Division of Economics
A.J. Palumbo School of Business Administration and
McAnulty College of Liberal Arts
Duquesne University
Pittsburgh, Pennsylvania

Assessing the Impact of a Privacy Breach on a Firm's Market Value

Will Gangewere

Submitted to the Economics Faculty
In partial fulfillment of the requirements for the degree of
Bachelor of Science in Business Administration

December 2013

Faculty Advisor Signature Page

Pinar Geylani, Ph.D. Date
Associate Professor of Economics

Firms are being exposed to an increasing amount of security and privacy risks. In an attempt to counter these risks and protect consumers, data breach disclosure laws have been enacted. These laws require firms to notify impacted parties that sensitive information has been accessed or acquired without authorization in the event of a data breach. Previous research has shown that the effect of data breach disclosures on a firm's overall market value is negative. In this event study, I estimate the cumulative abnormal returns (CAR) that publicly traded entities suffer due to privacy breaches. Afterwards, a model is constructed using firm specific variables to discover the driving forces behind the magnitude of the CARs.

The results of the model suggest that firms that suffer multiple breaches tend to receive stronger negative feedback from investors. The model also suggests that firms with more growth opportunity are associated with a greater negative stock market reaction. Lastly, the effect of time on CARs is discussed.

JEL classifications: G14, G28, O38, D83

Key words: Data Breach, Event Study, Market Value Impact, Privacy, Information Security

Table of Contents

I. Introduction

Symantec Corporation and Ponemon Institute (2013) estimated an average cost of $188 per record stolen in the year 2012. During this time, organizations that suffered breaches incurred an average loss of $5.4 million. Whether a data breach is a malicious attack from an identity thief or a system glitch imposed by human error, unauthorized exposures to sensitive information can harm all parties involved. Risk Based Security (2012) reports that names, passwords, email addresses, and other pieces of personal information were exposed in 45% of reported data breaches in the year 2012. Information like this allows identity thieves to gain financial benefit at the expense of the breached victim.

While recent figures show that there may be a downward trend in the total cost of data breaches suffered by firms (see Ponemon, 2013), some sources project an increase in the number of data breach incidents. Juniper (2013) reports that mobile malware incidents grew by 614% between March 2012 and March 2013. This leads to the question of whether mobile devices in the workplace are worth the risk of a data breach and a possible financial loss. Ponemon Institute and Websense (2013) found that while 77% of questioned professionals find mobile devices necessary in the workplace, 76% of the respondents believe mobile devices pose "serious" security risks. The increasing amount of insecure computing practices could be what leads to the prevalence of data breaches. During the past decade, the United States has witnessed an increasing number of data breaches [see Figure 1 in Appendix A].

In response to the increasing number of data breaches, several states have enacted data breach disclosure laws in attempt to incentivize safe computing practices. A direct, positive impact of these laws is the increasing availability of data breach disclosure data, which in turn allows researchers to determine more accurately the impacts of such cases. Since 2003, 46 out of

50 states in United States of America have enacted data breach disclosure laws along with several federal laws.[1] Data breach disclosure laws require that firms inform impacted parties that personal information has been stolen in the event of a data breach. Romanosky et al. (2011) show that the implementation of these regulations do not reduce identity theft, and that corporations suffer a negative impact on market value after the event of disclosing information about a data breach. However, the negative market reaction is not the only consequence of a data breach. Data breach regulation also poses external costs on the firms. Because data breach statutes differ across all states, these entities face complex compliance challenges when a data breach falls within more than one jurisdiction.[2] This is often the case with publicly traded entities, because they usually conduct business in all 50 states.

Aside from state legislation, some federal legislation attempts to protect consumer information. Table A.1 in Appendix A lists several pieces of federal legislation that relate to information privacy.

Data breach regulation is enacted with the goals of enhancing both firm security management and protecting consumer privacy. While these breach notification laws seek to accomplish this through the means of informing impacted parties, some argue that the impact of incentivizing firms in the form data breach disclosure regulations is losing its effectiveness. Previous research has also shown that there is a possible "information fatigue" effect regarding the amount of mass media exposure a data breach disclosure event receives. This means that because more states now require data breach disclosures via legislation, media outlets have been exposed to an increasing number of these data breach instances. As a result, it is possible that society has lost interest in what now seems to be a routine scenario.

[1] The states with absence of data disclosure laws are Alabama, Kentucky, New Mexico, and South Dakota.
[2] Several states closely follow the very first data breach disclosure law: California's SB 1386, Cal. Civ. Code 1798.82 and 1798.29 enacted on July 1, 2003.

Previous literature focuses strongly on the financial costs of security breaches (see Cavusoglu et al. [2004], Ettredge and Richardson [2003], and Havov and D'Arcy [2005]). The focus of this paper follows Acquisti et al. (2006), who analyze the financial costs of privacy breaches. While some privacy breaches can be considered security breaches, it is important to understand the fundamental differences between the two. Security breaches focus on firms whose information technology systems have been breached. Suffering a security breach can force a company to evaluate its current security system and may interrupt data flows within the company, possibly leading to even more financial loss for the firm. Privacy breaches focus on sensitive information, usually a consumer's, which has been accessed without authorization. While not all privacy breaches will interrupt data flows within a firm, especially in the instance of a physically stolen device, instances of privacy breaches have negative repercussions, such as a decrease in corporate trust.

In this paper, event study methodology is utilized to examine the impact of a privacy breach disclosure on a firm's market value. McWilliams and Siegel (1997) define event study as a way to determine whether there is an 'abnormal' stock price effect associated with an event that was unanticipated by the market. After measuring the stock variances, a researcher can infer if the event had a significant impact on the stock price fluctuation. This paper adopts models previously used in academic research to calculate a firm's cumulative abnormal return (CAR), an aggregation of all the variations in stock price within a specified time frame. While no model is considered a flagship for estimating abnormal returns, the CAPM and Fama-French models serve as the standard for event study research.

After estimating the cumulative abnormal returns, a cross-sectional regression analysis is conducted to investigate the driving forces behind a firm's lost market value. Stemming from

previous literature, the model considers a firm's market capitalization and market to book ratio, which are often found by previous research to be associated with abnormal market returns. The model also considers two other factors that that rarely appear in data breach event studies: whether a firm has recently suffered a breach incident and the age of data breach regulation.

This study provides two extensions to data breach event study literature. First, it includes observations from a wide range of years (2005-2013). This lengthened dataset will help determine if these data breach regulation goals of protecting sensitive information are still being accomplished. Second, because of the additional years included in this study, the effect of time plays an important role. Examining the effect of these privacy breach disclosures throughout time may help guide the policy makers in creating better incentives for firms to securely handle sensitive consumer information.

II. Literature Review

Previous literature analyzes the impacts of data breaches in two primary sectors: healthcare and publicly traded entities. The healthcare sector is appealing to researchers because of the availability of data. Legislation such as HIPAA (1996) and HITECH (2009) require organizations to disclose data breach events to impacted individuals such as breach victims, health administrators, information technology affiliates, and the Department of Health and Human Services. HHS.gov provides detailed statistics for every health related data breach that impacted over 500 individuals [see Table A.1 in Appendix A for more detail.] Publicly traded entities are also appealing to researchers because of the methods established to measure the impact of breach. Most existing research that examines the impact of data breaches of publicly

traded entities use stock price as a proxy for a firm's market value. This makes it possible to measure a firm's lost market value, due to the daily fluctuations in stock prices.

Several studies in recent literature have measured the stock market impact of data breaches. Acquisti et al. (2006) compiled the first comprehensive analysis of market value variations as they are impacted by a firm's privacy failures. Using 79 breach events from 2000-2006, they conducted an event study while measuring cumulative abnormal returns using three different models: the Market Model, the Market Adjusted Model, and the Mean Adjusted Model. They found evidence suggesting that there is a negative association between a privacy breach announcement and a firm's market value.

While other researchers usually examine the day before the breach (in case of an information leak) and the day after the breach (in case of uncertainty or a closed stock market), Acquisti et al. (2006) and Hendricks and Singhal (1996) argue for the examination of a singular event day for two reasons. First, a shorter event period allows for a more accurate estimation of stock price effects, because it reduces the possibility of extraneous factors unrelated to the announcement of a data breach. Second, it boosts the power of the statistical tests. Unfortunately, investigating only the event day omits the possible effects that may occur the day before or the day after. While yielding similar results with each model, Acquisti et al. demonstrate how the use of different asset pricing models can introduce varied results in abnormal returns. In their study, the mean abnormal return on the event day varied from -0.35% to -0.52%, using a 92 day estimation period.

Gatzlaff and McCullough (2010) conducted a similar event study by examining the stock market's reaction to the cost of data breaches. In the study, they verified the finding of Acquisti et al. (2006), who asserted that there is an overall negative effect of a data breach on

shareholder wealth. They also found that there is a negative association between the reaction of the market and firms that are less "forthcoming" about details of the breach. In addition, they note that firm size, as proxied for by market capitalization, and being a subsidiary, alleviates the negative effect of a breach. Also, they conclude that corporations with higher market-to-book ratios experience significantly larger abnormal returns in the event of a breach. Lastly, they introduce a time element within the cross-sectional analysis of the cumulative abnormal returns by including the chronological month in which a specific breach event occurred with respect to the first event date observation.[3] They found that as the number of months since January 1, 2004 increases, cumulative abnormal returns decrease slightly. In an alternative regression model, they segmented the breach events into twelve different quartiles, assigning dummy variables to the observations that fell within the given quartiles. They found statistically significant evidence that events within quarters 3 and 6 were associated with a negative coefficient (at the 10% level) and that events within quarters 11 and 12 were associated with stronger negative coefficients (at the 5% level). They concluded that more recent instances of data breaches are more strongly associated with negative cumulative abnormal returns.

Schwartz and Janger (2007) note that a possible "boy-who-cried-wolf" effect can diminish the impact that data breach regulation has on protecting consumer privacy. To combat this issue, they develop other approaches that aim to be more efficient strategies to reduce privacy risks in the long run. In order to do this, they analyzed two separate data breach models: the Californian model and Interagency Guidance model. [4] After finding that the manner in which a particular notification occurs is important, they suggest a model that could come closer to

[3] For example, their first observation fell on January 1, 2004. An observation with an event date of February 6, 2005 would receive a (14) for being 14 months past the first event date.

[4] The Californian model has low threshold for notification. This closely follows the first state level data breach regulation adopted in 2003. The Interagency Guidance model has a high threshold for notification and low threshold for oversight.

reaching the goal of privacy protection. Their model would place more pressure on businesses to improve their information security practices, strengthen the awareness of privacy errors, and enable easier access to public information. They advise that a more detailed information set could help shape public policy into a better course for the future.

Davis et al. (2007) investigate the connection between cyber security risks and mitigation strategies. They found that the likelihood of a security breach incident being reported in well-known press increases with the total number of affected individuals. This slightly differs from the findings of Schwartz and Janger (2007). While Davis et al. argue that a larger breach will lead to more awareness, Schwartz and Janger argue that the maturity of regulation and timing of the data breach disclosure play a role in awareness.

Hovav et al. (2007) examine whether specific characteristics of data breaches influence abnormal stock returns. Using ANOVA to examine the differences amongst effects of each characteristic, they found that characteristics such as attacker type, result of the attack, objective of the attacker, and tools utilized during an intrusion have a statistically significant impact on abnormal stock returns. They also found that the type of access obtained has a marginal effect on a firm's market value.

While several researchers have examined the impact of data breach disclosures on a firm's market value, methodologies differ slightly across analyses. For example, Goel and Shawky (2009) find that security breaches result in about a 1% negative impact on the market value of a firm on the day of the breach announcement. To estimate this, they used the Fama and French (1993) three-factor model. This model incorporates observed market anomalies dealing with the size of the firm and the value premium.[5] They argue that this model is a more accurate

[5] A value premium refers to the greater risk-adjusted return of value stocks over growth stocks. Equity returns are measured as the high book-to-market ratio less the low book-to-market ratio.

estimation compared to a standard market model (CAPM). However, some other studies using abnormal return estimations follow the Brown and Warner (1985) model which is often used by financial economists, consisting of a standard Ordinary Least Squares regression that assumes that the regressors' error terms are independent, have zero mean, and are homoscedastic.

III. Hypothesis Development

As discussed above, several pieces of literature found that data breaches negatively impact a firm's market value. While the types of breaches in these studies differ, an overwhelming majority of researchers find a negative association between the disclosure of a breach incident and the market value for the impacted firm. Therefore, in order to proceed with analyzing the magnitude of the abnormal returns earned by firms, Hypothesis 1 must be developed as follows:

H1: A firm suffers a loss in market value whenever a privacy breach is announced.

Several studies have investigated the relationship between the size of a firm and the magnitude of abnormal returns. In financial economics, firm size is usually proxied as the natural logarithm of a firm's market capitalization. Gatzlaff and McCullough (2010), Acquisti et al. (2006), and Cavusoglu et al. (2004) found a significant negative relationship between the size of a firm and (negative) cumulative abnormal return, however, Kannan et al. (2007) found no statistical evidence of this correlation. Theoretically, a breach incident should be bigger news for smaller firms and smaller firms are assumed to be more volatile in the market. Therefore, it should be expected that the market acts more dramatically for small firm breach events. Hypothesis 2 is as follows:

H2: The magnitude of the negative CARs due to a privacy breach is greater for smaller firms than it is for larger firms, ceteris paribus.

To date, Gatzlaff and McCollough (2010) is the only data breach event study that accounts for repeated offenses for firms. Since data breach disclosure laws have been enacted, several firms have experienced multiple privacy breach events. It is possible that investors react more strongly to firms that fail to take appropriate measures to protect sensitive information after a breach incident occurs for the first time. Because of this, Hypothesis 3 states:

H3: The magnitude of the negative CARs due to a privacy breach is greater for events that are a repeated occurrence of a privacy breach.

Lastly, previous literature has studied the effect that time has on data breaches. Gatzlaff and McCollough (2010) and Bharadwaj et al. (2009) found that abnormal returns due to security and IT failures are positively correlated with the passage of time. This shows that as time passes, investors do not react so strongly to the information disclosed to them regarding a data breach. This is hypothesized in Schwartz and Janger (2007) with their "boy-who-cried-wolf" theory dealing with data breach disclosure laws. Because data breach disclosure laws are yet to be considered mature, investors are still in their "learning curve" in assessing the financial impacts that data breaches will have on the future, as noted by Mikhail et al. (1997). If investors are still in their "learning curve", there should still be a positive relationship between (negative) cumulative abnormal returns and the passage of time. Thus, Hypothesis 4 can be stated:

H4: The magnitude of the negative CARs due to a privacy breach is less for events that have occurred more recently.

IV. Methodology

Assumptions

The key assumption in event study methodology is derived from Fama (1970)'s efficient market hypothesis, which states that markets will instantaneously react to the information provided. This is empirically validated by Jung and Shiller (2005), who note that individual stocks react more efficiently than the stock market as a whole. Another assumption in event study is that the events that occur are unanticipated by the market. This means that the events being investigated were not foreseen by any investors. Lastly, it is assumed that no other events occur around the time of the event of interest.

Event Study Methodology

McWilliams and Siegel (1997) define event study methodology as a way to determine whether there is an 'abnormal' stock price fluctuation associated with an unforeseen event. MacKinlay (1997) outlines event study methodology involving 6 steps: (1) identify the event of interest; (2) define the event window; (3) select sample of firms to be included in the analysis; (4) predict 'normal' returns within event window, in absence of the event; (5) estimate 'abnormal' returns within the event window; (6) calculate cumulative abnormal returns (CARs), then test for statistical significance. Previous literature often cites MacKinlay as the most efficient approach for event study methodology.

(1) Identify the Event of Interest

As stated above, privacy breach announcements are the events of interest. Parties, inside or outside a firm, disclose information of a privacy breach. According to the efficient market hypothesis, markets will quickly react to this information. While there is variability between

each observation's data breach event and its public disclosure date, having an accurate disclosure date is key in determining the timely response of the market.

(2) Define the Event Window

The "event window" indicates the number of trading days before and after the event of interest date. In this study, [-X, +Y] denotes the event window, where X is the total amount of days prior to the data breach disclosure and Y is the total amount of days following the data breach disclosure. Typically, "*day-0*" is denoted as the day of the event of interest. There is no scientific method to determine the exact length of the event window; however, the nature of the event of interest should help dictate the intuition for selecting an appropriate window length.

It is preferred that the event window is as small as possible while still being able to confidently predict 'normal' returns. A window length greater than such is exposed to risk of including other major events that could contaminate stock price movement estimations. The length of the event window must be uniform across all observations. It is important that the event window and estimation period used to predict 'normal' returns do not overlap, in order to prevent biased predicted stock returns.

Following the footsteps of closely related previous literature, several different event windows are examined in this paper.

(3) Sample of Firms

The selected sample of firms must fulfill criteria that will allow a researcher to examine the variation in stock returns. In this paper, publicly traded entities without any notable events within a week of the data breach disclosure are examined.

(4) Predict 'Normal' Returns

There are two generally accepted models used to calculate 'normal' returns, the simple market (CAPM) model and the Fama-French model. Womack and Zhang (2003) state two key assumptions in the CAPM model. First, because investors only care about expected return, they will act as rational agents in attempt to always maximize expected return. Second, all investors have analogous beliefs about risk versus reward payoffs in the market. The CAPM model assumes only one risk factor, market risk, which is the only influence on expected return.

The Fama-French model adjusts for two other types of risk besides market risk: the size factor and the value factor. The size factor is an index number computed as the average return of the smallest 30% of stocks minus the average return of the largest 30% of stocks within a given time period. Theoretically, small market capitalization firms are riskier investments compared to large market capitalization firms, thus in the long run, yield higher returns. This is notion was confirmed by Banz (1981), who found that smaller firms, on average, have higher risk-adjusted returns than large firms. The value factor is an index number computed as the average return for the 50% of stocks with the highest book-to-market ratio minus the average return of the 50% stocks with the lowest book-to-market ratio. Value stocks exist for corporations that have high book value, but struggle to interest investors. Growth stocks exist when investors perceive a corporation as more valuable compared to what a corporation's true book value implies. Thus, with a corporation being a value company, investors can buy shares cheaper than they would have otherwise, yielding greater returns in the long run. Fama and French argue that controlling for these two extra risk factors generate more accurate 'normal' return estimates. The Fama-French model is as follows:

$$r_{it} = \alpha_i + r_{ft} + \beta_{im}(R_{mt} - r_{ft}) + \beta_{is}SMB_t + \beta_{ih}HML_t + \varepsilon_{it} \quad (1)$$

In this model, r_{it} represents the 'normal' return of stock for firm *i* at time *t*. Firms are also assumed to get the risk free rate, r_{ft}, as measured by the one month Treasury bill rate. The return on the market portfolio less the risk free rate is measured by $R_{mt} - r_{ft}$. The small firm premium and the value firm premium are represented as SMB_t and HML_t respectively. The disturbance term is represented by ε_{it}. In financial research, β_{im} (beta), is a parameter that is often examined to measure the amount of systematic risk. In this study, it is a raw beta estimated through simple OLS regression. By subtracting the r_{ft} term from both sides of the equation, the equation takes the form of a regular regression model as shown below:

$$[r_{it} - r_{ft}] = \alpha_i + \beta_{im}(R_{mt} - r_{ft}) + \beta_{is}SMB_t + \beta_{ih}HML_t + \varepsilon_{it} \quad (2)$$

(5) Estimate 'Abnormal' Returns

After predicting 'normal' return, subtracting it from the actual return, R_{it}, yields the abnormal return, AR_{it}. The abnormal return is essentially the difference between what returns actually were less what they should have been in the absence of the event, as shown below:

$$AR_{it} = R_{it} - [\hat{\alpha}_i + \hat{\beta}_{im}(R_{mt} - r_{ft}) + \hat{\beta}_{is}SMB_t + \hat{\beta}_{ih}HML_t] \quad (3)$$

(6) Calculate CARs

Cumulative abnormal returns, CAR_i, can be found by aggregating the abnormal returns throughout time for each firm. The CARs show the accumulated amount of total abnormal returns within a given event window. They can be interpreted as the total difference between what stock returns were and what stock returns should have been in the absence of a data breach. The CARs from period t_1 though t_2 is calculated by the following:

$$CAR_{i[t_1,t_2]} = \sum_{t=t_1}^{t=t_2} AR_{it} \quad (4)$$

V. Data Summary

Data Collection and Description

The sample of privacy breach observations, which includes 335 events from February 2005 through October 2013, was gathered from Privacy Rights Clearinghouse, a non-profit organization that "educates and empowers" individuals to protect their privacy.[6] This organization acquires observations from sources such as Open Security Foundation, DataBreaches.net, PHI Privacy, and NAID. By closely monitoring several media outlets, government websites, and blog posts, these sources are combined to provide the most comprehensive dataset for privacy breach events.

The raw dataset provided by Privacy Rights Clearinghouse contained 1,499 data breach events in sectors including business, educational institutions, government/military, healthcare/medical providers, and non-profit organizations. Filtering for appropriate observations consisted of three steps. First, to filter for potential publicly traded entities, all sectors except Business were omitted. Second, all observations that are not publicly traded entities were omitted, otherwise it would be nearly impossible to measure accurately each company's respective market value.[7] Third, observations where another major event occurred within a week of the privacy breach date were omitted. This is necessary because including observations in which a major event occurs could bias results.

Once all observations satisfied the criteria above, all ticker symbols were entered into the Bloomberg Terminal to find stock returns from the day of the data breach, 255 trading days before, and 10 days after.

[6] First available breach data occurred on Feb. 25, 2005. https://www.privacyrights.org/data-breach.
[7] Following most previous research, the companies that are publicly traded in NYSE or NASDAQ are selected.

The Commercial Law League of America provides a spreadsheet containing each state's specific data breach disclosure regulation. This spreadsheet separates state level legislation into different components, but for the scope of this research, only the effective date of regulation was used.

The last data source used is the Kenneth French Data Library.[8] This electronic library contains Fama-French factors used for the 'normal' stock return estimations while using different factors to control for market behavior. These factors include SMB (Small minus Big), HML (High minus Low), and Rm-Rf (excess market return).

As stated above, data breach incidents have been increasing over the past few years. However, because this study focuses solely on publicly traded entities, the upward trend of data breach incidents may not be apparent. Table 1 shows the distribution of data breaches in publicly traded entities (NYSE and NASDAQ) per year within the sample:

Table 1. Privacy Breach Incidents per Year

Year	Number of Incidents
2005	18
2006	49
2007	50
2008	25
2009	11
2010	53
2011	44
2012	49
2013 (thru July)	39
Total	335

While the type of data breach is accounted for in almost all data breach event studies, the type of breach is usually found to be an insignificant factor most of the time. Over the span of the dataset, stolen portable devices have been the most popular type of data breach. While this

[8] http://mba.tuck.dartmouth.edu/pages/faculty/ken.french/data_library.html

may seem like a surprise to some, Miller and Tucker (2011) found that due to the use of encryption software, holders of sensitive information tend to treat their data storage devices more loosely than they otherwise would, leading to an increasing number of stolen devices. Table 2 shows the distribution of data breaches in publicly traded companies by type of data breach within the sample:

Table 2. Privacy Breach Incidents per Type of Breach

Type	Number of Incidences	Definition
DISC	56	Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.
HACK	61	Electronic entry by an outside party, malware and spyware.
CARD	14	Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
INSD	62	Someone with legitimate access intentionally breaches information - such as an employee or contractor.
PHYS	13	Lost, discarded or stolen non-electronic records, such as paper documents.
PORT	107	Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.
STAT	11	Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.
UNKN	111	Does not fall under any of the above categories.

VI. Cumulative Abnormal Returns

Because there is no scientific way to determine the length of the estimation period and the event window, this study relies on previous research for guidance. Similar to Acquisti et al. (2006), this study uses [-100,-8] as the estimation window. This estimation window fits the scope of this study because it is short-term oriented and a longer estimation period would not marginally provide a more accurate estimation [see Table B.1 in Appendix B.] This estimation window is relatively shorter than those used in other studies: however, the risk of contamination inside this event window is much lower compared to a larger estimation window.

Most event studies focus at least on *day-0* (the day of the breach) to measure the impact of a data breach on abnormal returns. However, as stated previously, leakages and lags may spread out the effect across multiple days. Thus, extending the event window will help capture these effects (if leakages and lags do occur). Table 3 shows the mean cumulative abnormal return after a data breach announcement within each specified event window. Comparison outputs for CARs can be found in Tables B.1, B.1, and B.3 in Appendix B.

Table 3. Cumulative Abnormal Returns by Selected Event Windows

Cumulative Abnormal Returns				
Event Window	[0]	[0,+1]	[-1,+1]	[-1,+2]
CAR	-0.20811% (0.007)	-0.4280% (0.000)	-0.4958% (0.000)	-0.3745% (0.007)

All of the mean (negative) cumulative abnormal returns are statistically significant at the 1% level for all specified event windows. The largest mean CAR is captured using the [-1,+1] event window. This finding is consistent with Kannan et al. (2007), where they found a statistically significant decrease in cumulative abnormal returns when accounting for a leakage and information lag. Therefore, there is significant evidence suggesting that a firm suffers a loss in market value whenever a privacy breach is announced. On average, a firm loses about -0.4% to -0.5% in market value due to a privacy breach incident. Thus, the null hypothesis of cumulative abnormal returns not being significantly different from zero can be rejected at the 1% level in favor of the alternative hypothesis, *H1*.

VII. Model

Following the event study methodology of MacKinlay (1997), the CARs for each firm are used as the dependent variable within a cross-sectional regression analysis. The goal of this

regression analysis is to test Hypotheses 2 to 4 stated above. Table 4 shows the name of each variable used, the definition of the variable, and the source of the data.

Table 4. Variable Description

Variable Name	Definition	Source
LN_MARKET_CAP	Proxy for size of a firm. Market Capitalization is equal to (the natural logarithm of) the number of shares outstanding times the share price.	Bloomberg Terminal
MARKET_TO_BOOK	A firm's market capitalization divided by its book value.	Bloomberg Terminal
MATURITY	Amount of months since data breach disclosure laws started in America (January 1, 2003).	Commercial Law League of America
REPEAT	Breach incident is a repeated occurrence of a Firm within the sample (1=yes, 0=otherwise)	Privacy Rights Clearinghouse

Table 5 shows the Summary Statistics of the total sample.

Table 5. Summary Statistics

Variable Name	N	Mean	Std. Dev	Min	Max
LN_MARKET_CAP	334	9.819614	1.642596	5.150954	13.35778
MARKET_TO_BOOK	334	45340.51	2000364.8	-5407.235	2547987
MATURITY	335	74.17015	30.13131	19	121
REPEAT	335	0.4238806	0.4949111	0	1

The significance of the negative CARs in the [-1,+1] window clarifies the existence of leakages and lags in the market reaction to privacy breaches. Based on the general idea that event windows should be small to keep estimations more accurate, but large enough so that the window fully captures market reaction, this study carries out the [-1,+1] event window. To investigate Hypotheses 2 to 4, a cross-sectional regression is used to determine the effects of firm size, repeated incidents, and the time effect. The following model is estimated:

$$CAR_i = \alpha + \beta_1 LN\_MARKET\_CAP_i + \beta_2 REPEAT_i + \beta_3 MATURITY_i + \beta_4 MARKET\_TO\_BOOK_i + \varepsilon_i \quad (5)$$

In this model, *CAR* is the cumulative abnormal return of firm *i* inside the event window. *LN_MARKET_CAP*, a proxy for size, is the natural logarithm of a firm *i*'s market capitalization (number of shares outstanding times the share price). *REPEAT* is a dummy variable indicating whether a privacy breach has occurred for firm *i* in the past (relative to the dataset). *MATURITY* is the number of months since data breach regulation has become enacted in California on July 1, 2003. *MARKET_TO_BOOK* is a control for firm *i*'s market to book ratio, which accounts for how investors value firm *i*'s stock in comparison to firm *i*'s book value.

VIII. Results

Based on previous research discussed in the previous sections, hypotheses 2 to 4 are tested using the cross-sectional regression analysis demonstrated in Equation (5). Using the [-1,+1] event window to account for leakages and lags, the results show similarities and differences compared to previous research. It is difficult to fully compare and contrast this study with previous research that deals with security breaches. Therefore, comparisons of privacy breaches and security breaches should be handled cautiously. Aside from Acquisti et al. (2006), the only other privacy breach event study conducted was Liginlal et al. (2009), who focus on privacy breaches due to human error. Between those two, Acquisti et al. is the only study that examines the determinants of CARs due to privacy breaches.

Some event studies in the past had to correct for heteroskedasticity (variance of the error term is non-constant). White's test for heteroskedasticity was applied and the null hypothesis of constant variance was rejected, so the regression model was corrected by estimating the standard

errors using the Huber-White sandwich estimators.[9] Table 6 shows the results of the regression output:

Table 6. Regression Output (CAR)

Variable Name	Coefficient	Robust Standard Error
Constant	0.0001988	0.0092674
LN_MARKET_CAP	0.0001988	0.0008963
REPEAT	0.0043945*	0.0023982
MATURITY	-0.0000257	0.0000365
MARKET_TO_BOOK	-1.63e-08**	8.23e-09
Observations	333	
R^2	0.0302	

Dependent variable: Cumulative Abnormal Return. Using 333 observations from the years 2005 – 2013. Corrected for heteroskedasticity with robust standard errors. Significance levels: * p<0.10, ** p<0.05, ***p<0.01.

The results shown in Table 6 are somewhat consistent with previous research. The *REPEAT* coefficient is positive and statistically significant at the 10% level. This confirms the finding of Gatzlaff and McCollough (2010), where they found a significant positive correlation between (negative) CARs and repeated offenses of a privacy breach. This finding suggests that investors react more strongly to firms that do not take the appropriate actions after the first privacy breach occurs. Thus, the null hypothesis of the magnitude of CARs not being significantly greater for events that are repeated occurrences is rejected in favor of the alternative hypothesis, *H3*.

The *MARKET_TO_BOOK* coefficient is also statistically significant at the 5% level. This finding suggests that firms with more growth opportunity are associated with a greater negative stock market reaction. This confirms the findings of Gatzlaff and McCollough (2010). Theoretically, this makes sense because a breach should inhibit the existing growth of a firm. For example, if an existing growth company experiences a privacy breach, it would be forced to transfer resources from generating more growth opportunities towards projects that directly generate revenue for the firm.

[9] Test results confirm presence of heteroskedasticity. Results: Chi2(1) = 6.29. Prob > chi2 = 0.0122.

The *MATURITY* coefficient is insignificant at all significance levels. While a time effect is believed to impact CARs, these results suggest that the age of a privacy breach, in respect to the first state data breach regulation, does not play a crucial role. Thus, the null hypothesis of the magnitude of CARs not being significantly less for events that have occurred more recently cannot be rejected in favor of alternative hypothesis, *H4*. This differs from the findings of Bharadwaj et al. (2009) and Gatzlaff and McCollough (2010), who found a significant relationship between (negative) CARs and time. It is important to consider that the time effect, *MATURITY*, is measured differently in this study compared to other literature. In this study, *MATURITY* is the number of months since the first enacted state data breach law. In Bharadwaj et al. and Gatzlaff and McCollough, the time effect is measured relative to their sample. Table B.4 in Appendix B shows the same regression model, only using the same *time effect* measurement as Bharadwaj et al. and Gatzlaff and McCollough.

The *LN_MARKET_CAP* coefficient is insignificant at all significance levels. This finding suggests that the size of the firm is not associated with (negative) abnormal returns. Thus, the null hypothesis of the magnitude of CARs not being significantly greater for smaller firms than it is for larger firms cannot be rejected in favor of alternative hypothesis, *H2*. This finding is inconsistent with Cavusoglu et al. (2004), Acquisti et al. (2006), and Gatzlaff and McCollough (2010), who found a significant negative relationship between firm size and cumulative abnormal returns. However, this finding supports the finding of Kannan et al. (2007), who found no statistical evidence of this relationship.

The size and time span of the sample used should be considered. Table 7 shows similar studies' size and time span used in each piece of research:

Table 7. Similar Studies

Researchers	Topic	Sample Size	Sample Time Span
Cavusoglu et al. (2004)	Security Breach	66	Jan. 1996 – Dec. 2001
Acquisti et al. (2006)	Privacy Breach	79	2000 – 2005
Kannan et al. (2007)	Security Breach	72	Jan. 1997 – Dec. 2003
Gatzlaff and McCollough (2008)	Data Breach	77	Jan. 2004 – Dec. 2006
Bharadwaj and Keil (2009)	Security Breach	213	1990 - 2000
Liginlal et al. (2009)	Privacy Breach	181	Jan. 2005 – June 2008
****Gangewere (2013)***	***Privacy Breach***	***335***	***Feb. 2005 – July 2013***

As shown in Table 7, this study consists of 154 more observations then the second largest sample dataset. Also, this study is the only one that consists of breach events that occurred from 2009 through 2013. These years are important to include because they capture the market's response towards data breaches over the last few years. Based on the research of Schwartz and Janger (2007) and Acquisti et al. (2006), the market can suffer "information fatigue." Information fatigue means that the market experiences marginally decreasing awareness due to overexposure of information.[10] As stated earlier, overexposing the market to data breach incidents can lead to the diminishing interest of data breaches to society.

Another time factor to be considered is the investor "learning curve." Mikhail et al. (1997) note that new events for the market, like data breach disclosures, give investors uncertainty about future financial implications. It is possible that the insignificant factors seen in Table 6 can be attributed to either "information fatigue" or the investor "learning curve."

As a robustness check, the same regression is used, only this time using observations from 2005 – 2008. This sample set closely resembles the data used from previous literature. If similar results to previous literature are obtained using this sample set, two conjectures can be made: the dataset used in this study is of high quality because it yields similar results using a

[10] Schwartz and Janger (2006) call this the "boy-who-cried-wolf" effect. Acquisti et al. (2006) call this "privacy fatigue".

similar sample set, and the possibility that the market is now experiencing "information fatigue" or the investor "learning curve" has been met. Table 8 shows the results of the regression using the limited sample:

Table 8. Regression Output (CAR)

Variable Name	Coefficient	Robust Standard Error
Constant	-0.0353588*	0.0185656
LN_MARKET_CAP	0.0029684*	0.0016756
REPEAT	0.0061034*	0.0032256
MATURITY	0.0000173	0.0001702
MARKET_TO_BOOK	-4.77e-08	5.93e-08
Observations R^2	141 0.0747	

Dependent variable: Cumulative Abnormal Return. Using 141 observations from the years 2005 – 2008. Corrected for heteroskedasticity with robust standard errors. Significance levels: * p<0.10, ** p<0.05, ***p<0.01.

Although *MATURITY* remains insignificant, the size of the firm (*LN_MARKET_CAP*) becomes significant. This result can infer that investors used to react more strongly towards smaller firms, but now they no longer have a lower threshold for smaller firms. For example, if a firm suffered a breached in the year 2005, because data breach disclosure laws were relatively new at the time, investors were uncertain about the implications of the breach. In response, investors acted more negatively towards smaller firms than they did for large firms. However, now that time has passed and investors seem have a better idea of what to expect after a firm suffers a breach, there is no need to have a lower threshold for smaller firms.

Appendix B consists of several robustness checks to further investigate the driving forces behind the magnitude of the CARs. Table B.5 in Appendix B shows the regression output using the model from Equation 5, with the addition of dummy variables, controlling for the type of the breach incident. Although the majority of event study research finds "type of breach" to be insignificant, it is good practice to recognize the distinction between different breaches types.

The results suggest that there are not any specific types of breaches that have a significant impact on cumulative abnormal returns.

Tables B.6 and B.7 in Appendix B show the regression outputs using the model from Equation 5, with the addition of variables controlling for the number of records breached. In Table B.6 in Appendix B, *RECORDS* is the total number of records breached due to the privacy breach incident. In Table B.7 in Appendix B, following Acquisti et al. (2006), a dummy variable (*Dummy_RECORDS*) is assigned if the privacy breach exceeded 100,000 records. The results in Tables B.6 and B.7 show that both of these methods used to control for the number of breached victims do not yield significant results. This is not a concern because the majority of previous research finds that the number of records breached does not have a significant impact on cumulative abnormal returns. It should be noted that a large number of observations dropped from these regression in Tables B.6 due to the lack of observations within the dataset.

IX. Limitations and Considerations

Several limitations in this study should be considered. First, event study methodology assumes that markets are efficient and that investors are rational. Like all other event studies, the idea that markets can differ from absolute efficiency is an issue to consider. Second, the method used to capture fully the time effect within data breach event study is not solidified yet by previous research. While several sources suggest that market reaction changes throughout time, there is no uniform way across literature to measure this effect. Third, the quality of the dataset in this study should be considered. While there was an effort to eliminate all other major events around the time of the breach, other unknown factors, either inside or outside the market, could have impacted the estimations in this study.

Also, more information about each privacy breach would be useful. For this reason, several researchers have proposed federal data breach legislation that would provide available data for major data breaches; much like HHS.gov does for healthcare breaches. Fourth, this study solely focuses on publicly traded entities in the United States. This limitation generalizes the results, disregarding how markets in other countries function. If a study wanted to analyze the effects of privacy breaches on organizations that are not publicly traded, the value of the organization would not be able to be measured via market value (stock price). Last, a deeper classification of breach specific characteristics would more accurately differentiate each breach incident. Researchers could use the specific classifications to determine the unique impacts of each characteristic.

X. Future Research Suggestions

As privacy breaches continue to occur and regulation continues to be revised, the analysis of privacy breaches and their impacts on a firm's market value will need to be extended. Future research on the impact of individual state legislation would be useful to help guide policy makers. Also, a cost-benefit analysis of securing sensitive information versus the incurred costs (direct and indirect) of a privacy breach would help understand a firm's perspective on managerial IT decision making. On the consumer side, a cost-benefit analysis of consumer decisions can help understand the dilemma between privacy and consuming/costs. Lastly, following this study, further investigating the issues of "information fatigue" and the investor "learning curve" could help explain if data breach regulation is in fact withering the consequences of privacy breaches. By further analyzing the incentives on both the consumer-end

and the firm-end, policy makers can formulate better laws that will enhance both firm security management and the protection of consumer privacy.

XI. Conclusion

The purpose of this research was to assess the impact of a privacy breach on a firm's market value. Using event study methodology, the cumulative abnormal returns that publicly traded entities suffer due to a privacy breach were estimated. To do this, a similar privacy breach event study, Acquisti et al. (2006), was followed using the estimation period [-100,-8] to help predict abnormal returns. There was statistically significant evidence that firms suffer negative cumulative abnormal returns (on average -0.4% to -0.5% of its market value) on the day of a privacy breach announcement, as well as the days directly before and after the announcement. This confirms the existence of an information leakage and a lag due to either uncertainty or the stock market being closed at the time of the announcement. Therefore, the event window [-1,+1] was used to capture the cumulative abnormal returns.

Using the each firm's CAR as the dependent variable, three hypotheses derived from previous literature were tested. The results suggest that firms that suffer multiple breaches tend to receive stronger negative feedback from investors. The model also suggests that firms with more growth opportunity are associated with a greater negative stock market reaction. Lastly, the effect of time on CARs is discussed. Because the dataset in this study includes the addition of recent years, different results were yielded from this study compared to other research. When only including observations from older time periods, matching that of other previous studies, similar results to previous literature were found. From this, two conjectures were made: the possibility that the market is now experiencing "information fatigue" and the possibility of the

investor “learning curve” being met. Finally, future research suggestions were made to help guide the investigation of the rarely studied time effect of data breaches.

The findings in this study are of interest both to firms and to investors. All parties involved in a data breach should be aware of the negative reaction by investors. As this study shows, investors act more negatively towards firms that fail to fix their information security flaws. Therefore, if a firm does suffer a privacy breach, it should take the appropriate actions to make sure that the same mistake does not result in another breach. What should also be considered by firms is how investors respond to privacy breach announcements throughout time. This could help IT managers make more knowledgeable long-term decisions regarding information security.

This study is also of interest to state and federal lawmakers. While state and federal legislation continues to be revised and proposed, analyzing the effects of privacy breaches could better direct how incentives can be implemented. With the increasing number of data breach incidents and the growing threats of security risks, it is important that lawmakers put firms in an appropriate position to be able to prevent, monitor, and respond to data breaches.

XII. References

Acquisti, Alessandro, Allan Friedman, and Rahul Telang. 2006. "Is There a Cost to Privacy Breaches? An Event Study." *WEIS*.

Banz, Rolf W. 1981. "The Relationship Between Return and Market Value of Common Stocks." *Journal of Financial Economics* 9.1: 3-18.

Bharadwaj, Anandhi, Mark Keil, and Magnus Mahring. 2009. "Effects of Information Technology Failures on the Market Value of Firms." *The Journal of Strategic Information Systems* 18.2: 66:79.

Bloomberg L.P. 2013. "Stock Prices, Market Capitalization, Market to Book Ratio, and IPO date data from 2005-2013." Bloomberg database. Duquesne University, Pittsburgh, PA. November 26, 2013.

Brown, Stephen J., and Jerold B. Warner. 1985. "Using Daily Stock Returns: The Case of Event Studies." *Journal of Financial Economics* 14.1: 3-31.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. 2004. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breach Firms and Internet Security Developers." *International Journal of Electronic Commerce* 9.1: 70-104.

Commercial Law League of America. 2013. "Data Breach Notification Laws By State." File last modified December 2, 2011. Microsoft Excel file.

Davis, Ginger, Alfredo Garcia, and Weide Zhang. 2009. "Empirical Analysis of the Effects of Cyber Security Incidents." *Risk Analysis* 29.9: 1304-1316.

Ettredge, Michael L., and Vernon J. Richardson. 2003. "Information Transfer Among Internet Firms: The Case of Hacker Attacks." *Journal of Information Systems* 17.2: 71-82.

Fama, Eugene F., and Kenneth R. French. 1993. "Common Risk Factors in the Returns on Stocks and Bonds." *Journal of Financial Economics* 33.1: 3-56.

Fama, Eugene F. 1970. "Efficient Capital Markets: A Review of Theory and Empirical Work." *The Journal of Finance* 25.2: 383-417.

Gatzlaff, Kevin M., and Kathleen A. McCullough. 2010. "The Effect of Data Breaches on Shareholder Wealth." *Risk Management and Insurance Review* 13.1: 61-83.

Goel, Sanjay, and Hany A. Shawky. 2009. "Estimating the Market Impact of Security Breach Announcements on Firm Values." *Information & Management* 46.7: 404-410.

Havov, Anat, and John D'Arcy. 2005. "Capital Market Reaction to Defective IT Products: The Case of Computer Viruses." *Computers & Security* 24.5: 409-424.

Hendricks, K.B. and Singhal, V.R. 1996. "Quality Awards and the Market Value of the Firm: An Empirical Investigation." *Management Science* 42.3

Health Insurance Portability and Accountability Act of 1996

Health Information Technology for Economic and Clinical Health Act of 2009

Hovav, Anat, Francis K. Andoh-Baidoo, and Gurpreet Dhillion. 2007. "Classification of Security Breaches and Their Impact on the Market Value of Firms." *Proceedings of the Sixth Annual Security Conference, Las Vegas*.

Jung, Jeeman, and Robert J. Shiller. "Samuelson's Dictum and the Stock Market." 2007. *Economic Inquiry* 43.2: 221-228.

Juniper Networks Third Annual Mobile Threats Report. 2013. Juniper Networks. Sunnyvale, California, USA.

Kannan, Karthik, Jackie Rees, and Sanjay Sridhar. 2007. “Market Reaction to Information Security Breach Announcements: An Empirical Analysis.” *International Journal of Electronic Commerce* 12.1: 69-91.

Kenneth French Data Library. 2013. U.S. Research Returns Data. (accessed Oct. 1, 2013).

Liginlal, Divakaran, Inkook Sim, and Lara Khansa. 2009. “How Significant is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management.” Computers & Security 28.3: 215-228.

MacKinlay, A. Craig. 1997. "Event Studies in Economics and Finance." *Journal of Economic Literature* 35.1: 13-39.

McWilliams, Abagail, and Donald Siegel. 1997. "Event Studies in Management Research: Theoretical and Empirical Issues." *Academy of Management Journal* 40.3: 626-657.

Mikhail, Michael B., Beverly R. Walther, and Richard H. Willis. 1997. “Do Security Analysts Improve Their Performance with Experience?” *Journal of Accounting Research* 35: 131-157.

Miller, Amalia R., and Catherine E. Tucker. 2011. “Encryption and the Loss of Patient Data.” *Journal of Policy Analysis and Management* 30.3: 534-556.

Ponemon Institute 2013 Cost of Data Breach Study: United States. 2013. Ponemon Institute Research Report, Traverse City, Michigan, USA.

Ponemon Institute 2013 Global Study on Mobility Risks (Websense & CRN). 2013. Ponemon Institute Research Report, Traverse City, Michigan, USA.

Privacy Rights Clearinghouse. 2013. Chronology of Data Breaches. www.privacyrights.org/data-breach. (accessed Sep. 1, 2013)

Risk Based Security Management: United States. 2012. Ponemon Institute Research Report, Traverse City, Michgan, USA.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. 2011. "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management* 30.2: 256-286.

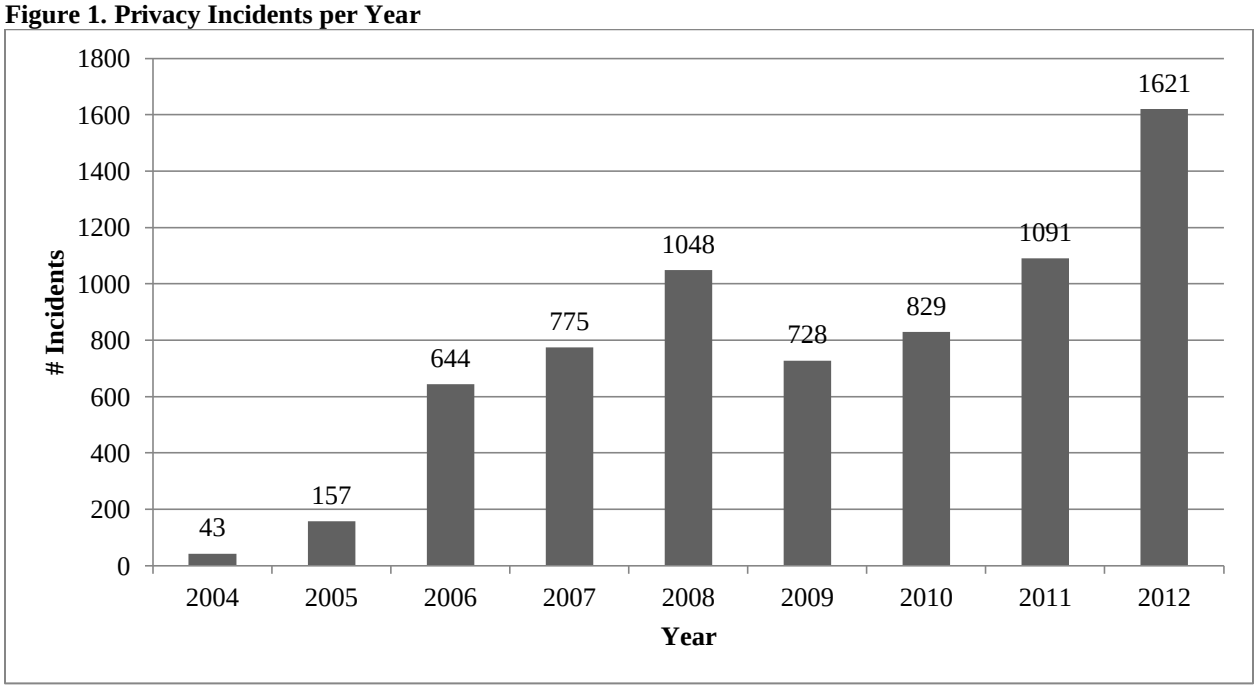
Schwartz, Paul, and Edward Janger. 2007. "Notification of Data Security Breaches." *Michigan Law Review* 105: 913.

U.S. Department of Health and Human Services. 2013. Breaches Affecting 500 or More Individuals. www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html. (accessed November 15, 2013)

Womack, Kent, and Ying Zhang. 2003. "Understanding Risk and Return, the CAPM, and the Fama-French Three-Factor Model." *Tuck Case* 03-111.

Appendix A

Figure 1. Privacy Incidents per Year



Appendix A

Table A.1. United States Legislation Related to Privacy Breaches[11]

Legislation	Privacy Focus	Specific Provision
Health Insurance Portability and Accountability Act (HIPPA)	Specifies how protected health information (PHI) should be managed by covered entities.	• Organizations may only release PHI with the prior written consent of the individuals. • Organizations should take reasonable steps to ensure the confidentiality of PHI and maintain proper records. • Individuals maintain the right to request to retrieve their PHI and to correct any inaccurate information.
Gramm-Leach-Bliley Act (GLBA)	Governs the collection and disclosure of customers' personal financial information by financial institutions	• Organizations must provide a consumer with a privacy notice when the consumer relationship is established and annually thereafter. • The privacy notice must describe which information is collect, where and how that information is used, and how that information is protected. • It must identity the consumer's right to opt-out of the sharing information with unaffiliated parties. • If the privacy policy changes, the consumer's consent must be obtained.
Family Educational Rights and Privacy Act (FERPA)	Regulated the rights and restrictions of parents, employees, and state agencies to access student educational records.	• Organizations must allow students to inspect and review their education records within 45 days of a request. • Students maintain the right to request the amendment of their education records that they believe is inaccurate, misleading, or otherwise in violation of their privacy rights. • Schools must obtain the students or parent's permission before allowing student records to be shared with a third party.
U.S.A. Patriot Act	Requires all U.S. businesses to provide access to customer information for law enforcement.	• Companies should establish a document management system to ensure ready access to documents and retention of documents relevant in litigation or other government investigation.

[11] Source: Liginlal et al. (2009)

		• Financial institutions must ensure that they have procedures for identifying customer account information and the ability to verify customer identity and maintain records of information used to verify identity.
The Fair and Accurate Credit Transactions Act	Requires proper disposal of consumer report information and records.	• Any person or company who maintains or otherwise possess consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.
The Identity Theft Penalty Enhancement Act	Established a new federal crime, i.e., aggravated identity theft.	• Any U.S. resident, knowingly transfers, possesses, or uses, without lawful authority a means of identification of another person or a false identification document will face punishment.
California SB 1386[12]	Defines and specifies the notification requirements, procedures, and timelines of customers' 'personal information.	• Specifies what type of data is subject to breach law (an individual's name, SSN, identification card number, account or credit card number, date of birth, biometric data). • Any person or business who reasonably believes that personal information has been acquired by an unauthorized person is required to notify the affected party. • Notice must be provided to affected individuals using either written notice, electronic notice with customer's consent, or a substitute notice.

[12] Most other state level data breach legislation is model after California SB 1386. Several proposed federal legislations have been modeled by this legislation.

Appendix B

Below are 3 CAR outputs for comparison. They compare Fama-French vs. CAPM using small, medium, and long estimation windows.

Table B.1

EVENT WINDOW	[0]	[+1]	[-1,+1]	[-1,+2]	[0,+1]	[0,+2]	[0,+3]
CAR (Fama-French)	-0.2081%	-0.2199%	-0.4958%	-0.3745%	-0.4280%	-0.3079%	-0.2813%
p-value (Fama-French)	0.0070	0.0000	0.0000	0.0070	0.0000	0.0150	0.0470
CAR (CAPM)	-0.1796%	-0.2349%	-0.4559%	-0.2489%	-0.4144%	-0.2075%	-0.1976%
p-value (CAPM)	0.0250	0.0000	0.0000	0.0890	0.0000	0.1030	0.1750

Small Estimation Window: [-100,-8], following Acquisti et al. (2006).

Table B.2

EVENT WINDOW	[0]	[+1]	[-1,+1]	[-1,+2]	[0,+1]	[0,+2]	[0,+3]
CAR (Fama-French)	-0.2136%	-0.2410%	-0.5331%	-0.4216%	-0.4546%	-0.3431%	-0.3260%
p-value (Fama-French)	0.0050	0.0000	0.0000	0.0020	0.0000	0.0060	0.0180
CAR (CAPM)	-0.1912%	-0.2501%	-0.4981%	-0.3037%	-0.4412%	-0.2469%	-0.2331%
p-value (CAPM)	0.0150	0.0000	0.0000	0.0380	0.0000	0.0540	0.1080

Medium Estimation Window: [-160,-2], following Cavusoglu et al. (2004).

Table B.3

EVENT WINDOW	[0]	[+1]	[-1,+1]	[-1,+2]	[0,+1]	[0,+2]	[0,+3]
CAR (Fama-French)	-0.2157%	-0.2309%	-0.5224%	-0.4100%	-0.4467%	-0.3355%	-0.3053%
p-value (Fama-French)	0.0040	0.0000	0.0000	0.0030	0.0000	0.0080	0.0270
CAR (CAPM)	-0.1986%	-0.2475%	-0.4977%	-0.3200%	-0.4460%	-0.2655%	-0.2501%
p-value (CAPM)	0.0120	0.0000	0.0000	0.0310	0.0000	0.0390	0.0870

Large Estimation Window: [-252,-7], following Gatzlaff and McCollough (2010).

Appendix B

Table B.4. Gatzlaff and McCollough (2010) metric of *MATURITY*

Variable Name	Coefficient	Robust Standard Error
Constant	0.006666	0.0091334
LN_MARKET_CAP	0.0002044	0.000897
REPEAT	0.0043982*	0.0023983
MATURITY	-0.0000258	0.0000365
MARKET_TO_BOOK	-1.66e-08***	8.38e-09
Observations	333	
R^2	0.0302	

Dependent variable: Cumulative Abnormal Return. Using 333 observations from the years 2005 – 2013. Corrected for heteroskedasticity with robust standard errors. Significance levels: * p<0.10, ** p<0.05, ***p<0.01.

Table B.5. Controlling for Type of Breach

Variable Name	Coefficient	Robust Standard Error
Constant	-0.0013491	0.012122
LN_MARKET_CAP	0.0001751	0.0009414
REPEAT	0.0035578*	0.00237
MATURITY	-0.0000264	0.0000396
MARKET_TO_BOOK	-1.54e-08*	8.39e-09
DISC	-0.0037857	0.008597
HACK	-0.0067947	0.0087678
CARD	-0.0085164	0.0142981
INSD	-0.0006278	0.0086869
PHYS	-0.0055167	0.008964
PORT	-0.0037982	0.0084362
STAT	-0.0119382	0.009457
Observations	333	
R^2	0.0439	

Dependent variable: Cumulative Abnormal Return. Using 333 observations from the years 2005 – 2013. Corrected for heteroskedasticity with robust standard errors. Significance levels: * p<0.10, ** p<0.05, ***p<0.01.
Note: Dummy variable descriptions *Source = Privacy Rights Clearinghouse.
DISC is a breach incident attributed to mishandling of sensitive information.
HACK is a breach incident attributed to an electronic entry of an outside source.
CARD is a breach incident attributed to fraud involving debit or credit cards that is not accomplished via hacking.
INSD is a breach incident attributed to an inside source intentionally breaches information.
PHYS is a breach incident attributed to the loss of a physical, non-electronic device.
PORT is a breach incident attributed to the loss of a physical, electronic device.
STAT is a breach incident attributed to lost, discarded, or stolen stationary electronic devices.
UNKN (suppressing) is a breach incident attributed to a breach that does not fall in any of the other categories.

Table B.6. Controlling for Number of Records Breached

Variable Name	Coefficient	Robust Standard Error
Constant	-0.0032753	0.0131544
LN_MARKET_CAP	0.0000789	0.0012193
REPEAT	0.0064933*	0.0033098
MATURITY	-0.0000675	0.0000703
MARKET_TO_BOOK	-2.78e-08***	2.19e-09
RECORDS	-3.32e-11	1.51e-10
Observations	159	
R^2	0.0831	

Dependent variable: Cumulative Abnormal Return. Using 159 observations from the years 2005 – 2013. Corrected for heteroskedasticity with robust standard errors. Significance levels: * p<0.10, ** p<0.05, ***p<0.01.

Table B.7. Controlling for Records Breached > 100,000

Variable Name	Coefficient	Robust Standard Error
Constant	-0.0044766	0.0092212
LN_MARKET_CAP	0.0001554	0.0008873
REPEAT	0.0047006*	0.0024499
MATURITY	-0.0000385	0.0000405
MARKET_TO_BOOK	-1.32e-08**	6.70e-09
Dummy_RECORDS	-0.0178956	0.0144689
Observations	333	
R^2	0.0477	

Dependent variable: Cumulative Abnormal Return. Using 333 observations from the years 2005 – 2013. Corrected for heteroskedasticity with robust standard errors. Significance levels: * p<0.10, ** p<0.05, ***p<0.01.
Acquist et al. (2006) found significance of (Records > 100,000) at the 10% level.