Data Breach Disclosure and Insider Trading

Xi Chen
xc144@georgetown.edu

Gilles Hilary*
Gilles.hilary@georgetown.edu

Xiaoli (Shaolee) Tian
xt51@georgetown.edu

McDonough School of Business, Georgetown University, Washington, DC 20057

March 2019

Very first draft –

Please do not quote without permission.

*Corresponding author: Gilles Hilary, Georgetown University, 37th and O Streets, N.W., Washington D.C. 20057, gilles.hilary@georgetown.edu.

Data Breach Disclosure and Insider Trading

Abstract

Recent data breach have generated concerns that insiders might use cyber risk related nonpublic information in their trading. Using the staggered adoption of data breach notification laws at the state level, we examine whether mandatory breach disclosure affects insider selling behavior. We find that insiders' selling profit is larger and selling speed is faster after the laws become effective. Furthermore, the effects of the laws are more prominent for firms that likely suffer from higher data breach risk. However, the effect is mitigated in states with stricter laws. These findings highlight the unintended consequence of prompting opportunistic insider selling.

Keywords: Cybersecurity, Data breach, Regulation, Disclosure, Insider trading

JEL Classification Codes: G18; M41; K22; K24

I. Introduction

The 2019 Global Risks Report from the World Economic Forum ranked cyber-risk as one of the top ten risks in terms of both likelihood and impact. As a result, cybersecurity and its related disclosure have become a significant concern for regulators. For instance, the SEC formed a Cyber Unit that focuses on investigating cyber related delinquencies in 2017 and updated its guidelines on cyber risk disclosure in 2018. However, cyber-risk is a multi-facetted threat ranging from the destruction of physical assets (e.g., Aramco), the theft of intellectual property (e.g., Nortel) or the damage to electronic system (e.g., Maersk). Yet, one of the most sensitive topics for the public may be the massive losses of data that violate individual privacy. From 2005 to 2010, data breaches have compromised an estimated 350 million records (Shaw 2010). High profile data leaks such as the ones that occurred at Equifax or Marriott have made headlines on regular basis and regulators have published a slew of legal instruments to address this problem. For example, the European Union has recently the General Data Protection Regulation (GDPR), a wide-ranging data protection legislation.

Naturally, insider trading provisions apply to this area as well. Nevertheless, in its 2018 guideline, the SEC specifically mentioned that insider trading based on nonpublic information of cyber risk or cyber incident is prohibited. The recent high profile SEC investigations and charges for data breach related insider trading accentuated this concern into the public spotlight. For instance, the SEC charged executives at Equifax with insider trading related to the data breach in 2017.

We examine the relevance of this issue by examining the effect of mandatory data breach disclosure on insider trading behaviors. There is a long held view among regulators that "Sunlight is said to be the best of disinfectants."[1] This view has had major influences on

[1] The quote is attributed to Justice Louis D. Brandeis (https://www.brandeis.edu/legacyfund/bio.html).

disclosure regulations and securities laws in the U.S., including disclosures on cyber risks. Evidence from academic studies is, however, rather mixed as regulations often induce unintended behaviors or other externalities.[2] To investigate the effect of mandatory cyber risk disclosure on insider trading, we use the staggered adoption of data breach disclosure laws at the state level as our setting.

From 2003 to 2018, all states and the District of Columbia have implemented state-level disclosure regulations for security breaches. These laws require organizations to notify consumers or affected parties of the breach incident after it is discovered. Existing studies demonstrate that public disclosures of data breach incidents have increased substantially after each state implemented the notification law (e.g., Romanosky, Telang and Acquisti 2011; Ashraf and Sunder 2018).

The effect of these laws on insider trading is undetermined *ex ante*. On the one hand, the mandated data breach disclosure may reduce opportunistic insider trading by speeding the public revelation of the data breach incidents and thus constraining executives' ability to trade on private information. Further, mandatory disclosure of breaches may impose additional costs on firms. Public disclosure of data breaches may raise stakeholders' concern about firms' cyber risk management. It can increase firms' reputation concerns and invest more to improve cybersecurity (Romanosky et al. 2011; Shaw 2010). Given these potential additional costs, state legislations may encourage firms and their executives to mitigate the likelihood, size and consequences of data breaches. The potential ensuing improvement in cybersecurity may reduce data breach risks and incidents, and thus reduce managers' opportunity to trade on negative events by preventing the events in the first place.

[2] See Fung, Graham, Weil 2007; Gao, Wu and Zimmerman 2009; Beyer, Cohen, Lys and Walther 2010; Berger 2010; Tian 2015; Leuz and Wysocki 2016.

On the other hand, the required breach disclosures may also prompt opportunistic insider trading, particularly, opportunistic sales. Insider profits stemming from sales is facilitated by the existence of predictable sharp drops in price. The revelation of a data breach may create such setting. Essentially, mandating breach disclosures will reveal a negative event to the market that may not have become public otherwise. If executives anticipate that breach disclosures will result in a drop in their company's stock prices then this required public disclosure of breach incidents may prompt managers to sell their shares ahead of time to avoid losses. Existing studies often link public revelation of bad news to opportunistic insider sales ahead of negative news announcements (e.g., Ke, Huddart, and Petroni 2003; Dechow, Lawrence, and Ryans 2016; Ryan, Tucker, and Zhou 2016). Anecdotal evidence from high profile cases such as Yahoo and Equifax also suggest that insiders do try to sell their shares after discovering breach incidents but before its public disclosures. Thus, it is plausible that mandated data breach disclosures may also increase managers' opportunities to sell their shares so that they can avoid future personal losses. We empirically investigate the effect of these legislations.

Using a different-in-different design (DID), we find that insider sales' profits (i.e. losses avoided) are significantly larger after states implement data breach notification laws. We verify that the parallel trend assumption holds in our DID design. We find that there is no significant difference in selling profits and selling speed for our treated and control samples in the pretreatment period. In other words, as expected, the effect of state notification laws occur after the laws become effective but not before. These findings suggest that mandated disclosures of data breach incidents may have unintended consequence of prompting executives to sell their shares ahead of negative news revelation quicker.

Aside from considering the profitability of the trade, we also examine the speed of execution. Existing insider trading literature evidence that the threat of litigation restricts insider selling immediately before public revelation of bad news (e.g., Ke et al. 2003; Billings et al. 2015). Indeed, regulators such as the SEC and FINRA screen trades for potential suspicious behavior around public announcement of significant news (Nathan 2017). Thus, the ability to spread information-based trades over longer period of time is valuable for insiders. Breach laws constrain this ability by forcing earlier disclosure. Our results indicate that trading speed increase after the passage of the laws.

Next, we explore whether the effects of data breach notification laws differ conditional on how strict the laws are. As of 2018, all states have adopted the data breach notification laws but with key differences in their language. In particular, they vary in their strictness, frequency of updates and specificity. We find the negative externality on insider trading created by the breach laws is mitigated when the laws are stronger on each of these dimensions.

Furthermore, we investigate the effect of firms' ex-ante data breach risks on the effect of the state laws. To quantify firms' data breach risk, we identify the top 20% of the most impactful data breach incidents from a major database of data breaches and measure how other firms' price reacted to these data breach incidents. Firms that react badly to the announcement of a breach somewhere else are labeled as high data breach risks. Essentially, this method captures an ex ante measure of the exposure to data breach risk. As expected, we find that the effect of data breach law on insider trading is concentrated in firms with high data breach risk exposure.

Lastly, we perform two placebo test to support our conclusions. First, we run our tests using purchase instead of sales. The public disclosure of breach incidents captures a revelation of bad news event. Managers have incentives to sell ahead of such news disclosure to avoid losses. The same predication does not apply to purchases. As predicted, we find that the state breach notification laws have no significant impact on insider purchase profits or speed.

Second, we run our main analysis splitting our sample between routine and non-routine sales. Executives selling their stocks ahead of a breach announcement should be a non-routine transaction. Existing literature finds that non-routine trades capture managers' opportunistic use of nonpublic information in their trading strategies because non-routine trades earn substantially higher profits (e.g, Cohen, Malloy, and Pomorski 2012). We find that the effects of the law on insider selling profits and speed are significant only for non-routine sales.

Our findings have potential policy implications. First, the SEC is concerned about insiders using their nonpublic information to trade on cyber risks and incidents. In an effort to improve cyber risk disclosures, the SEC issued guidelines in 2011 and then again in 2018. Currently, there is no federal law specifically designed for data breach disclosures. However, the Data Security and Breach Notification Act has been repeatedly introduced in the last few years by different senators and house representatives.[3] Although state-level breach laws have led to an increase in the number of breach disclosure, our findings indicate that these laws have increased insiders' selling profits and speed. However, stricter laws appear to mitigate such negative externality. This suggests that the design of the cyber risk disclosure regulations is important. Stricter design might lead to less negative unintended consequences. Trading on nonpublic information is one of the most significant threat to the SEC's goal of "leveling the playing field" for different investors in the capital market. Our study informs the SEC about insider trading behavior on cyber related nonpublic information and how it might be affected by other non-capital market disclosure regulations.

Furthermore, this study also contributes to our understanding of the disciplinary mechanisms for insider trading. Existing literatures indicate that opportunistic insider trading are reduced when insider trading regulations are implemented, when firms set restrictions such

[3] For instance, one was introduced in 2013 by Sen. John D. Rockefeller, another was introduced in 2015 by Rep. Marsha Blackburn, and the most recent one was introduced by Sen. Bill Nelson.

as blackout window for insider trading, when insiders are required to disclose its trading faster and when media disseminates the disclosure (e.g., Dai, Parwada, and Zhang 2015; Jagolinzer, Larcker and Taylor 2011; Brochet 2010). Our study extends existing literature and find that mandated disclosures of a negative news event may actually prompt insider to sell faster and to avoid losses from future bad news. Thus, disclosure of nonpublic information may not be enough to preclude managers from taking advantage of nonpublic information in their trading behavior. Careful designs in the disclosure regulation and enforcement are also necessary to discipline insiders' trading behaviors.

II. Disclosure Laws

As of 2019, there is no comprehensive United States (US) federal law governing the disclosures of data breach incidents.[4] However, from 2002 to 2018, all states in the U.S. have adopted data breach notification laws. The first state to adopt data a breach notification law was California. The law was adopted in 2002 and became effective in 2003. Subsequently, all states have adopted laws that are broadly consistent in their approach but do vary in the establishment of specific provisions. Many of these laws contain provisions pertaining to the breach definition and coverage, required notification details, notification timeliness, penalties, and enforcement. Aside from some relatively minor variations, the first dimension is largely similar across states. A data breach is generally defined as a situation when an unauthorized person or entity obtain sensitive information. The breached entity is liable to notify the affected parties and third parties, such as credit agency or attorney general if applicable, for the incident.

Although the required content of the notification varies significantly across different states, the basic required notification is similar. It typically includes some general description

[4] However, firms under the jurisdiction of the SEC or falling under specific statutes (e.g., Health Insurance Portability and Accountability Act of 1996) may have additional specific requirements.

of the breach incident such as the date of the breach, and information that is affected by the breach. Beyond these general requirement, states may also require more detailed disclosures. For instance, California requires disclosures of any delay due to law enforcement request. Florida requires disclosure of firm policies regarding breaches and their remedies. States either requires breached entity to disclose as soon as possible (e.g., District of Columbia) or specify a deadline for disclosure (e.g., no later than 45 days in Ohio). Penalties can vary significantly across states. While some states do not specify penalties for violating the law (e.g., Georgia), others specify do (e.g. Alaska). The last major dimension, enforcement, also vary greatly across states. At one end of the spectrum, some states disallow private rights of action (e.g. Florida) while at the other end, some states (e.g., Iowa) specifically require entities to disclose breaches to Attorney General and allow this office to bring law suits against entities that violate the law.[5]

Overall, the intent of disclosure requirement is to make the breach incidents publicly known, and as a result, to induce organizations to invest to improve their cybersecurity. Figure 1 shows the time series of the number of disclosure before and after the passage of the breach laws. It indicates an uptick in the number of reported cases. Naturally, since the disclosure policy is not constant, it is not possible to evaluate whether the actual number of breaches changes after the implementations of the different state laws.

Existing studies find mixed evidence on how the market reacts to data breach disclosures with some find significant and negative market reaction while others find little reaction (Hilary, Segal and Zhang 2016; Mitts and Talley 2018). However, results from existing study suggest that firms improve their cybersecurity after states implement notification laws. For instance, Romanosky, Telang and Acquisti (2011) use identity theft data from U.S. Federal trade Commission and find that the adoptions of data breach notification at the state

[5] In Section IV we will exploit these differences and build cross-sectional tests on the strictness of law.

level do reduce the identity theft caused by data breaches. Ashraf and Sunder (2018) shows that firms' cost of equity decreases after states adopt notification laws. If disclosing data breach incidents raises firms' concerns for reputation costs then firms might invest more resources to reduce such incidents.

III. Data and Descriptive Statistics

Table 1 summarizes our sample selection procedures. Our initial sample includes insider transactions of firms listed on the NYSE, AMEX, or NASDAQ covered in Thomson Reuters Insider Filings (Form 4) from 2000 to 2017. It starts three years before California implements the data breach disclosure law in 2003 and ends three years after Florida and Kentucky implements the data breach disclosure law in 2014. To ensure that we have sufficient data for both pre- and post-implementation time period, we excluded three states that implemented the data breach notification law in 2017 and 2018 (New Mexico, Alabama and South Dakota). We summarize the implementation timeline for each state in Appendix A.

The insider transaction data contains insider trades information from directors, officers, and beneficial owners with holdings greater than 10 percent of a firm's stock. All of these insider transactions are subject to disclosure requirements as defined in Section 16 of the Exchange Act of 1934 until August 2002 and in Section 403 of the Sarbanes-Oxley Act subsequently.[6] Our analyses focus on insiders' open market sales, hence we exclude option exercises, private transactions and open market purchases from our main tests (e.g., Massa et al. 2015; Cohen, Malloy, and Pomorski 2012; Dai et al. 2016).

[6] In robustness check, we exclude the observations before 2002 and obtain qualitatively similar results.

We further limit the sample by requiring that share codes in CRSP be 10 or 11, and we exclude the following transactions from the sample: (1) transactions with less than 100 shares or those with trading prices less than $2; (2) transactions with traded prices outside the range between the daily low and high prices reported in CRSP; (3) transactions with the number of shares exceeding the total number of shares outstanding in CRSP; (4) transactions with the number of shares traded exceeding the total daily trading volume in CRSP; and (5) regulated firms in the financial or utilities industries (firms with SIC codes between 6000 and 6999 or between 4900 and 4999) (e.g. Gao, Lisic, and Zhang 2014; Dai et al. 2016).

These restrictions result in a sample of 31,535 firm-year observations. We combine the initial sample with COMPUSTAT/CRSP data.. After merging and deleting observations with missing data, we obtain a final sample of 28,800 firm-year observations. However, the sample size for each test varies depending on the availability of the data in the analysis due to variations in data requirements across tests. In some of the test, we use a list of data breach incidents identified by Private Rights Clearinghouse's Chronology of Data Breaches (the breach database hereafter).[7]

< INSERT TABLE 1 >

We define our different variables in Appendix B. In particular, *SELL_PROFIT* is the profitability of insider sales defined as the losses avoided by selling shares. Similar to Huddart and Ke (2007) and Skaife, Veenman, and Wangerin (2013), we measure insider trading profits as the one-year buy and hold abnormal return on the stock over the following the trade multiplied by the value of the trade (in millions of dollars).[8] For sales, we take the negative of

[7] The data can be accessed publicly online http://www.privacyrights.org/data-breach.

the product to represent the loss avoided by selling the stocks.[9] Lastly, we aggregate individual transactions at the firm-year level. *SELL_SPEED* is insider selling speed. Similar to Massa et al. (2015), this variable is defined as the number of days that an insider in a given firm takes to complete sale transactions in a year. We take the natural logarithm transformation of the number of days (plus one), multiplied by -1 to denote the speed. The larger the *SELL_SPEED*, the faster the insiders' trading speed is.

Table 2, Panel A, presents the descriptive statistics for the main variables for our sample. 67% (33%) of firm-year observations in our sample are after (before) the implementation of a data breach disclosure law. The mean SELL_PROFIT (profit associated with insider sales) is around 200,000 dollars. In addition, we find that 30% of our sample sales transactions are made by insiders of firms with negative net income during the most recent fiscal year (LOSS). 56%of our sample sales transactions are made by insiders of firms reporting non-zero R&D expenditures (RND). The mean BTM is 0.478, and average size of firms in our sample is 6.67 million dollars in market capitalization (SIZE). The mean of stock return volatility is 0.032. In general, the magnitude of our variables are consistent with prior literature (e.g., Skaife, Veenman, and Wangerin 2013; Huddart and Ke 2007; Chi, Pincus, and Teoh 2014).

In Panel B of table 2, we present Pearson correlations. The correlations between our dependent variables (SELL_PROFIT and SELL_SPEED) and our variable of interest (POST, an indicator variable that takes the value of 1 after the implementation of breach laws) are negative and significant (p-value<0.01). At a first glance, this univariate correlation suggests that sates' notification laws will reduce insiders' opportunistic selling behavior. However, prior literature (e.g., Brochet 2010) shows that the enforcement of anti-insider trading provision and the speed of Form 4 disclosure increased over time. Consistent with these prior findings, Figure

2 shows a secular decline in overall profitability of insider trading in our sample period. Once we ensure we address the effects of this time trend, the univariate correlations become positive. For instance, the univariate correlation between post and selling profit (speed) becomes 0.148 (0.191) after controlling for the time trend effects. The majority of control variables are significantly correlated with insider selling profits and speed and have the predicted sign.

< INSERT TABLE 2>

IV. Research Design and Results Discussion

IV.1 Impact of staggered adoption of data breach disclosure regulation on insider trading

We use a difference-in-difference approach to examine how the implementation of the data breach disclosure law affects the insiders' sales behaviors in firms headquartered in affected states. Our primary analyses follow the prior literature (e.g., Bertrand and Mullainathan 2003; Armstrong, Balakrishnan, and Cohen 2012)) and utilize the following specification:

$$SELL\_PROFIT(SELL\_SPEED)j,t = \alpha + \beta 1POSTj,t + \sum \beta nControlsj,t + \sum \beta iFirms\ Fixed\ Effectsj,t + \sum \beta mYear\ Fixed\ Effectsj,t + \varepsilon jit$$

Our variable of interest in this study is *POST.* We include firm fixed effects and year fixed effects. β_1 essentially captures a difference-in-difference estimator where the control group is firms in states that have not yet implemented a data breach disclosure law as of year t or implemented a data breach disclosure law effectively prior to year t (e.g., Bertrand and Mullainathan 2003; Armstrong, Balakrishnan, and Cohen 2012). We cluster standard errors by state of headquarters because *POST* is a state-level variable.

We control for firm size (*SIZE*) because Seyhun (1986) finds that insiders buy more in smaller firms and sell more in larger firms, while Lakonishok and Lee (2001) finds that insiders trade more profitably in smaller firms. We also control for the book-to-market ratio (*BTM*), because prior research shows that insiders trade more actively in low book-to-market firms (Rozeff and Zaman 1998). Following Huddart and Ke (2007) and Brochet (2010), we also include a *LOSS* indicator variable to control for a firm's financial performance. We control for an R&D indicator variable because insider sales are likely to be more informative in firms with higher R&D intensity, in which information asymmetry problems are perceived to be higher (Aboody and Baruch 2000). We also include *RETVOL*, the standard deviation of daily stock returns over the fiscal year and include DV, defined as cash dividend scaled by shareholder equity (SEQ) to control for earnings growth opportunities (Chi, Pincus, and Teoh 2014).

Table 3, Columns (1) and (2), report the results of our regressions when we consider selling profits and speed, respectively. The coefficients for *POST* are positive and significant in both cases (p-value<0.01), indicating that the implementation of data breach disclosure laws has a positive and statistically significant impact on the sales behaviors of insiders. Specifically, the estimated coefficient in Column (1) implies that after the implementation of data breach disclosure laws, on average, affected firms' insiders avoid 278,000 dollars in losses by selling shares ahead of data breach incident known to public. Conversely, the coefficient reported in Column (2) suggests that the implementation of data breach disclosure law is associated with a 12% increase in the average selling speed of insider transactions.[10] We then restrict our definition of insiders to officers and directors and exclude large shareholders. Arguably, officers and directors might have firsthand information about their firms' cyber risks or data breaches. Thus, one should observe the findings from these insiders if insiders are really trading on cyber risk related information. Untabulated results indicate that our conclusions hold if we focus on this group. Second, California is the first state that adopted the notification breach laws and home to many data driven firms. Untabulated results indicate that our conclusions hold if we exclude this state. Third, the Sarbanes-Oxley Act was enacted in 2002 and

[10] The impact of data breach disclosure law on insiders' selling time span is (exp (0.113) – 1) * 100 = 12.

substantially modified the corporate environment (our main sample starts in 2000).[11] Untabulated results indicate that our conclusions hold if we restrict our sample to the post-SOX era.

Overall, the results from Table 3 suggest that insiders in firms operating in affected states might exploit their information advantage to a greater extent and sell their stocks faster ahead of public revelation of cyber breach incidents. In other words, an increase of likelihood that data breach information will become publicly known in the near future due to an exogenous regulation prompt insiders to sell their shares faster to avoid future losses.

< INSERT TABLE 3>

Next, we examine the validity of our parallel trend assumption imbedded in our DID design. Essentially, we investigate when the changes in selling behaviors occured relative to the implementation of the data breach disclosure laws. To this end , we create a series of indicator variables EFFECTIVE indexed t+i from t-2 to t+2 with t=0 being the year of implementation of a breach law in the state where the firm is headquartered. The variables take the value of one if a law is passed within t-i. The results are reported in Table 4. We find that the coefficients on $EFFECTIVE^{-2}$ and $EFFECTIVE^{-1}$ are statistically insignificant, have inconsistent signs and have a small magnitude, while the coefficients on $EFFECTIVE^{0}$, $EFFECTIVE^{+1}$, $EFFECTIVE^{+2}$ are all consistently positive and statistically significant. Overall, these results support the validity of the parallel trend assumption in our setting.

< INSERT TABLE 4>

IV.2 Does the effect vary conditional on the strictness of the law?

[11] In particular, Section 403 requires insiders to report their trades to the Securities and Exchange Commission (SEC) on a Form 4 within two business days. Until August 2002, the requirement had only been to file the form within ten days after the close of the calendar month in which the transaction had occurred.

As discussed above, data breach disclosure laws generally require firms to notify each affected individual when that person's personally identifiable information is obtained by an unauthorized third-party. However, not all disclosure laws are identical in their requirements. Thus, the strictness of these laws can have a differential impact on insiders' incentives or opportunities to avoid losses stemming from the disclosures of data breach incidents. Extant research suggests that regulation design can significantly affect its effectiveness of the law and amount of externalities it creates (e.g., Meyer and Rowan 1977, Fung, Graham and Weil 2007). We surmise that states where the law is stricter prompt a more significant response from firms that are covered. We summarize four key dimensions that have been identified as significant factors in studies of data breaches (e.g., Joerling 2010, Peters 2014, Skinner 2003, Romanosky, Teland and Acquisti 2011, Shaw 2010).[12] The four dimensions are: (a) whether a law explicitly allow enforcement from state Attorney General; (b) whether a law imposes an explicit deadline by which firms must disclose a data breach after it has been discovered; (c) whether a law specifies explicit penalties for violating the law; (d) whether a law specifies the disclosure items in details. We first create an indicator for each one of the above dimensions and assign a value of 1 to the indicators when the answer to each of the four dimension is yes. We then construct an index (*LAWINDEX*) by summing up the indicators. .

In addition to examine the detailed design of the law by creating the *LAWINDEX*, we also test two other general characteristics that can capture the strictness of the law. First, we observe that some of the data breach disclosure laws have been amended several times since their original version. In most cases, these changes increased the strictness of the law by adding one of the four dimensions discussed above. We create a variable, *LAWCHANGE* that increase in increment of one each time the legal framework has been updated (*LAWCHANGE* ranges

[12] Some of the laws have been amended after their original implementation . To avoid adding noise and cofounds, we focus on data breach disclosure laws at their first effective date and in the form they are first implemented rather than their amended edition

from zero to four) and rescale it between zero and one. . Finally, we also observe that some laws are more detailed than other and that length and specificity is usually associated with a greater strictness. We form a third variable (*LAWLENGTH)* based on the the number of words in the law, and rank the lengths into quintiles. We scale the three variables between zero and one to increase their comparability. . Finally, we calculate LAW as the average of LAWINDEX, LAWCHANGE and LAWLENGHTH.

We then interact POST with LAW and our three different proxies and restimate our baseline model. We report the results in Table 5. We consider the effect of the strictness of the law on trade profitability in Columns (1), (3), (5) and (7). We consider the effect on trading speed in Columns (2), (4), (6) and (8).

Consistent with the notion that the strictness of the law plays a disciplinary role in mitigating unintended impact of the law on insiders' selling behaviors, the interactions between *POST* and the four variables are all significantly negative. This suggestsg that stricter, more frequently updated and more detailed legislations mitigate the effect of disclosure on the profitability and the speed of insider trading. POST remains significantly positive in all specifications. Our measures of legal strictness are statistically insignificant only when we consider LAWINDEX . < INSERT TABLE 5>

IV.3 Firms with higher data breach risks

Our main findings suggest that insiders expect future disclosures of data breach incidents will lead to a significant decline in stock price. This expectation should be stronger when the firm is facing a greater risk associated with data breaches. To test this conjecture, we estimate an ex ante measure of exposure to this risk. To do so, we list data breach incidents identified by Private Rights Clearinghouse's Chronology of Data Breaches. This database compiles breach information from various sources including Open Security Foundation listserve, Databreaches.net, Personal Health Information (PHI) Privacy, National Association for Information Destruction (NAID) and the California Attorney General. This database, which has been used in prior literature (e.g., Hilary, Segal, and Zhang (2016); Romanosky, Hoffman, and Acquisti (2014)), covers the affected entity's name, date when the data breach first became public, brief description of the breach and, for a limited number of breaches, the number of records affected. We identify breach information for business entities (i.e. exclude education, non-profit etc.) with available GVKEY on COMPUSTAT between years 2005-2017, using the entity name. We then rank the breach incidents by the number of records affected within the year when data breaches occur, and we identify the top 20% impactful data breach incidents.[13] This approach yields 426 most impactful data breach incidents by 224 unique breach companies with valid GVKEY data. We then test the market reaction of our sample firms on the data breach release date and use investors' perspective to classify firms into those that can face high data breach risk versus low risk. Specifically, we calculate the abnormal returns of our sample firms on peer firms' data breach release date and obtain the bottom 10% firms which suffer most negative market reactions. We classify these firms as high data breach risk firms, and the rest of the firms as low risk firms. We form an indicator variable, RISKFIRM, that equals one if a firm-year observations is classified as high risk in at least one year and zero if it is always classified as low risk. We then interact RISKFIRM with POST. This identification leaves us with a reasonably well balanced panel of 2,176 high risk and 2,291 low risk firms.[14] This translates to 13,296 high risk firm-year observations and 14,265 low risk firm-year observations. We present the results of this analysis in Table 6. The interaction between RISKFIRM and POST is significantly positive. Interestingly, the coefficients for *POST* are statistically insignificant, suggesting that increase in selling profits and selling speed

[13] We obtain similar results when using 30% as cut off.

[14] The data breach database is available only after 2005, which reduce the number of observations available for this test.

mostly comes from affected firms with higher data breach risk. On average, insiders from firms with greater *ex ante* exposure to the risk of data breach save 380,000 dollars more per firm-year and sell 17% faster relative to insiders in firms with low *ex ante* data breach risks.

< INSERT TABLE 6>

V. Placebo tests

We consider two placebo tests. First, the new laws only affect the disclosure of bad news (i.e., the fact that the firm has been breached). This should affect the sales of securities by insiders but not the purchase of additional shares. We investigate if this is indeed the case. Results reported in Table 7 confirm that the adoption of the notification law has no statistical or economical significant impact on either insider's purchasing profits or purchasing speed.

< INSERT TABLE 7>

Next, since the event being disclosed should be unusual in nature, we expect that the trades should reflect this. In other words, non-routine trades should be impacted but not pre-planned routine ones. To test this conjecture, we follow prior literature (e.g., Cohen, Malloy, and Pomorski (2012), Massa et al. (2015)) and identify information driven insider trades based on a "routines" and "opportunistic" classifications. Specifically, we categorize an insider as a routine trader if he or she has been trading in the same month for at least the past three consecutive years. The rest of the insiders are categorized as opportunistic (i.e. non-routine) traders if they sell in the period under consideration. We then aggregate insider trading profit and speed at the firm-year . Table 8 presents the results. As expected, the impact of data breach disclosure law concentrates in opportunistic sales. These two placebo tests further strengthen our conclusions that the state data breach notification laws prompt insiders to sell their shares earlier to avoid future losses.

< INSERT TABLE 8>

VI. Conclusion

Increased cyber risk in the last few decades has increased regulators' concerns about information security and cyber risk disclosure. Recent cases of data breaches followed by insiders trading on cyber related nonpublic information has also raised concerns that insiders might trade on their private information of cyber risks and breach incidents. Using the staggered adoption of data breach notification laws across different states we test whether mandatory data breach disclosures affect insiders' selling behavior. Our findings indicate that mandated data breach disclosures prompt managers to sell their shares to avoid future losses likely due to managers' fear that breach disclosures might put a downward pressure on stock prices. The effect is stronger for firms for which there is a stronger ex ante risk exposure to data breaches. In contrast, we also find that strict regulation tends to reduce this negative unintended consequences on insider trading.

References

Aboody, David, and Lev Baruch. 2000. “Information Asymmetry, R&D, and Insider Gains.” *Journal of Finance*..

Ali, Usman, and David Hirshleifer. 2017. “Opportunism as a Firm and Managerial Trait: Predicting Insider Trading Profits and Misconduct.” *Journal of Financial Economics*.

Alldredge, Dallin M., and David C. Cicero. 2015. “Attentive Insider Trading.” *Journal of Financial Economics*.

Armstrong, Christopher S., Karthik Balakrishnan, and Daniel Cohen. 2012. “Corporate Governance and the Information Environment: Evidence from State Antitakeover Laws.” *Journal of Accounting and Economics*.

Ashraf, Musaib and Jayanthi Sunder (2018), Mandatory disclosure of cyber incidents and the cost of equity, working paper , The University of Arizona

Badertscher, Brad A., S. Paul Hribar, and Nicole Thome Jenkins. 2011. “Informed Trading and the Market Reaction to Accounting Restatements.” *Accounting Review*.

Berger, Philip G. 2011. “Challenges and Opportunities in Disclosure Research-A Discussion of ‘the Financial Reporting Environment: Review of the Recent Literature.’” *Journal of Accounting and Economics*.

Bernile, Gennaro, Jianfeng Hu, and Yuehua Tang. 2016. “Can Information Be Locked up? Informed Trading Ahead of Macro-News Announcements.” *Journal of Financial Economics*.

Bertrand, Marianne, and Sendhil Mullainathan. 2003. “Enjoying the Quiet Life? Corporate Governance and Managerial Preferences.” *Journal of Political Economy*.

Bettis, J. C., J. L. Coles, and M. L. Lemmon. 2000. “Corporate Policies Restricting Trading by Insiders.” *Journal of Financial Economics*.

Beyer, Anne, Daniel A. Cohen, Thomas Z. Lys, and Beverly R. Walther. 2010. “The Financial Reporting Environment: Review of the Recent Literature.” *Journal of Accounting and Economics*.

Billings, Mary Brooke, and Matthew C. Cedergren. 2015. “Strategic Silence, Insider Selling and Litigation Risk.” *Journal of Accounting and Economics*.

Brochet, Francois. 2010. “Information Content of Insider Trades before and after the Sarbanes-Oxley Act.” *Accounting Review*.

Chen, Chen, Xiumin Martin, and Xin Wang. 2013. “Insider Trading, Litigation Concerns, and Auditor Going-Concern Opinions.” *Accounting Review*.

Chi, Sabrina S., Morton Pincus, and Siew Hong Teoh. 2014. “Mispricing of Book-Tax Differences and the Trading Behavior of Short Sellers and Insiders.” *Accounting Review*.

Cohen, Lauren, Christopher Malloy, and Lukasz Pomorski. 2012. "Decoding Inside Information." *Journal of Finance*.

Dai, Lili, Renhui Fu, Jun Koo Kang, and Inmoo Lee. 2016. "Corporate Governance and the Profitability of Insider Trading." *Journal of Corporate Finance*.

Dai, Lili, Jerry T. Parwada, and Bohui Zhang. 2015. "The Governance Effect of the Media's News Dissemination Role: Evidence from Insider Trading." *Journal of Accounting Research*.

Dechow, Patricia M., Alastair Lawrence, and James P. Ryans. 2016. "SEC Comment Letters and Insider Sales." *Accounting Review*.

Denis, David J., and Jin Xu. 2013. "Insider Trading Restrictions and Top Executive Compensation." *Journal of Accounting and Economics*.

Fung, Archon, Mary Graham, and David Weil. 2007. *Full Disclosure: The Perils and Promise of Transparency*. *Full Disclosure: The Perils and Promise of Transparency*.

Gao, Feng, Ling Lei Lisic, and Ivy Xiying Zhang. 2014. "Commitment to Social Good and Insider Trading." *Journal of Accounting and Economics*.

Gao, Feng, Joanna Shuang Wu, and Jerold Zimmerman. 2009. "Unintended Consequences of Granting Small Firms Exemptions from Securities Regulation: Evidence from the Sarbanes-Oxley Act." *Journal of Accounting Research*.

Hilary, Gilles, Benjamin Segal, and May H. Zhang. 2016. "Cyber-Risk Disclosure: Who Cares?" *SSRN*.

Huddart, Steven J., and Bin Ke. 2007. "Information Asymmetry and Cross-Sectional Variation in Insider Trading." *Contemporary Accounting Research*.

Jagolinzer, Alan D., David F. Larcker, and Daniel J. Taylor. 2011. "Corporate Governance and the Information Content of Insider Trades." *Journal of Accounting Research*.

Jenter, Dirk. 2005. "Market Timing and Managerial Portfolio Decisions." *Journal of Finance*.

Jin, Li, and S. P. Kothari. 2008. "Effect of Personal Taxes on Managers' Decisions to Sell Their Stock." *Journal of Accounting and Economics*.

Kallunki, Juha Pekka, Henrik Nilsson, and Jörgen Hellström. 2009. "Why Do Insiders Trade? Evidence Based on Unique Data on Swedish Insiders." *Journal of Accounting and Economics*.

Ke, Bin, Steven Huddart, and Kathy Petroni. 2003. "What Insiders Know about Future Earnings and How They Use It: Evidence from Insider Trades." *Journal of Accounting and Economics*.

Lakonishok, Josef, and Inmoo Lee. 2001. "Are Insider Trades Informative?" *Review of Financial Studies*.

Loewenson, Carl H, Smithline, Ruti (2017). Insider Trading: Law and Developments. American Bar Association. Chapter 4 is written by Nathan

Lenkey, Stephen L. 2014. "Advance Disclosure of Insider Trading." *Review of Financial Studies*.

Leuz, Christian, and Peter D. Wysocki. 2016. "The Economics of Disclosure and Financial Reporting Regulation: Evidence and Suggestions for Future Research." *Journal of Accounting Research*.

Marin, Jose M., and Jacques P. Olivier. 2008. "The Dog That Did Not Bark: Insider Trading and Crashes." *Journal of Finance*.

Massa, Massimo, Wenlan Qian, Weibiao Xu, and Hong Zhang. 2015. "Competition of the Informed: Does the Presence of Short Sellers Affect Insider Selling?" *Journal of Financial Economics*.

Peters, Rachael M. 2014. "So, you've been notified, now what? The current problem with current data breach notification laws." *Arizona Law Review*.

Piotroski, Joseph D., and Darren T. Roulstone. 2005. "Do Insider Trades Reflect Both Contrarian Beliefs and Superior Knowledge about Future Cash Flow Realizations?" *Journal of Accounting and Economics*.

Romanosky, Sasha, David Hoffman, and Alessandro Acquisti. 2014. "Empirical Analysis of Data Breach Litigation." *Journal of Empirical Legal Studies*.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management*.

Roulstone, Darren T. 2003. "The Relation between Insider-Trading Restrictions and Executive Compensation." *Journal of Accounting Research*.

Rozeff, Michael S., and Mir A. Zaman. 1998. "Overreaction and Insider Trading: Evidence from Growth and Value Portfolios." *Journal of Finance*.

Ryan, Stephen G., Jennifer Wu Tucker, and Ying Zhou. 2016. "Securitization and Insider Trading." *Accounting Review*.

Seyhun, H. Nejat. 1986. "Insiders' Profits, Costs of Trading, and Market Efficiency." *Journal of Financial Economics*.

Shaw, Abraham. 2010. "Data Breach: From Notification to Prevention Using PCI DSS." *Columbia Journal of Law & Social Problems*.

Skaife, Hollis A., David Veenman, and Daniel Wangerin. 2013. "Internal Control over Financial Reporting and Managerial Rent Extraction: Evidence from the Profitability of Insider Trading." *Journal of Accounting and Economics*.

Tian, Xiaoli Shaolee. 2015. "Does Real-Time Reporting Deter Strategic Disclosures by Management? The Impact of Real-Time Reporting and Event Controllability on Disclosure Bunching." *Accounting Review*.

Veenman, David. 2012. “Disclosures of Insider Purchases and the Valuation Implications of Past Earnings Signals.” *Accounting Review*.

Appendix A: Time Distribution of When States Implement a Data Breach Notification Law

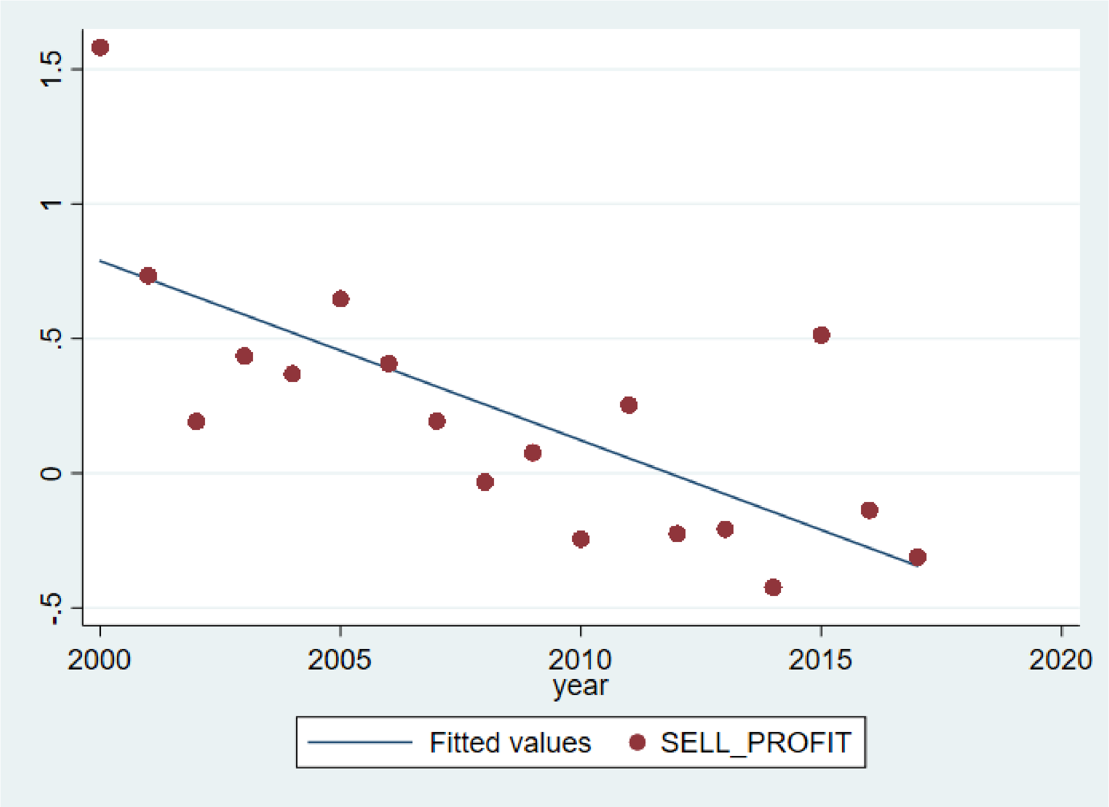
EFFECTIVE YEAR	STATES
2003	**CA**
2004	
2005	**WA, AR, DE, GA, NV, NY, NC, ND, TN**
2006	**WI, MN, MT, PA, PR, RI, OH, CO, CT, AZ, ID, IL, IN, NE, NJ, LA, ME**
2007	**WY, DC, MA, MI, NH, HI, OR, UT, KS**
2008	**IA, OK, MD, WV**
2009	**AK, MO, TX, SC**
2010	
2011	**MS, VA**
2012	**VT**
2013	
2014	**FL, KY**
2015	
2016	
2017	**NM**
2018	**AL, SD**

This table displays the year in which each state originally effectuates a data breach disclosure law.

Appendix B: Variable Definition

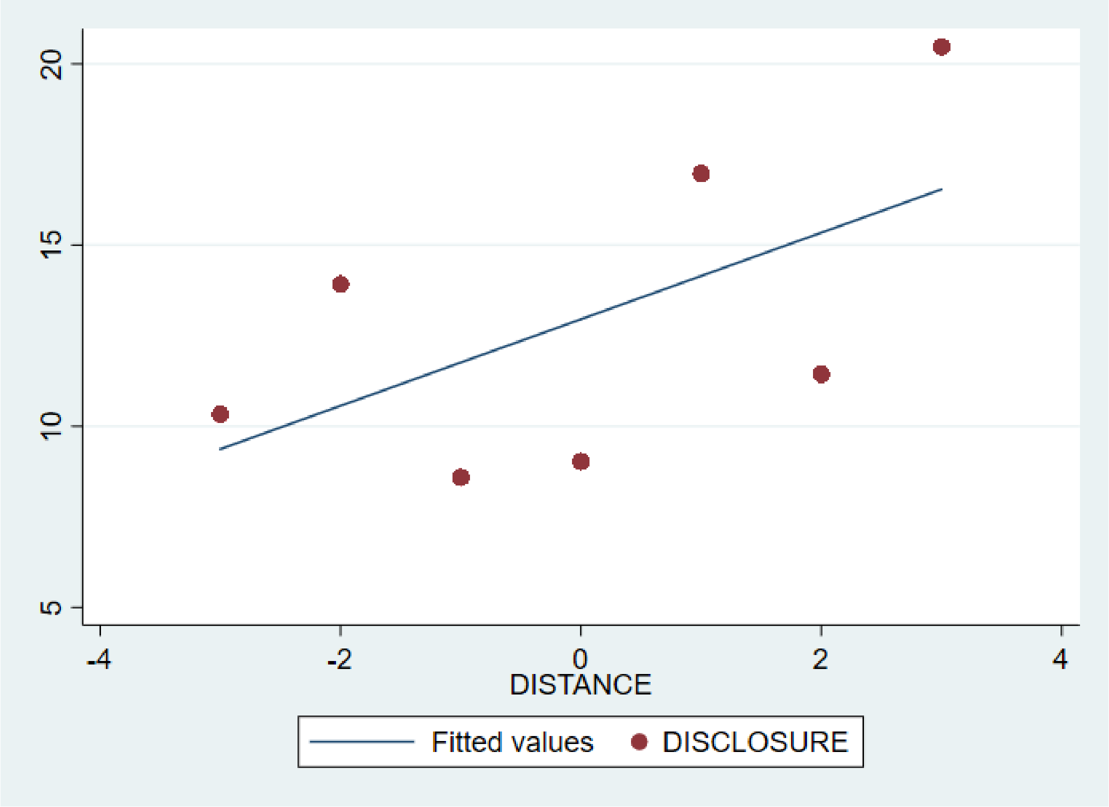
SELL_PROFIT	Market-adjusted (CRSP value-weighted index as market portfolio) abnormal return over 12 months following the trade multiplied by the value of trade (in millions of dollars). This value is multiplied by -1 so that the loss avoided on sales have the sign gains.
SELL_SPEED	Natural log of maximum number of days that the insider takes to make his sales in a given firm-year, multiplied by -1.
POST	Equals one if firm i's year t is after firm i's home state j has effectuated a data breach disclosure law, and zero otherwise.
SIZE	Natural log of firm i’s market value of equity (MKVALT) in the year over which trading is measured
BTM	The book value of equity divided by market capitalization
LOSS	An indicator variable equal to one if a firm reports negative net income in year t
RND	An indicator variable equal to one if a firm have positive research and development (R&D) expenses
DV	Cash dividends (DV) scaled by shareholders’ equity (SEQ)
RETVOL	The standard deviation of daily stock returns (CRSP) during the fiscal year
LAWINDEX	Sum value of the following five dimensions of data breach disclosure law intensity: (a) whether a law requires the firm to notify the Attorney General and allow Attorney General to bring law suits; (b) whether a law imposes an explicit deadline by which firms must disclose a data breach after it has been discovered; (c) whether a law specifies explicit penalties for violating the law; (d) whether a law specifies the disclosure items details. We assign each one of the above dimensions as value of 1, sum it up and scale it to range from 0 to 1.
LAWLENGTH	The quintile rank of the number of words in each state’s data breach disclosure law and scale it to range from 0 to1.
LAWCHANGE	The number of times that the data breach law in a given state has been amended. The frequency of law change varies from 0 to 4. We take this take and scale it to range from 0 to1
RISKFIRM	Equals to one, if the firm suffer higher data breach risk, and zero, otherwise. We identify a list of data breach incidents identified from http://www.privacyrights.org/data-breach. Then we rank the breach incidents by the number of records affected within the year when data breaches occur and identify the top 20% impactful data breach incidents. Abnormal returns of our sample firms on each data breach incident date are calculated and ranked by year. We consider firms with bottom 10% (most negative) abnormal returns plus the breach firms as the high data breach firms from investors’ perspective.

Figure 1 Insiders’ Selling Profits Over Calendar year



This graph reports the sell profit over the calendar year from 2000 to 2017. *SELL_PROFITS* is market-adjusted (CRSP value-weighted index as market portfolio) abnormal return over 12 months following the trade multiplied by the value of trade (in millions of dollars). This value is multiplied by -1 so that the loss avoided on sales have the sign gains.

Figure 2. Number of Data Breach Disclosures Around the Law Effective Year



This figure plots the number of data breach disclosures around [-3, 3] window when state data breach disclosure become effective. The DISTANCE is the time distance (year) to data breach disclosure law effective year. Y variable is the average number of data breach disclosures. The fitted line is based on a linear regression. Data breach incidents disclosures are identified Private Rights Clearinghouse's Chronology of Data Breaches (http://www.privacyrights.org/data-breach.

TABLE 1

Insider Trading Sample Selection Process

Description	Observations
Thomson Reuter Insider Trading Database Form4 open market sales aggregated at firm-year level (2000-2017)	31535
Less: Missing COMPUSTAT	(1425)
Less: Observations with historical state in 'NM' 'AL' 'SD'	(282)
Less: Missing control variables	(1028)
Total firm-year observations	28800
Total number of unique firms	5163

TABLE 2
Panel A: Descriptive Statistics for Insider Trading Sample

VARIABLES	N	Mean	Std. Dev.	Q1	Median	Q3
Test Variable						
POST	28,800	0.666	0.472	0.000	1.000	1.000
Dependent Variables						
SELL_PROFIT	28,800	0.211	5.016	-0.101	0.023	0.405
SELL_SPEED	28,800	-2.773	1.928	-4.446	-3.439	-0.560
Control Variables						
LOSS	28,800	0.295	0.456	0.000	0.000	1.000
RND	28,800	0.562	0.496	0.000	1.000	1.000
BTM	28,800	0.478	0.415	0.222	0.394	0.644
SIZE	28,800	6.664	1.854	5.413	6.600	7.834
DV	28,800	0.025	0.066	0.000	0.000	0.024
RETVOL	28,800	0.032	0.017	0.020	0.027	0.039

Panel B: Pearson Correlation Coefficients (n=28,800)

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
(1) SELL_PROFIT	1.000								
(2) SELL_SPEED	-0.005	1.000							
(3) POST	**-0.046**	**-0.103**	1.000						
(4) LOSS	**0.037**	**0.100**	**-0.042**	1.000					
(5) RND	**0.016**	**-0.074**	**0.076**	**0.173**	1.000				
(6) BTM	**0.014**	**0.168**	**-0.098**	**0.066**	**-0.158**	1.000			
(7) SIZE	-0.007	**-0.215**	**0.209**	**-0.312**	0.011	**-0.339**	1.000		
(8) DV	**-0.014**	0.007	**0.066**	**-0.140**	**-0.042**	**-0.152**	**0.217**	1.000	
(9) RETVOL	**0.090**	**0.145**	**-0.282**	**0.441**	**0.112**	**0.131**	**-0.502**	**-0.183**	1.000

Table 2 Panel A reports summary statistics of key variables for the full sample from 2000 to 2017. Panel B presents Pearson correlations, with the correlation coefficients with a significance level of 0.05 or better in bold. All continuous variables are winsorized to the 1st and 9th percentiles of their distributions. *SELL_PROFITS* market-adjusted (CRSP value-weighted index as market portfolio) abnormal return over 12 months following the trade multiplied by the value of trade (in millions of dollars). This value is multiplied by -1 so that the loss avoided on sales have the sign gains. *SELL_SPEED*, the natural log of maximum number of days that the insider takes to make his sales in a given firm-year, multiplied by -1. *POST* is an indicator variable equal to one if the firm is headquartered in a state which effectuates the data breach disclosure law, and zero otherwise. *LOSS* is an indicator variable equal to one if a firm reports negative net income in year t. *RND* is an indicator variable equal to one if a firm have positive research and development (R&D) expenses. *BTM* is the book value of equity divided by market capitalizations. *SIZE* is the natural log of firm *i*'s market value of equity in the year over which trading is measured. *DV* is cash dividend scaled by shareholder equity (SEQ). *RETVOL* is the standard deviation of daily stock returns over the fiscal year.

TABLE 3
Effect of Data Breach Disclosure Laws on Insiders' Selling Behaviors

	(1)	(2)
VARIABLES	SELL_PROFIT	SELL_SPEED
POST	0.278***	0.113***
	(0.091)	(0.038)
LOSS	0.209***	0.213***
	(0.077)	(0.035)
RND	-0.044	0.195
	(0.166)	(0.125)
BTM	0.782***	0.259***
	(0.113)	(0.055)
SIZE	0.902***	-0.483***
	(0.158)	(0.035)
DV	-0.002	0.379*
	(0.729)	(0.193)
RETVOL	33.297***	5.029***
	(6.853)	(1.865)
Constant	-7.492***	-0.098
	(1.333)	(0.310)
Observations	28,800	28,800
R-squared	0.204	0.364
firm FE	YES	YES
Year FE	YES	YES
Cluster at State	YES	YES

The table reports results from OLS regressions of insiders' trading behaviors on the indicator for the implementation of the data breach disclosure law. The sample spans the 2000-2017 period and include 28,800 firm-year observations. The dependent variables are insider *SELL_PROFIT* (model 1), *SELL_SPEED* (model 2). *SELL_PROFITS* market-adjusted (CRSP value-weighted index as market portfolio) abnormal return over 12 months following the trade multiplied by the value of trade (in millions of dollars). This value is multiplied by -1 so that the loss avoided on sales have the sign gains. *SELL_SPEED*, the natural log of maximum number of days that the insider takes to make his sales in a given firm-year, multiplied by -1. *POST* is an indicator variable equal to one if the frim is headquartered in a state which effectuates the data breach disclosure law, and zero otherwise. LOSS is an indicator variable equal to one if a firm reports negative net income in year t. *RND* is a dummy variable equal to one if a firm have positive research and development (R&D) expenses. *BTM* is the book value of equity divided by market capitalizations. *SIZE* is the natural log of firm *i*'s market value of equity in the year over which trading is measured. *DV* is cash dividend scaled by shareholder equity (SEQ). *RETVOL* is the standard deviation of daily stock returns over the fiscal year. Firm-fixed effects and year-fixed effects are included. All continuous variables are winsorized to the 1st and 99th percentiles. Standard errors are corrected for heteroskedasticity and clustering at state level (robust standards errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

TABLE 4

Timing of Changes in Insiders' Selling Behaviors Around Effectiveness of the Data Breach Disclosure Law

VARIABLES	(1) SELL_PROFIT	(2) SELL_SPEED
$EFFECTIVE^{-2}$	0.238	0.056
	(0.195)	(0.065)
$EFFECTIVE^{-1}$	-0.031	-0.021
	(0.268)	(0.074)
$EFFECTIVE^{0}$	0.368**	0.117*
	(0.175)	(0.067)
$EFFECTIVE^{+1}$	0.306*	0.131**
	(0.172)	(0.059)
$EFFECTIVE^{+2}$	0.345*	0.118*
	(0.196)	(0.064)
LOSS	0.210***	0.213***
	(0.078)	(0.035)
RND	-0.046	0.194
	(0.165)	(0.126)
BTM	0.781***	0.259***
	(0.113)	(0.055)
SIZE	0.900***	-0.484***
	(0.159)	(0.035)
DV	0.002	0.381*
	(0.730)	(0.194)
RETVOL	33.174***	5.001**
	(6.897)	(1.880)
Constant	-7.533***	-0.100
	(1.285)	(0.291)
Observations	28,800	28,800
R-squared	0.204	0.364
firm FE	YES	YES
Year FE	YES	YES
Cluster at State	YES	YES

This table reports results from OLS regression of *SELL_PROFIT* and *SELL_SPEED* on indicators for the timing of state' effectuations of the data breach disclosure law. The sample spans the 2000-2017 period and includes 28,800 firm-year observations. *$EFFECTIVE^{-2}$*, *$EFFECTIVE^{-1}$*, *$EFFECTIVE^{0}$*, *$EFFECTIVE^{1}$*, *$EFFECTIVE^{2}$*, which are equal to one if the firm is headquartered in a state that will implement the data breach disclosure law in two years, will implement the law in one year, implements the law, implemented the law in year ago, implemented the law two or more years ago, respectively, and zero otherwise. Control variables are defined in Tables 2 and 3 and include *LOSS*, *RND*, *BTM*, *SIZE*, *DV*, and *RETVOL*. Firm-fixed effects and year-fixed effects are included. All continuous variables are winsorized to the 1st and 99th percentiles. Standard errors are corrected for heteroskedasticity and clustering at state level (robust standards errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

TABLE 5

Disciplinary Effect of Stricter Data Breach Disclosure Law on Insiders' Selling Behaviors

	X=LAW		*X=LAWINDEX*		*X=LAWCHANGE*		*X=LAWLENGTH*	
VARIABLES	SELL_PROFIT	SELL_SPEED	SELL_PROFIT	SELL_SPEED	SELL_PROFIT	SELL_SPEED	SELL_PROFIT	SELL_SPEED
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Test Variables:								
POST	1.164***	0.355***	0.805***	0.241***	0.614**	0.212***	0.900***	0.303***
	(0.260)	(0.085)	(0.227)	(0.083)	(0.242)	(0.045)	(0.315)	(0.100)
X	1.323**	0.031	1.402***	-0.136	-0.107	0.112	0.680	0.010
	(0.607)	(0.268)	(0.385)	(0.176)	(0.548)	(0.135)	(0.544)	(0.245)
POST#X	-1.953***	-0.534***	-1.160***	-0.292**	-0.912*	-0.270***	-1.129***	-0.347***
	(0.412)	(0.150)	(0.382)	(0.139)	(0.483)	(0.086)	(0.415)	(0.127)
Control Variables:								
LOSS	0.206**	0.212***	0.204**	0.211***	0.209***	0.213***	0.208**	0.212***
	(0.077)	(0.035)	(0.076)	(0.035)	(0.076)	(0.035)	(0.078)	(0.036)
RND	-0.068	0.191	-0.076	0.192	-0.053	0.191	-0.039	0.198
	(0.163)	(0.125)	(0.169)	(0.125)	(0.162)	(0.125)	(0.164)	(0.125)
BTM	0.774***	0.257***	0.777***	0.258***	0.781***	0.259***	0.777***	0.258***
	(0.115)	(0.054)	(0.115)	(0.054)	(0.113)	(0.055)	(0.115)	(0.055)
SIZE	0.889***	-0.487***	0.899***	-0.484***	0.892***	-0.486***	0.896***	-0.485***
	(0.151)	(0.034)	(0.157)	(0.034)	(0.150)	(0.035)	(0.154)	(0.034)
DV	0.010	0.386*	-0.008	0.381*	0.013	0.382*	0.015	0.387**
	(0.733)	(0.192)	(0.731)	(0.192)	(0.729)	(0.194)	(0.731)	(0.192)
RETVOL	31.407***	4.527**	32.412***	4.827**	32.024***	4.643**	32.488***	4.787**
	(6.121)	(1.853)	(6.729)	(1.864)	(6.281)	(1.883)	(6.375)	(1.850)
Constant	-7.917***	-0.065	-8.048***	-0.033	-7.297***	-0.094	-7.797***	-0.080
	(1.343)	(0.295)	(1.375)	(0.300)	(1.329)	(0.304)	(1.465)	(0.299)

Observations	28,800	28,800	28,800	28,800	28,800	28,800	28,800	28,800
R-squared	0.204	0.364	0.204	0.364	0.204	0.364	0.204	0.364
firm FE	YES	YES	YES	YES	YES	YES	YES	YES
Year FE	YES	YES	YES	YES	YES	YES	YES	YES
Cluster at State	YES	YES	YES	YES	YES	YES	YES	YES

This table reports results from OLS regression of *SELL_PROFIT* and *SELL_SPEED* on indicators for the timing of state' effectuations of the data breach disclosure law. The sample spans the 2000-2017 period and includes 28,800 firm-year observations. *POST* is an indicator variable equal to one if the firm is headquartered in a state which effectuates the data breach disclosure law, and zero otherwise. LAW is the average of LAWINDEX, LAWCHANGE, LAWLENGTH. LAWINDEX is constructed based on five dimensions of data breach disclosure law intensity: (a) whether a law requires the firm to notify the Attorney General and allow Attorney General to bring law suits; (b) whether a law imposes an explicit deadline by which firms must disclose a data breach after it has been discovered; (c) whether a law specifies explicit penalties for violating the law; (d) whether a law specifies the disclosure items details. We assign each one of the above dimensions as value of 1 and calculate the total LAWINDEX by summing them together. LAWCHANGE measures the number of times that the data breach law in a given state has been amended. The frequency of law change varies from 0 to 4, thus we normalize the value by dividing 5. LAWLENGTH is the quintile rank of the number of words in each state's data breach disclosure law and we also normalize the value by dividing 5. We obtain qualitatively similar results by using the unnormalized raw value. Control variables are defined in Tables 2 and 3 and include *LOSS*, *RND*, *BTM*, *SIZE*, *DV*, and *RETVOL*. Firm-fixed effects and year-fixed effects are included. Standard errors are corrected for heteroskedasticity and clustering at state level (robust standards errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

TABLE 6

Effects of Data Breach Disclosure Laws on Insiders' Selling Behaviors in Firms with Greater Ex Ante Data Breach Risk

	(1)	(2)
VARIABLES	SELL_PROFIT	SELL_SPEED
POST	0.027	0.028
	(0.126)	(0.046)
POST#RISKFIRM	0.382*	0.162**
	(0.219)	(0.078)
LOSS	0.163**	0.200***
	(0.072)	(0.036)
BTM	0.815***	0.250***
	(0.118)	(0.051)
SIZE	0.874***	-0.500***
	(0.141)	(0.037)
DV	0.191	0.396*
	(0.784)	(0.201)
RETVOL	32.991***	5.211***
	(6.798)	(1.814)
Constant	-7.251***	0.109
	(1.172)	(0.304)
Observations	26,915	26,915
R-squared	0.167	0.360
firm FE	YES	YES
Year FE	YES	YES
Cluster at State	YES	YES

This table reports results from OLS regression of *SELL_PROFIT* and *SELL_SPEED* on indicators for the timing of state' effectuations of the data breach disclosure law. The sample spans the 2005-2017 period and includes 26,915 firm-year observations. *POST* is an indicator variable equal to one if the firm is headquartered in a state which effectuates the data breach disclosure law, and zero otherwise. RISKFIRM equals to one, if the firm suffer higher data breach risk, and zero, otherwise. We identify a list of data breach incidents identified from http://www.privacyrights.org/data-breach. Then we rank the breach incidents by the number of records affected within the year when data breaches occur and identify the top 20% impactful data breach incidents. Abnormal returns of our sample firms on each data breach incident date are calculated and ranked by year. We consider firms with bottom 10% (most negative) abnormal returns as the high data breach risk firms from investors' perspective. Control variables are defined in Tables 2 and 3 and include *LOSS*, *RND*, *BTM*, *SIZE*, *DV*, and *RETVOL*. Firm-fixed effects and year-fixed effects are included. Standard errors are corrected for heteroskedasticity and clustering at state level (robust standards errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

TABLE 7
Effect of Data Breach Disclosure Laws on Insiders' Purchasing Behaviors

	(1)	(2)
VARIABLES	BUY_PROFIT	BUY_SPEED
POST	0.016	0.069
	(0.031)	(0.065)
LOSS	-0.077**	-0.078
	(0.033)	(0.060)
RND	0.037	0.227*
	(0.054)	(0.128)
BTM	-0.097**	-0.020
	(0.038)	(0.072)
SIZE	-0.038	0.080**
	(0.026)	(0.039)
DV	-0.045	0.356
	(0.177)	(0.402)
RETVOL	1.135	4.785***
	(1.089)	(1.496)
Constant	0.250*	-2.351***
	(0.147)	(0.291)
Observations	18,511	18,511
R-squared	0.172	0.344
firm FE	YES	YES
Year FE	YES	YES
Cluster at State	YES	YES

This table reports results from OLS regression of *BUY_PROFIT* and *BUY_SPEED* on indicators for the timing of state' effectuations of the data breach disclosure law. The sample spans the 2000-2017 period and includes 18,511 firm-year observations. *POST* is an indicator variable equal to one if the firm is headquartered in a state which effectuates the data breach disclosure law, and zero otherwise. *BUY_PROFITS* market-adjusted (CRSP value-weighted index as market portfolio) abnormal return over 12 months following the trade multiplied by the value of trade (in millions of dollars). *BUY_SPEED*, the natural log of maximum number of days that the insider takes to make his sales in a given firm-year, multiplied by -1. Control variables are defined in Tables 2 and 3 and include *LOSS*, *RND*, *BTM*, *SIZE*, *DV*, and *RETVOL*. Firm-fixed effects and year-fixed effects are included. All continuous variables are winsorized to the 1st and 99th percentiles. Standard errors are corrected for heteroskedasticity and clustering at state level (robust standards errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

TABLE 8

Effect of Data Breach Disclosure Laws on Insiders' Selling Behaviors (Opportunistic VS Routine Sales)

	OPPORTUNISTIC SALES		*ROUTINE SALES*	
VARIABLES	SELL_PROFIT	SELL_SPEED	SELL_PROFIT	SELL_SPEED
	(1)	(2)	(3)	(4)
POST	0.288**	0.128***	0.141	-0.038
	(0.109)	(0.040)	(0.184)	(0.162)
LOSS	0.128	0.240***	0.059	-0.082
	(0.087)	(0.034)	(0.196)	(0.102)
RND	-0.009	0.153	-0.330	-0.135
	(0.202)	(0.124)	(0.283)	(0.455)
BTM	0.845***	0.298***	0.757**	0.363
	(0.084)	(0.048)	(0.293)	(0.267)
SIZE	0.789***	-0.452***	0.524***	-0.457***
	(0.135)	(0.034)	(0.125)	(0.100)
DV	-0.520	0.556**	0.123	0.036
	(1.018)	(0.212)	(1.279)	(0.600)
RETVOL	33.208***	3.872**	16.143	21.876***
	(5.487)	(1.538)	(10.216)	(5.785)
Constant	-6.723***	-0.168	-4.705***	-1.153
	(1.132)	(0.303)	(1.238)	(0.861)
Observations	28,508	28,508	5,407	5,407
R-squared	0.179	0.327	0.260	0.460
firm FE	YES	YES	YES	YES
Year FE	YES	YES	YES	YES
Cluster at State	YES	YES	YES	YES

This table reports results from OLS regression of SELL_PROFIT and SELL_SPEED on indicators for the timing of state' effectuations of the data breach disclosure law. The sample spans the 2000-2017 period. We follow Cohen, Malloy, and Pomorski (2012), Massa et al. (2015) and identify information driven insider trades based on a "routines" and "opportunistic" classifications. Specifically, routine insiders are those who have traded in the same month for at least the past three consecutive years, and opportunistic insiders are everyone else. This identification leaves us 28,508 firm-year observations for opportunistic sales and 5,407 firm-year observations for routine sales. Control variables are defined in Tables 2 and 3 and include *LOSS, RND, BTM, SIZE, DV*, and *RETVOL*. Firm-fixed effects and year-fixed effects are included. All continuous variables are winsorized to the 1st and 99th percentiles. Standard errors are corrected for heteroskedasticity and clustering at state level (robust standards errors are in parentheses). *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.