cash flow, and bankruptcy possibility (Ko and Dorantes 2006; Ko, Osei-Bryson, and Dorantes 2009; Lending et al. 2018; Richardson et al. 2019; Kamiya et al. 2020) and generated mixed results (see Richard et al. 2019 for a review). We find

[15] Furthermore, to mitigate the potential measurement biases and limitation of using the above two measures, following Dechow and Dichev (2002) and Gray et al. (2009), we also use accrual estimation errors to proxy for information risk from the accounting-based perspective and find similar results (untabulated).

[16] The *Z-score* is very similar to *Prob. Bankruptcy* as both measure default risk.

[17] Furthermore, to test the effect of these mechanisms on the loan terms, we compute the first principal component of the five default risk measures (*Loss of Major Customers*, *Market Share Growth*, *ROA*, *CFO*, and *Prob. Bankruptcy*) and of the two information risk measures (*Stock Illiquidity* and *Std. Return*). We find (in untabulated results) that firms with higher values of these two principal components have more unfavorable bank loan terms, confirming that data breaches affect bank loan terms through the channels of default risk and information risk. We do not include *Covenant Violation* in the test as doing so would significantly reduce the sample size. However, the results would still be robust if *Covenant Violation* is included.

evidence supporting the adverse effect of data breaches on these variables. Our study also provides additional evidence on the adverse consequences of data breaches from the perspectives of a loss of major customers, debt covenant violation, and information risk.

Data Breaches, Remediation, and Bank Loan Contracting

In this final additional test, we examine whether breached firms can mitigate the adverse consequences of data breaches by taking corrective actions. We manually collect data on the measures taken by breached firms to fix the data breach problem. Specifically, through breached firms' public statements and news searches in Factiva, Bloomberg, and Google, we collect the following seven variables: *CEO Resigned or Fired*, *Other Employees Resigned or Fired*, *Third Party Retained*, *IT System Improved*, *Policy or Training Improved*, *Credit Monitoring Provided*, and *Compensation Provided to Customer*. Appendix A provides a detailed description of these variables. We then use principal component analysis to find the first principal component of these seven remediation variables and name it *Remediation*. Next, we limit the sample to the breached firms and replace the interaction terms of *Data Breach* and year dummies by *Remediation**Post* in Equation (2). Table 9 reports the results. We find that the coefficient on *Remediation**Post* is significantly negative when the dependent variables are *Ln(Loan Spread)* and *Secured*. The results suggest that banks do take breached firms' corrective actions into consideration when adjusting their loan terms and treat these firms less unfavorably than they would those that do not engage in any corrective actions.[18]

VI. CONCLUSIONS

This study examines how reported data breaches affect firms' bank loan terms. Using the staggered difference-in-differences approach, we find that breached firms experience significantly

[18] The vast majority of these remedial actions were either taken or announced before the firms' first post-breach bank loan. Thus, these post-breach loan terms already reflect the positive effect of these remedial actions.

higher increases in loan spread, the likelihood of collateral requirement, and the number of covenants than do control firms. In cross-sectional tests, we find that the post-breach bank loan terms are more unfavorable when the data breaches involve criminal activities, when a larger number of records are lost, and when the breached firms belong to certain industries. Furthermore, we show that banks respond differently to breached firms with a high IT reputation (disconfirmatory evidence) and to those with ICWs (confirmatory evidence) by extending more unfavorable loan terms to the former but not to the latter. Specifically, although the IT reputation effects in our baseline analyses are insignificant,[19] IT reputation importantly affects the occurrence and consequences of data breaches. We show that firms with strong IT reputation are more likely to experience data breaches, suggesting that IT reputation is associated with firms' ability to collect and maintain valuable databases making them attractive targets. Moreover, banks have high expectation for firms with a strong IT reputation (consistent with Kim et al. 2018) and significantly adjust their risk assessment of these firms following data breaches.

Using the enactment of data breach notification laws as an exogenous shock, we also find that these laws exacerbate the negative effect of a data breach on bank loan terms. In addition, we show that breached firms experience losses of major customers and market share, decreases in operational performance, increases in the probability of bankruptcy and covenant violation, and increases in information risk, consistent with data breaches causing a deterioration in bank loan terms. Furthermore, our results indicate that breached firms that take remedial actions receive less unfavorable loan terms. Nowadays, firms spend billions of dollars annually on data collection and protection. Our paper extends our understanding of how banks respond to the data breaches of

[19] This inconsistency with Kim et al. (2018) is likely caused by sample difference. While their sample is based on firms that have appeared at least once on the InformationWeek 500 list, our sample is comprised of breached firms and their propensity-score-matched control firms. We are able to produce similar results to those of Kim et al. (2018) using a similar sample to theirs.

borrower firms. We show that the responses are affected by data breach characteristics, the prior IT reputation of borrowers, regulations, and the subsequent remedial actions taken by the borrowers.

REFERENCES

Akey, P., S. Lewellen, and I. Liskovich. 2018. *Hacking corporate reputations*. Working paper, University of Toronto, Pennsylvania State University, and University of Texas at Austin.

Altman, E. 1968. Financial ratios, discriminant analysis and the prediction of corporate bankruptcy. *Journal of Finance* 23 (4): 589-609.

Amihud, Y. 2002. Illiquidity and stock returns: Cross-section and time-series effects. *Journal of Financial Markets* 5 (1): 31-56.

Amir, E., S. Levi, and T. Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies* 23 (3): 1177-1206.

Armstrong, C. S., K. Balakrishnan, and D. Cohen. 2012. Corporate governance and the information environment: Evidence from state antitakeover laws. *Journal of Accounting and Economics* 53 (1-2): 185-204.

Asquith, P., A. Beatty, and J. Weber. 2005. Performance pricing in bank debt contracts. *Journal of Accounting and Economics* 40 (1-3): 101-128.

Banker, R., and Q. Feng. 2019. The impact of information security breach incidents on CIO turnover. *Journal of Information Systems* 33 (3): 309-329.

Barton, D. 2015. When will your data breach happen? Not a question of if but when. *Securityinfowatch* (March10). Available at: https://www.securityinfowatch.com/cybersecurity/infor mation-security/article/12052877/preparing-for-your-companys-inevitable-data-breach .

Bauer, A., D. Henderson, and L. Daniel. 2018. Supplier internal control quality and the duration of customer-supplier relationships. *The Accounting Review* 93 (3): 59-82.

Beatty, A., K. Ramesh, and J. Weber. 2002. The importance of accounting changes in debt contracts: The cost of flexibility in covenant calculations. *Journal of Accounting and Economics* 33 (2): 205-227.

Berger, A., and G. Udell. 1995. Relationship lending and lines of credit in small firm finance. *Journal of Business* 68 (3): 351-381.

Bertrand, M., and S. Mullainathan. 1999a. Is there discretion in wage setting? A test using takeover legislation. *RAND Journal of Economics* 30 (3): 535-554.

Bertrand, M., and S. Mullainathan. 1999b. *Corporate governance and executive pay: Evidence from takeover legislation.* Working Paper, Princeton University and Massachusetts Institute of Technology.

Bertrand, M., and S. Mullainathan. 2003. Enjoying the quiet life? Corporate governance and managerial preferences. *Journal of Political Economy* 111 (5): 1043-1075.

Black, B., B. Cheffins, and M. Klausner. 2006. Outside director liability. *Stanford Law Review* 58: 1055-1159.

Bradley, M., and M. Roberts. 2015. The structure and pricing of corporate debt covenants. *Quarterly Journal of Finance* 5 (2): 1550001-37.

Cavusoglu, H., B. Mishra, and S. Raghunathan. 2004. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce* 9 (1): 70-104.

Chava, S., C. S. Cheng, H. Huang, and G. Lobo. 2010. Implications of securities class actions for cost of equity capital. *International Journal of Law and Management* 52 (2): 144-161.

Chen, P. F., S. He, Z. Ma, and D. Stice. 2016. The information role of audit opinions in debt contracting. *Journal of Accounting and Economics* 61 (1): 121-144.

Chen, Y. C., M. Hung, and Y. Wang. 2018. The effect of mandatory CSR disclosure on firm profitability and social externalities: Evidence from China. *Journal of Accounting and Economics* 65 (1): 169-190.

Columbus, L. 2014. The year big data adoption goes mainstream in the enterprise. *Forbes* (January 12). Available at: https://www.forbes.com/sites/louiscolumbus/2014/01/12/2014-the-year-big-data-adoption-goes-mainstream-in-the-enterprise/#1aad46da2055

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2013. *Internal Control-Integrated Framework*. New York, NY: COSO.

Costello, A., and R. Wittenberg-Moerman. 2011. The impact of financial reporting quality on debt contracting: Evidence from internal control weakness reports. *Journal of Accounting Research* 49 (1): 97-136.

Dhaliwal, D., J. Judd, M. Serfling, and S. Shaikh. 2016. Customer concentration risk and the cost of equity capital. *Journal of Accounting and Economics* 61 (1): 23-48.

DeFond, M., and C. Lennox. 2017. Do PCAOB inspections improve the quality of internal control audits? *Journal of Accounting Research* 55 (3): 591-627.

Dechow, P., and I. Dichev. 2002. The quality of accruals and earnings: The role of accrual estimation errors. *The Accounting Review* 77 (s-1): 35-59.

Deng, S., R. Willis, and L. Xu. 2014. Shareholder litigation, reputational loss, and bank loan contracting. *Journal of Financial and Quantitative Analysis* 49 (4): 1101-1132.

Dichev, I., and D. Skinner. 2002. Large-sample evidence on the debt covenant hypothesis. *Journal of Accounting Research* 40 (4): 1091-1123.

Drucker, S., and M. Puri. 2009. On loan sales, loan contracting, and lending relationships. *Review of Financial Studies* 22 (7): 2835-2872.

Duffie, D., and D. Lando. 2001. Term structures of credit spreads with incomplete accounting information. *Econometrica* 69 (3): 633-664.

Easley, D., S. Hvidkjaer, and M. O'Hara. 2002. Is information risk a determinant of asset returns? *Journal of Finance* 57 (5): 2185-2221.

Ernst & Young. 2006. *Leveraging value from internal controls*. London, U.K.: Ernst & Young.

Fauver, L., M. Hung, X. Li, and A. Taboada. 2017. Board reforms and firm value: Worldwide evidence. *Journal of Financial Economics* 125 (1): 120-142.

Florov, M. 2019. If security breaches are inevitable, what do organisation do about it? *Computer Business Review* (Jan. 23). Available at: https://www.cbronline.com/news/if-security-breaches-are-inevitable-what-do-organisations-do-about-it.

Fuhrmans, V. 2017. New worry for CEOs: A career-ending cyberattack. *Wall Street Journal* (October 12).

Freixas, X., and J. Rochet. 1997. *Microeconomics of banking*. Cambridge, MA: MIT Press.

Gray, P., P. Koh, and Y. Tong. 2009. Accruals quality, information risk and cost of capital: Evidence from Australia. *Journal of Business Finance & Accounting* 36 (1-2): 51-72.

Gopalan, R., O. Kadan, and M. Pevzner. 2012. Asset liquidity and stock liquidity. *Journal of Financial and Quantitative Analysis* 47 (2): 333-364.

Graham, J., S. Li, and J. Qiu. 2008. Corporate misreporting and bank loan contracting. *Journal of Financial Economics* 89 (1): 44-61.

Gwebu, K., J. Wang, and L. Wang. 2018. The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems* 35 (2): 683-714.

Health Sector Cybersecurity Coordination Center. 2019. *A cost analysis of healthcare sector data Breaches*. Washington, DC: U.S. Department of Health and Human Services.

Higgs, J. L., R. E. Pinsker, T. J. Smith, and G. R. Young. 2016. The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems* 30 (3): 79-98.

Huang, H., G. Lobo, C. Wang, and J. Zhou. 2018. Do banks price independent directors' attention? *Journal of Financial and Quantitative Analysis* 53 (4): 1755-1780.

Janakiraman, R., J. Lim, and R. Rishika. 2018. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing* 82 (2): 85-105.

Johnson, M., K. Nelson, and A. Pritchard. 2000. In Re Silicon Graphics Inc.: Shareholder wealth effects resulting from the interpretation of the private securities litigation reform act's pleading standard. *Southern California Law Review* 73: 773-810.

Kamiya, S., J. Kang, J. Kim, A. Milidonis, and R. Stulz. 2020. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* (forthcoming).

Karpoff, J., and J. Lott. 1993. The reputational penalty firms bear from committing criminal fraud. *Journal of Law and Economics* 36 (2): 757-802.

Kim, J. B., B. Y. Song, and L. Zhang. 2011. Internal control weakness and bank loan contracting: Evidence from SOX Section 404 disclosures. *The Accounting Review* 86 (4): 1157-1188.

Kim, J. B., B. Y. Song, and T. Stratopoulos. 2018. Does information technology reputation affect bank loan terms? *The Accounting Review* 93 (3): 185-211.

Ko, M., and C. Dorantes. 2006. The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management* 17 (2): 13-22.

Ko, M., K-M. Osei-Bryson, and C. Dorantes. 2009. Investigating the impact of publicly announced information security breaches on three performance indicators of the breached firms. *Information Resources Management Journal* 22 (2): 1-21.

Kopp, E., L. Kaffenberger, and N. Jenkinson. 2017. *Cyber risk, market failures, and financial stability*. Working paper, International Monetary Fund. Available at: https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104

LaCroix, K. 2017. Equifax data breach litigation now includes securities suit. *The D&O Diary* (September 13). Available at: https://www.dandodiary.com/2017/09/articles/cyber-liability/equifax-data-breach-litigation-now-includes-securities-suit/.

LaCroix, K. 2019. Equifax data breach-related securities suit dismissal motion denied in part, granted in part. *The D&O Diary* (January 30). Available at: https://www.dandodiary.com/2019/01/articles/securities-litigation/equifax-data-breach-related-securities-suit-dismissal-motion-denied-part-granted-part/.

Lawrence, A., M. Minutti-Meza, and D. Vyas. 2018. Is operational control risk informative of financial reporting deficiencies? *Auditing: A Journal of Practice & Theory* 37 (1): 139-165.

Lending, C., K. Minnick, and P. J. Schorno. 2018. Corporate governance, social responsibility, and data breaches. *The Financial Review* (53): 413-455.

Li, H., W. No, and J. Boritz. 2020. Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory* 39 (1): 151-171.

Lobo, G., C. Wang, X. Yu, and Y. Zhao. 2020. Material weakness in internal controls and stock price crash risk. *Journal of Accounting, Auditing & Finance* 35 (1): 106-138.

Low, A. 2009. Managerial risk-taking behavior and equity-based compensation. *Journal of Financial Economics* 92 (3): 470-490.

Martin, K., A. Borah, and R. Palmatier. 2017. Data privacy: Effects on customer and firm performance. *Journal of Marketing* 81 (1): 36-58.

McKenna, F. 2018. SEC issues updated cybersecurity risk guidance but some say not nearly enough. *MarketWatch* (February 21). Available at: https://www.marketwatch.com/story/sec-issues-updated-cybersecurity-risk-guidance-but-some-say-not-nearly-enough-2018-02-21

Murphy, D., R. Shrieves, and S. Tibbs. 2009. Understanding the penalties associated with corporate misconduct: An empirical examination of earnings and risk. *Journal of Financial and Quantitative Analysis* 44 (1): 55-83.

Nordlund, J. 2017. *Director experience and cybersecurity events*. Working paper, Louisiana State University.

Piccoli, G., and B. Ives. 2005. IT-dependent strategic initiatives and sustained competitive advantage: A review and synthesis of the literature. *MIS Quarterly* 29 (4): 747-776.

Ponemon Institute. 2017. *2017 Cost of data breach study: United States*. Traverse City, MI: Ponemon Institute LLC.

Rajan, R., and A. Winton. 1995. Covenants and collateral as incentives to monitor. *Journal of Finance* 50 (4): 1113-1146.

Richardson, V., R. Smith, and M. Watson. 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems* 33 (3): 227-265.

Romanosky, S., D. Hoffman, and A. Acquisti. 2014. Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies* 11 (1): 74-104.

Rosati, P., M. Cummins, P. Deeney, F. Gogolin, L. Van der Werff, and T. Lynn. 2017. The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis* 49: 146-154.

Securities and Exchange Commission (SEC). 2011. *CF Disclosure guidance: Topic No.2: Cybersecurity.* Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Securities and Exchange Commission (SEC). 2018. *Commission statement and guidance on public company cybersecurity disclosures*. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf

Shipman, J., Q. Swanquist, and R. Whited. 2017. Propensity score matching in accounting research. *The Accounting Review* 92 (1): 213-244.

Sheneman, A. G. 2017. *The effect of operating control failures on the cost of capital -Evidence from data breaches*. Working paper, Ohio State University.

Shumway, T. 2001. Forecasting bankruptcy more accurately: A simple hazard model. *Journal of Business* 74 (1): 101-124.

Smith, T. J., J. L. Higgs, and R. E. Pinsker. 2019. Do auditors price breach risk in their audit fees? *Journal of Information Systems* 33 (2): 177-204.

Solove, D., and D. Citron. 2018. Risk and anxiety: A theory of data breach harms. *Texas Law Review* 96: 737-786.

Stoel, D., and W. Muhanna. 2009. IT capabilities and firm performance: A contingency analysis of the role of industry and IT capability type. *Information & Management* 46 (3): 181-189.

Tom, J. 2010. A simple compromise: The need for a federal data breach notification law. *St. John's Law Review* 84 (4): 1569-1603.

Wang, T., K. Kannan, and J. Ulmer. 2013. The association between the disclosure and the realization of information security risk factors. *Information Systems Research* 24 (2): 201-218.

Westland, J. 2018. *The information content of Sarbanes-Oxley in predicting security breaches*. Working paper, University of Illinois at Chicago.

Wixom, B., and H. Watson. 2001. An empirical investigation of the factors affecting data warehousing success. *MIS Quarterly* 25 (1): 17-41.

Yang, Y., B. Zhang, and C. Zhang. 2020. Is information risk priced? Evidence from abnormal idiosyncratic volatility. *Journal of Financial Economics* 135 (2): 528-554.

.

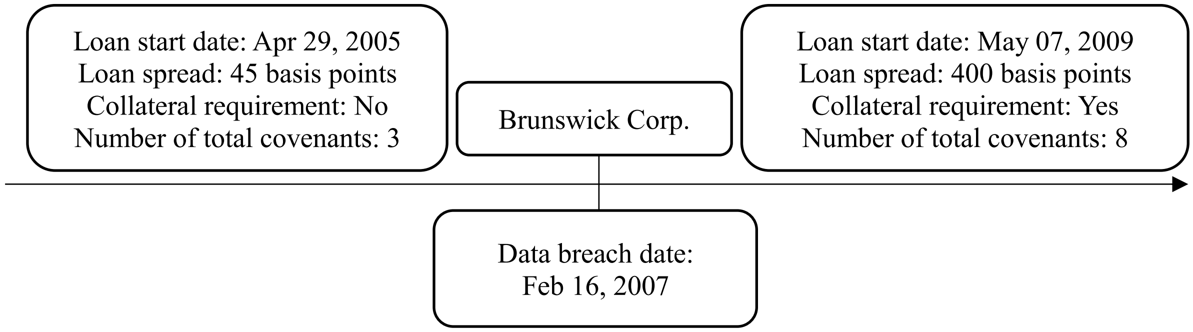
Appendix A

Variable name	Variable definition and construction
Data Breach Variables	
Data Breach Event	Indicator variable that equals 1 if the company discloses a data breach event in a particular year, and 0 otherwise. Source: https://www.privacyrights.org/data-breaches
Data Breach	Indicator variable that equals 1 if the company discloses a data breach during 2005-2014, and 0 otherwise. Source: https://www.privacyrights.org/data-breaches
POST	Indicator variable that equals 1 for the three-year period after the firm experiences a data breach, and 0 for the three years prior to the data breach incident including the incident year.
Data Breach Type	Data breaches are classified into the following eight types: payment card fraud (CARD), hacking or malware (HACK), insider (INSD), physical loss (PHYS), portable device (PORT), stationary device (STAT), unintended disclosure (DISC), and unknown (OTH). More specifically, payment card fraud refers to fraud involving debit and credit cards that is not accomplished via hacking. For example, it may involve skimming devices at point-of-service terminals. Hacking or malware refers to the situation where the system is hacked by an outside party or infected by malware. Insider refers to the case where someone with legitimate access—such as an employee, contractor or customer—intentionally releases sensitive information. Physical loss includes paper documents that are lost, discarded or stolen. Portable device includes lost, discarded or stolen laptops, personal digital assistants, smartphones, memory sticks, CDs, hard drives, data tapes, etc. Stationary device refers to the loss of stationary computers (lost, inappropriately accessed, discarded or stolen computers or servers not designed for mobility). Unintended disclosure refers to disclosures not involving hacking, intentional breach or physical loss (for example, sensitive information posted publicly, mishandled or sent to the wrong party via publishing online, via email, via post or via fax). Unknown refers to data breach events other than the seven types described above. Source: https://www.privacyrights.org/data-breaches
Number of Records	Number of records lost or stolen in the data breach. Source: https://www.privacyrights.org/data-breaches
Criminal Data Breach	Indicator variable that equals 1 if the data breach is of the HACK or CARD type, and 0 otherwise. Source: https://www.privacyrights.org/data-breaches
More Records	Indicator variable that equals 1 if the number of records lost or stolen in the data breach exceeds the sample median, and 0 otherwise. Source: https://www.privacyrights.org/data-breaches
Vulnerable Industries	Indicator variable that equals 1 for the health (Fama-French code 11), personal services (33), business services (34), computer (35), electronic equipment (36), and transportation (40) industries, and 0 otherwise.
Post Notification Law	Indicator variable that equals 1 if the data breach occurred after the state data breach notification law became effective, and 0 otherwise.
Bank Loan Variables	
Loan Spread	The interest rate the borrower pays in basis points over LIBOR for each dollar drawn down. Source: DealScan.
Ln(Loan Spread)	Natural logarithm of the interest rate the borrower pays in basis points over LIBOR for each dollar drawn down. Source: DealScan.
Loan Size	The loan amount of the facility in billion USD. Source: DealScan.
Ln(Loan Size)	Natural logarithm of the loan amount of the facility in billion USD. Source: DealScan.
Loan Maturity	The number of months to maturity. Source: DealScan.
Ln(Loan Maturity)	Natural logarithm of the number of months to maturity. Source: DealScan.

Secured	Indicator variable that equals 1 if the loan involves collateral, and 0 otherwise. Source: DealScan.
Performance Pricing	Indicator variable that equals 1 if the loan includes performance pricing provisions, and 0 otherwise. Source: DealScan.
Number of Total Covenants	Number of total covenants. Source: DealScan.
Number of General Covenants	Number of general covenants. Source: DealScan.
Number of Financial Covenants	Number of financial covenants. Source: DealScan.
Firm-level Variables	
Firm Size	Natural logarithm of total assets. Source: Compustat.
ROA	EBITDA scaled by total assets. Source: Compustat
Leverage	Sum of current debt and long-term debt scaled by total assets. Source: Compustat
Operational Risk	The standard deviation of yearly cash flows from operations divided by total assets over the past five fiscal years. Source: Compustat.
Tangibility	Gross property, plant, and equipment scaled by total assets. Source: Compustat
Z-score	Modified Altman (1968) Z-score = (1.2*working capital + 1.4*retained earnings + 3.3*income before extraordinary items + 0.999*sales)/total assets. Source: Compustat.
MB	Market-to-book ratio. Source: Compustat.
IT Expertise	Indicator variable that equals 1 if the borrower has a chief information officer, a chief security officer, or any high-ranking officer devoted to information or security, and 0 otherwise. Source: Compustat Execucomp.
IT Reputation	Indicator variable that equals 1 if the borrower appears on the InformationWeek 500 list for five consecutive years, and 0 otherwise. Source: InformationWeek.
Number of Segments	Number of business segments. Source: Compustat Segment.
ICW	Indicator variable that equals 1 if the borrower has an internal control weakness under SOX 302, and 0 otherwise. Source: Audit Analytics
Channel Test Variables	
Loss of Major Customers	Indicator variable that equals 1 if the borrower loses at least one of its major customers, and 0 otherwise. Source: Compustat Segment
Market Share Growth	Changes in annual market share. Source: Compustat
CFO	Operating cash flow scaled by total assets. Source: Compustat
Prob. Bankruptcy	The probability of bankruptcy following Shumway (2001). Source: Compustat
Covenant Violation	Indicator variable that equals 1 if the current ratio is less than the minimum current ratio or the debt-to-EBITDA ratio is greater than the maximum debt-to-EBITDA ratio required by the loan contract, and 0 otherwise. Source: DealScan
Stock Illiquidity	Natural logarithm of the stock illiquidity measure from Gopalan, Kadan and Pevzner (2012).
Std. Return	Standard deviation of monthly stock return over the next 12 months. Source: CRSP
Remediation Variables	
CEO Resigned or Fired	Indicator variable that equals 1 if the CEO resigned or was fired due to the breach event, and 0 otherwise.
Other Employees Resigned or Fired	Indicator variable that equals 1 if employees other than the CEO resigned or were fired due to the data breach event, and 0 otherwise.
Third Party Retained	Indicator variable that equals 1 if the breached firm hired or retained a third-party entity to deal with the data breach, and 0 otherwise.
IT System Improved	Indicator variable that equals 1 if the breached firm subsequently improved its IT system, and 0 otherwise.
Policy or Training Improved	Indicator variable that equals 1 if the breached firm subsequently improved its IT management policy or improved its employee training, and 0 otherwise.
Credit Monitoring Provided	Indicator variable that equals 1 if the breached firm subsequently provided customers with credit monitoring service, and 0 otherwise.

Compensation Provided to Customers	Indicator variable that equals 1 if the breached firm compensated affected customers, and 0 otherwise.
Remediation	The first principal component of the seven remediation variables above.

Appendix B

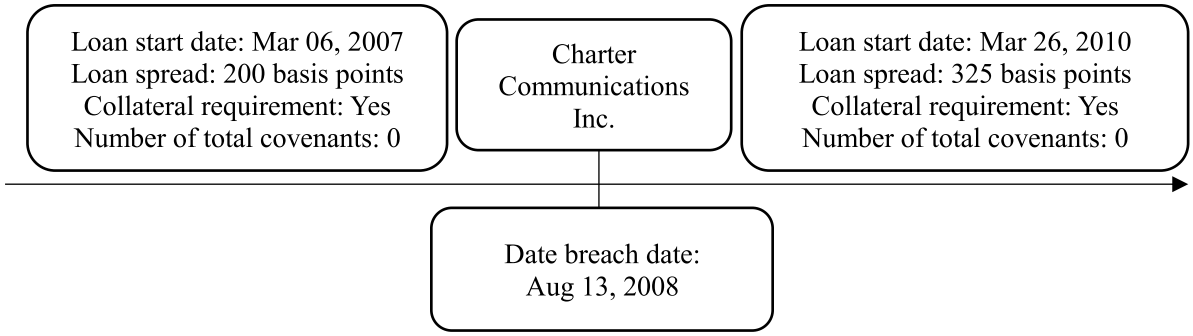


Loan start date: Apr 29, 2005
Loan spread: 45 basis points
Collateral requirement: No
Number of total covenants: 3

Brunswick Corp.

Loan start date: May 07, 2009
Loan spread: 400 basis points
Collateral requirement: Yes
Number of total covenants: 8

Data breach date:
Feb 16, 2007



Loan start date: Mar 06, 2007
Loan spread: 200 basis points
Collateral requirement: Yes
Number of total covenants: 0

Charter
Communications
Inc.

Loan start date: Mar 26, 2010
Loan spread: 325 basis points
Collateral requirement: Yes
Number of total covenants: 0

Date breach date:
Aug 13, 2008

TABLE 1
Sample Development and Distribution

Panel A: Sample Development

The sample consists of 1,081 bank loan observations from 2003 to 2016. Variables are defined in Appendix A.

Number of data breach event firms available at www.privacyrights.org and merged with Compustat from 2005 to 2014	551
Less:	
Number of event firms with a prior breach event from 2003 to 2004	(16)
For firms with multiple events, the number of events that are not the most significant one (in terms of number of records lost)	(70)
Number of event firms lacking the data for propensity score matching (PSM)	(252)
Number of event firms after PSM	213
213 event firms + 213 control firms	426
Bank loan observations in DealScan for 426 sample firms from 2003 to 2016	1,428
Less:	
Observations from financial services industries	(254)
Observations with bridge loans and non-fund-based facilities such as leases and standby letters of credit	(55)
Observations with insufficient data to calculate control variables	(37)
Observations of control firms having experienced prior data breach events during the period from 2003 to 2004	(1)
Final sample (involving 139 data breach event firms)	1,081

Panel B: Distribution of 139 Data Breach Event firms by Fama-French Industry

Fama-French Code	Fama-French Industry	Number of Data Breach	Fama-French Code	Fama-French Industry	Number of Data Breach
2	Food Products	1	30	Petroleum & Natural Gas	3
3	Candy & Soda	2	31	Utilities	2
7	Entertainment	5	32	Communication	9
8	Printing & Publishing	1	33	Personal Services	1
9	Consumer Goods	1	34	Business Services	28
11	Healthcare	4	35	Computers	5
12	Medical Equipment	2	36	Electronic Equipment	6
13	Pharmaceutical Products	4	37	Measuring & Control Equipment	2
14	Chemicals	1	38	Business Supplies	2
15	Rubber & Plastic Products	1	40	Transportation	2
17	Construction Materials	1	41	Wholesale	6
18	Construction	2	42	Retail	25
21	Machinery	5	43	Restaurants, Hotels & Motels	12
23	Automobiles & Trucks	1	48	Other Industries	3
24	Aircraft	2			

Panel C: Distribution of Data Breach Events by Type

	Freq.	Percent	Cum.
Payment card fraud	4	2.88	2.88
Unintended disclosure	16	11.51	14.39
Hacking or malware	38	27.34	41.73
Insider	15	10.79	52.52
Physical loss	12	8.63	61.15
Portable device	43	30.94	92.09
Stationary device	8	5.76	97.84
Unknown	3	2.16	100
Total	139	100	

TABLE 2
Descriptive Statistics and Correlation

Panel A: Descriptive Statistics

Variables	N	Mean	Std.	P25	Median	P75
Bank Loan Characteristics						
Loan Spread	1,081	210.500	157.600	112.500	175.000	275.000
Ln(Loan Spread)	1,081	5.048	0.865	4.723	5.165	5.617
Loan Amount (in Billions)	1,081	0.954	1.345	0.175	0.500	1.100
Ln(Loan Amount)	1,081	0.526	0.461	0.161	0.406	0.742
Maturity (in Months)	1,081	55.310	18.280	51.000	60.000	60.000
Ln(Maturity)	1,081	3.923	0.494	3.932	4.094	4.094
Performance Pricing	1,081	0.423	0.494	0.000	0.000	1.000
Secured	1,081	0.485	0.500	0.000	0.000	1.000
Number of Total Covenants	1,081	3.069	3.379	0.000	2.000	5.000
Number of General Covenants	1,081	1.966	2.532	0.000	1.000	3.000
Number of Financial Covenants	1,081	1.104	1.144	0.000	1.000	2.000
Data Breach Variables						
Data Breach	1,081	0.543	0.498	0.000	1.000	1.000
Post	1,081	0.475	0.500	0.000	0.000	1.000
Firm-level Variables						
Firm Size	1,081	8.779	1.899	7.420	8.745	9.933
Leverage	1,081	0.503	0.239	0.350	0.464	0.626
ROA	1,081	0.144	0.066	0.097	0.136	0.175
Operational Risk	1,081	0.043	0.043	0.018	0.027	0.050
Tangibility	1,081	0.568	0.372	0.226	0.527	0.861
Z-score	1,081	2.883	1.808	1.497	2.434	3.834
MB	1,081	2.372	3.053	1.371	2.109	3.285
IT Expertise	1,081	0.391	0.488	0.000	0.000	1.000
IT Reputation	1,081	0.114	0.318	0.000	0.000	0.000
Number of Segments	1,081	2.181	2.177	0.000	1.000	3.000
ICW	1,081	0.030	0.170	0.000	0.000	0.000
Macroeconomic Variables						
Credit Spread	1,081	0.987	0.251	0.840	0.920	1.110
Term Spread	1,081	1.450	0.907	0.770	1.630	2.180

Panel B: Correlation (N=1,081)

		A	B	C	D	E	F
Data Breach	A	1					
Post	B	-0.015	1				
*Data Breach*Post*	C	0.536***	0.613***	1			
Ln(Loan Spread)	D	0.077**	0.224***	0.214***	1		
Secured	E	0.057*	0.059*	0.109***	0.560***	1	
Number of Total Covenants	F	-0.061**	0.041	0.014	0.150***	0.387***	1

This table presents the descriptive statistics and correlation of the main variables in regressions, including bank loan characteristics, and data breach, firm-level, and macroeconomic variables and reports the correlation among the main variables. *, **, and *** indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

TABLE 3
First Stage of Propensity Score Matching (PSM) Analysis

Panel A: Probit Regression

	(1)
Dependent Variable	*Data Breach Event*$_t$
Firm Size$_{t-1}$	0.154***
	(10.99)
Leverage$_{t-1}$	-0.016
	(-0.22)
ROA$_{t-1}$	0.089***
	(4.56)
Operational Risk$_{t-1}$	0.358*
	(1.81)
Tangibility$_{t-1}$	-0.005
	(-1.11)
Z-score$_{t-1}$	-0.086
	(-0.89)
MB$_{t-1}$	-0.000**
	(-2.20)
IT Expertise$_{t-1}$	0.233***
	(4.10)
IT Reputation$_{t-1}$	0.222**
	(2.17)
Number of Segments$_{t-1}$	-0.009
	(-0.68)
ICW$_{t-1}$	-0.134
	(-0.93)
Intercept	-7.881***
	(-25.78)
Industry/Year	Included
Number of Observations	57,462
Pseudo R^2	0.166
AUC	0.870

Panel B: Difference in Variables for firms Matched by PSM (Number of Observations: 426)

Variable	Treated	Control	Diff.	P
Firm Size	8.308	8.190	0.118	0.591
Leverage	0.459	0.485	-0.026	0.768
ROA	0.122	0.124	-0.002	0.859
Operational Risk	0.059	0.077	-0.018	0.137
Tangibility	0.431	0.449	-0.018	0.643
Z-score	3.245	2.129	1.116	0.408
MB	2.330	2.455	-0.125	0.859
IT Expertise	0.364	0.341	0.023	0.616
IT Reputation	0.092	0.083	0.009	0.735
Number of Segments	2.055	1.853	0.203	0.252
ICW	0.028	0.009	0.018	0.154

The dependent variable is *Data Breach Event*. The variables are defined in Appendix A. In the parentheses below the coefficient estimates are robust z-statistics based on standard errors adjusted for heteroskedasticity. For brevity, the coefficients for the industry and year dummies are not reported. *, **, and *** indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

TABLE 4
Relation between Data Breaches and Bank Loan Contracting: Main Test

	(1)	(2)	(3)
Dependent Variable	*Ln(Loan Spread)*	*Secured*	*Number of Total Covenants*
Data Breach*Year -1	-0.014	-0.008	-0.332
	(-0.17)	(-0.18)	(-0.96)
Data Breach*Year 0	0.052	0.067	-0.074
	(0.66)	(1.41)	(-0.21)
Data Breach*Year 1	**0.221****	**0.114****	**0.783***
	(2.41)	**(2.26)**	**(1.84)**
Data Breach*Year 2+	**0.037**	**0.097****	**0.830****
	(0.49)	**(2.14)**	**(2.13)**
Ln(Loan Size)	-0.369***	-0.129***	0.196
	(-6.82)	(-3.95)	(0.82)
Ln(Loan Maturity)	0.197***	0.114***	-0.145
	(4.56)	(4.79)	(-0.91)
Performance Pricing	-0.193***	-0.029	2.135***
	(-5.25)	(-1.19)	(9.44)
Firm Size	-0.089	-0.024	-1.096*
	(-0.82)	(-0.43)	(-1.94)
Leverage	0.360*	-0.237*	-2.853**
	(1.93)	(-1.85)	(-2.46)
ROA	-3.625***	-0.848	-10.396**
	(-3.93)	(-1.57)	(-2.51)
Operational Risk	0.593	-0.070	6.207
	(0.56)	(-0.12)	(1.53)
Tangibility	-0.322*	0.089	-1.232
	(-1.66)	(0.69)	(-1.13)
Z-score	0.064	-0.038	-0.186
	(1.00)	(-1.30)	(-0.71)
MB	0.002	0.008	-0.029
	(0.20)	(1.51)	(-0.44)
IT Expertise	-0.044	-0.078*	0.065
	(-0.70)	(-1.85)	(0.20)
IT Reputation	0.089	-0.060	0.309
	(1.00)	(-1.10)	(0.86)
Number of Segments	-0.064***	-0.005	0.185*
	(-2.84)	(-0.33)	(1.68)
ICW	-0.162	0.045	0.608
	(-0.92)	(0.49)	(0.72)
Credit Spread	0.375***	0.130*	1.774***
	(3.49)	(1.87)	(3.60)
Term Spread	0.119**	0.092**	0.950***
	(2.08)	(2.51)	(3.33)
Intercept	5.339***	0.812	10.657*
	(5.12)	(1.32)	(1.80)
Firm/Year	Included	Included	Included
Number of Observations	1,081	1,081	1,081
R^2	0.756	0.672	0.609

The dependent variables are *Ln(Loan Spread)*, *Secured*, and *Number of Total Covenants*. The variables are defined in Appendix A. In the parentheses below the coefficient estimates are robust t-statistics based on standard errors adjusted for heteroskedasticity. For brevity, the coefficients for the firm and year dummies are not reported. *, **, and *** indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

TABLE 5
Relation between Data Breaches and Bank Loan Contracting: Cross-sectional Test

Panel A: Type of Data Breach

	(1)	(2)	(3)
	Ln(Loan Spread)	*Secured*	*Number of Total Covenants*
Criminal Data Breach*Post	0.270**	0.199**	0.334
	(2.01)	(2.45)	(0.52)
Controls	Included	Included	Included
Firm/Year	Included	Included	Included
Number of Observations	587	587	587
R^2	0.712	0.695	0.656

Panel B: Number of Records Lost in a Data Breach

	(1)	(2)	(3)
	Ln(Loan Spread)	*Secured*	*Number of Total Covenants*
More Records*Post	0.265*	0.241*	-2.145
	(1.94)	(1.82)	(-1.58)
Controls	Included	Included	Included
Firm/Year	Included	Included	Included
Number of Observations	587	587	587
R^2	0.710	0.693	0.660

Panel C: Vulnerable Industries

	(1)	(2)	(3)
	Ln(Loan Spread)	*Secured*	*Number of Total Covenants*
Vulnerable Industries*Post	0.244**	0.156*	1.151*
	(2.05)	(1.87)	(1.76)
Controls	Included	Included	Included
Firm/Year	Included	Included	Included
Number of Observations	587	587	587
R^2	0.712	0.694	0.660

The dependent variables are *Ln(Loan Spread)*, *Secured*, and *Number of Total Covenants*. The variables are defined in Appendix A. In the parentheses below the coefficient estimates are robust t-statistics based on standard errors adjusted for heteroskedasticity. For brevity, the coefficients for control variables and firm and year dummies are not reported. *, **, and *** indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

TABLE 6
Effect of Data Breaches Conditional on IT Reputation and ICWs

Panel A: Data Breach and IT Reputation

	(1)	(2)	(3)
	Ln(Loan Spread)	*Secured*	*Number of Total Covenants*
IT Reputation*Post	0.293*	0.178*	0.980
	(1.71)	(1.74)	(1.07)
Controls	Included	Included	Included
Firm/Year	Included	Included	Included
Number of Observations	587	587	587
R^2	0.709	0.694	0.656

Panel B: Data Breach and ICWs

	(1)	(2)	(3)
	Ln(Loan Spread)	*Secured*	*Number of Total Covenants*
ICW*Post	-0.334	-0.0910	-0.691
	(-0.84)	(-0.48)	(-0.48)
Controls	Included	Included	Included
Firm/Year	Included	Included	Included
Number of Observations	587	587	587
R^2	0.708	0.692	0.655

The dependent variables are *Ln(Loan Spread)*, *Secured*, and *Number of Total Covenants*. The variables are defined in Appendix A. In the parentheses below the coefficient estimates are robust t-statistics based on standard errors adjusted for heteroskedasticity. For brevity, the coefficients for control variables and firm and year dummies are not reported. *, **, and *** indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

TABLE 7
Relation between Data Breaches and Bank Loan Contracting: Data Breach Notification Laws

Panel A: Effective Date of Data Breach Notification Laws

State	Effective Date	State	Effective Date	State	Effective Date
Alabama	2018/6/1	Louisiana	2006/1/1	Oklahoma	2008/11/1
Alaska	2009/7/1	Maine	2006/1/31	Oregon	2007/10/1
Arizona	2006/12/31	Maryland	2008/1/1	Oregon	2013/9/12
Arkansas	2005/8/12	Massachusetts	2007/10/31	Pennsylvania	2006/6/20
California	2003/7/1	Michigan	2007/7/2	Rhode Island	2016/7/2
California	2014/9/30	Michigan	2011/4/1	South Carolina	2009/7/1
Colorado	2006/9/1	Minnesota	2006/1/1	South Carolina	2013/4/23
Connecticut	2006/1/1	Mississippi	2011/7/1	South Dakota	2018/7/1
Delaware	2005/6/28	Missouri	2009/8/28	Tennessee	2005/7/1
Delaware	2010/6/10	Montana	2006/3/1	Tennessee	2016/7/1
D.C.	2007/7/1	Nebraska	2006/4/10	Tennessee	2017/4/4
Florida	2014/7/1	Nebraska	2016/7/20	Texas	2009/4/1
Georgia	2005/5/5	Nevada	2005/10/1	Texas	2013/6/14
Hawaii	2007/1/1	Nevada	2006/1/1	Utah	2007/1/1
Hawaii	2008/4/17	Nevada	2008/1/1	Utah	2009/5/12
Idaho	2006/7/1	Nevada	2011/10/1	Vermont	2012/5/8
Illinois	2006/6/27	New Hampshire	2007/1/1	Vermont	2013/5/13
Illinois	2012/1/1	New Jersey	2006/1/1	Virginia	2008/7/1
Illinois	2017/1/1	New Mexico	2017/6/16	Virginia	2011/1/1
Indiana	2006/7/1	New York	2005/12/7	Virginia	2017/7/1
Indiana	2009/7/1	North Carolina	2005/12/31	Washington	2005/7/24
Iowa	2008/7/1	North Carolina	2009/7/27	Washington	2010/7/1
Iowa	2014/7/1	North Dakota	2005/6/1	West Virginia	2008/6/6
Kansas	2007/1/1	North Dakota	2013/4/18	Wisconsin	2006/3/31
Kentucky	2014/7/15	Ohio	2006/02/29	Wyoming	2007/7/1
Kentucky	2015/1/1	Ohio	2007/3/30		

Panel B: Relation between Data Breaches and Bank Loan Contracting: Strengthened by Data Breach Notification Laws

	(1)	(2)	(3)
	Ln(Loan Spread)	*Secured*	*Number of Total Covenants*
*Post Notification Law*Post*	0.205**	0.002	1.249***
	(2.05)	(0.02)	(2.69)
Controls	Included	Included	Included
Firm/Year	Included	Included	Included
Number of Observations	587	587	587
R^2	0.710	0.692	0.662

In panel B, the dependent variables are *Ln(Loan Spread)*, *Secured*, and *Number of Total Covenants*. The variables are defined in Appendix A. In the parentheses below the coefficient estimates are robust t-statistics based on standard errors adjusted for heteroskedasticity. For brevity, the coefficients for control variables and firm and year dummies are not reported. *, **, and *** indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

TABLE 8
Effect of Data Breaches on Reputation Loss, Operational Performance, Default Risk and Covenant Violation, and Information Risk

Panel A: Reputation Loss

	(1) *Loss of Major Customers*	(2) *Market Share Growth*
Data Breach*Post	0.034*	-0.034**
	(1.91)	(-2.14)
Controls	Included	Included
Firm/Year	Included	Included
Number of Observations	1,081	1,081
R^2	0.540	0.564

Panel B: Operational Performance

	(1) *ROA*	(2) *CFO*
Data Breach*Post	-0.011**	-0.014**
	(-2.35)	(-2.55)
Controls	Included	Included
Firm/Year	Included	Included
Number of Observations	1,081	1,081
R^2	0.856	0.648

Panel C: Default Risk and Covenant Violation

	(1) *Prob. Bankruptcy*	(2) *Covenant Violation*
Data Breach*Post	0.002**	0.041*
	(2.34)	(1.67)
Controls	Included	Included
Firm/Year	Included	Included
Number of Observations	1,081	577
R^2	0.805	0.718

Panel D: Information Risk

	(1) *Stock Illiquidity*	(2) *Std. Return*
Data Breach*Post	0.013***	0.007**
	(4.18)	(2.45)
Controls	Included	Included
Firm/Year	Included	Included
Number of Observations	1,057	1,055
R^2	0.847	0.792

The dependent variables are *Loss of Major Customers*, *Market Share Growth*, *ROA*, *CFO*, *Prob. Bankruptcy*, *Covenant Violation*, *Stock Illiquidity*, and *Std. Return.* The variables are defined in Appendix A. In the parentheses below the coefficient estimates are robust t-statistics based on standard errors adjusted for heteroskedasticity. For brevity, the coefficients for control variables and firm and year dummies are not reported. *, **, and *** indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.

TABLE 9
Data Breaches, Remediation, and Bank Loan Contracting

	(1) *Ln(Loan Spread)*	(2) *Secured*	(3) *Number of Total Covenants*
Remediation*Post	-0.149**	-0.068**	0.026
	(-2.26)	(-2.40)	(0.16)
Controls	Included	Included	Included
Firm/Year	Included	Included	Included
Number of Observations	587	587	587
R^2	0.710	0.698	0.656

The dependent variables are *Ln(Loan Spread)*, *Secured*, and *Number of Total Covenants*. The variables are defined in Appendix A. In the parentheses below the coefficient estimates are robust t-statistics based on standard errors adjusted for heteroskedasticity. For brevity, the coefficients for control variables and firm and year dummies are not reported. *, **, and *** indicate statistical significance at the 10 percent, 5 percent, and 1 percent levels, respectively, in a two-tailed test.