The Stock Market and Audit Market Effects of Data Security Breach Involving a Public Accounting Firm

Paul Tanyi
Belk College of Business, University of North Carolina Charlotte
ptanyi@uncc.edu

Marcia Watson
Belk College of Business, University of North Carolina Charlotte
mwatso40@uncc.edu

November 2019

ABSTRACT: This research provides insights into how audit clients and investors respond to a breach of confidential client data by an audit firm. Specifically, on September 25, 2017, Deloitte & Touche (a.k.a., Deloitte), an international Big 4 audit firm, reported that its systems had sustained a six month long cyber-attack lasting from October 2016 to March 2017 (Hopkins 2017). We examine whether Deloitte's reputation was affected by the breach. We find that Deloitte's data security breach did (1) negatively influence the appointment of Deloitte as independent auditor by prospective clients, and (2) negatively influence audit fees paid by new clients of Deloitte. We also show that (1) market reaction around the disclosure of the breach is more negative for Deloitte clients, and (2) investors react more positively (negatively) to the dismissal (appointment) of Deloitte as the audit firm following the disclosure of the breach.

Key words: security breach; auditor reputation; hack; audit market impact; event study

I. INTRODUCTION

This research provides insights into how audit clients and investors respond to a breach of confidential client data of a public accounting firm. Specifically, on September 25, 2017, *The Guardian* newspaper broke the story that Deloitte & Touche (a.k.a., Deloitte), an international Big 4 audit firm, had sustained a six month long cyber-attack lasting from October 2016 to March 2017 (Hopkins 2017). The hacker(s) compromised Deloitte's global email system through a weakly setup administrator's account that gave the hacker unlimited access to all areas of the company's audit, tax, and consulting practices. While Deloitte knew about the breach in March 2017, it did not publicly acknowledge the breach until September 25, 2017 when *The Guardian* reported on the story.

In this study, we examine the consequences of the breach for Deloitte and its audit clients. First, we compare audit client dismissals and engagements of Deloitte (as the independent auditor) and the audit fees paid to Deloitte before and after the breach. Second, we examine stock market effects for Deloitte's clients. Specifically, we examine the stock market reaction for clients when: (1) the breach was disclosed, and (2) audit clients dismissed or engaged Deloitte as their auditor-both before and after the data breach disclosure.

The Deloitte security breach is among one of several major failures involving a large public accounting firm in the last two decades. Previous failures involving major accounting firms (e.g., the role of Arthur Andersen in Enron collapse or the role of Ernst and Young in Lehman Brothers collapse) arose from the failure of the accounting firm to discover intentional manipulation of the financial statements by the management of clients (audit failure). However, the Deloitte data security breach is more of an operational failure that is non-audit engagement related, but (still) with potential consequences for their audit clients.

Deloitte is a member of the Big 4 accounting firms, a group of firms with a reputation for providing high quality services, thus allowing them to charge a premium for their services as well as to attract and retain clients (Krishnamurthy, Zhou, and Zhou 2006; Skinner and Srinivasan 2012; Weber, Willenborg, and Zhang 2008). While the consequences of a public accounting firm's audit failure has been extensively examined in prior accounting literature (e.g., Chaney and Philipich 2002; Blouin, Grein, and Rountree 2007; Cahan, Zhang, and Veenman 2011), the consequences to auditors for a non-audit related failure, e.g., failing to protect or secure confidential client data, has not been examined. Also, extant research (e.g., Gatzlaff and McCullogh 2010; Layton and Watters 2014; Acquisti, Friedman, and Telang 2006) on security breaches has largely focused on the consequences of client-specific data breaches.

We expect a security breach to have an impact on auditor reputation for several reasons. First, as part of their professional responsibility, accountants must protect the confidentiality of client data and not disclose it to a third party (IFAC 2006). According to prior auditing standards on client information, "The auditor has an ethical, and in some situations a legal, obligation to maintain the confidentiality of client information. Because audit documentation often contains confidential client information, the auditor should adopt reasonable procedures to maintain the confidentiality of that information" (PCAOB, AU Section 339, Par .11). By not securing its information networks and making it vulnerable to data breaches, Deloitte could have exposed sensitive, confidential, and otherwise protected client information to bad actors, a violation of PCAOB auditing rules. The breach also potentially highlights the lack of (internal) cyber security investment by Deloitte, which may be a concern to current and future clients. Clients may lose confidence in Deloitte thinking their data is insecure and, this may have a negative impact on a company's client base, particularly if the breach involves sensitive information.

Second, affected clients and their stakeholders could pursue litigation against Deloitte for failure to exercise reasonable care in protecting their information. The cost associated with defending the litigation and the adverse publicity and damage to the reputation of Deloitte brought by an arduous and lengthy litigation process could inevitably prevent the accounting firm from focusing on its clients. Finally, Deloitte clients may also be affected by the breach. The predominant harm for these clients following a breach is the perceived risk that confidential and sensitive information is potentially in the hands of bad actors. This information, if disseminated, can be extremely attractive to third parties, including clients' (legal) adversaries or competitors.

For a sample of Big 4 clients, we show that there is no difference in audit client dismissals of Deloitte before and after the data breach. We attribute the lack of an association between the data breach and the subsequent dismissal of Deloitte to the nature of the breach. According to media reports (e.g., Hopkins 2017), Deloitte insists the number of clients affected by the breach is small and the number of emails that were at risk were just a fraction. Thus, Deloitte may have engaged in some kind of damage control to reduce client concerns and departures by minimizing the nature and consequences of the breach to incumbent clients. However, we find that audit clients are less likely to appoint Deloitte as their independent auditor after the breach as compared to before breach. With respect to audit fees paid by Deloitte clients, we do not find any significant effect of the data breach on audit fees earned by Deloitte. However, when we divide the sample into continuing and new clients, we show that new Deloitte clients pay significantly lower audit fees post data breach. This finding persists even when we estimate a "changes" regression that examines the effect of the breach on changes in audit fees.

To better understand how investors respond to Deloitte's data breach, we conduct two different event studies. First, we examine the market reaction around the announcement of

the data breach using a long event window (-150, +30) that encompasses the period between the discovery and the public disclosure of the breach and a short event window (-3, +3) that includes only the days around the breach disclosure. Second, we compare the market reaction to clients' announcements of the dismissal or engagement of Deloitte as independent auditor before and after the data breach disclosure. We find a marginally significant negative market reaction to the breach for the long event window and a significantly negative market reaction to the short event window. We also find that the market reacts significantly positive (negative) to the dismissal (engagement) of Deloitte after the breach disclosure compared to before the breach disclosure.

Given the growing threat of breaches to audit firms, our research should be of interest to variety of constituents, including audit firms, regulators, and audit committees. Specifically, audit firms need to understand the consequences of not protecting their clients' data. Our research may provide them with extra incentive to invest and secure internal systems. With respect to regulators, our results should provide valuable input for the PCAOB and SEC, both of which have recently prioritizing cyber security as major initiatives (Hammer and Zuckerman 2018; PCAOB 2017a, 2017b). With respect to audit committees, as part of the audit firm hiring/firing/retention process, audit committees' may want to procure written assurances about the quality and security of the audit firm's internal systems to ensure that their companies' data remains secure and confidential.

We also contribute to the literature on the consequences of data security breaches disclosed by third parties (e.g., Amir, Levi, Livne 2018). Prior research (e.g., Campbell, Gordon, Loeb, and Zhou 2003; Cavusoglu, Mishra, and Raghunathan 2004; Kannan, Rees, and Shridhar 2007; Gordon, Loeb, and Zhou 2011; Kvochko and Pant 2015) examine the stock price reaction to cyber-attacks with mixed results. However, Amiret al. (2018) argue that investors may be more concerned with management's motive for withholding

information when the data security breach is revealed by an independent party. In the case of the Deloitte breach, the information about the hack is made public by *The Guardian* months after Deloitte discovered that its emailed system had been hacked. We find a negative cumulative market reaction around the disclosure of breach, consistent with the findings in Amir et al. (2018).

We organize the remainder of the study as follows. In the next section, we provide a background on the breach. Then, we review prior research on data security breaches and on audit reputation literature and develop our hypotheses. Second, we describe our sample and research design. Finally, we discuss the results and provide concluding comments.

II. BACKGROUND AND HYPOTHESES DEVELOPMENT

Background on Deloitte's Cyber-Security Breach

On September 25, 2017, *The Guardian* revealed that hackers had breached the global email server of Deloitte. Deloitte did subsequently confirm the news by saying that hackers had breached its email platform. This hack is the first ever publicly reported major cybersecurity breach involving one of the largest public accounting firms in the world. The hackers were able to get into Deloitte's email system by deciphering the password on an administrator's account that did not require a two-step authentication process (Davis 2017). The hackers in the sophisticated attack had compromised confidential emails and communications between Deloitte and clients across all sectors including some of Deloitte's largest clients like the U.S. Government (Hopkins 2017). According to *The Guardian*, the hackers may have had access to Deloitte systems in October or November of 2016. However, Deloitte did not discover the security breach of its email system until March 2017.

Following the discovery of the data security breach, on April 27, 2017, Deloitte hired the US law firm Hogan Lovells on "special assignment" to review what it called "a possible cybersecurity incident" (Hopkins 2017). Interestingly, Gartner, one of the world's leading

research and advisory company ranked Deloitte's Cyber Intelligence Centre, as the highest ranked firm based on revenue – among security consulting services companies. Deloitte had achieved the top revenue-based ranking for the sixth consecutive year (Deloitte 2016). The data security breach at Deloitte comes on the heels of a massive breach at a number of major U.S. corporations including Target Equifax, Sonic Whole Foods Markets, and Tinder. Figure 1 presents the timeline for the breach.

[Insert Figure 1 about her.]

In 2021, the estimated annual cost of cyber-crime will be $6 trillion, twice as much as it cost in 2015, and the "greatest transfer of economic wealth in history" (Morgan 2018). Well-established business leaders like Ginni Rommetty (IBM's CEO, chairman and president) and Warren Buffett (CEO of Berkshire Hathaway) stated that cyber-crimes/attacks are "the greatest threat to every company in the world" and the "number one problem with mankind" (Morgan 2018, Oyedele 2017), respectively. So, all companies need to prepare for, and attempt to prevent, cyber-attacks, which may lead to a data breach. A data breach is an "incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so…[it] may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property" (Lord 2018).

Not only is the number and magnitude of data breaches increasing, but the financial impact to companies is also increasing (Foltyn 2017). A 2016 survey by Ponemon Institute estimates the cost of a data breach to a company as $7 million dollars (Puzas 2016). The potential costs include remediation expenses to identify and stop the breach; regulatory fines; loss of revenues due to business disruption(s); legal expenses; direct financial loss from bank account drainages; and costs of notifying, assisting, and providing ID monitoring to affected parties (Puzas 2016). There are also the harder-to-quantify expenses such as

diminished goodwill and reputation leading to customer loss (Puzas 2016). In fact, a 2016 survey of 2,000 U.S. consumers finds that 76 percent would "move away" from companies with a high record of data breaches (Dark Reading Staff 2016).

Using this setting as a backdrop, we examine the audit market and stock market effects associated with the announcement of a Big 4 auditor breach of confidential client information. Specifically, on September 25, 2017, Deloitte & Touche (a.k.a., Deloitte), an international Big 4 audit/accounting firm, reported that its systems had sustained a six month long cyber-attack lasting from October 2016 and March 2017 (Hopkins 2017). The hacker compromised Deloitte's global email system through a weakly setup administrator's account that gave the hacker unlimited access to all areas of the company's audit, tax, and consulting practices. While Deloitte knew about the breach in March 2017, it did not publicly announce it until September 25, 2017.

Prior Literature on Data Security Breaches

Most extant research on security breaches focuses on the impact to the breached company by examining market reaction to the disclosure of the breach. However, the empirical studies that examine the stock price reaction to cyber-security attacks find mixed results. Several studies find negative abnormal market returns the disclosure of data security breaches and other cyber-attacks. For example, Cavusoglu et al. (2004) find a statistically significant negative effect to the disclosure of a data security breach. Campbell, et al. (2003) and Kannan, et al. (2007) do not find any significant market reaction to the disclosure of data security breach. Some studies e.g., Gordon, et al. (2011) provide empirical evidence that show a decline in the effect of breaches on stock prices over time. Kvochko and Pant (2015) also provide empirical evidence in recent cases in which major data breaches had a small impact on the firm share prices. These studies argue that the increased frequency of data breaches without apparent devastating effects on these firms (e.g., a firm filing

bankruptcy or going out of business because of a cyber-security incident) has lowered investors assessments of the risk associated with data security breaches.

However, empirical evidence from prior research shows that market reaction to cyber-attacks is influenced by whether the cyber-attack is voluntarily disclosed by the target firm to the public or whether the information was withheld from public and later independently reported by a third party like the Deloitte cyber-attack. Amir et al. (2018) show that target firms that withheld cyber-attack information are associated with a significant decline in market value when the attack is subsequently disclosed by a third party compared to firms that self- disclosed attacks.

Auditor Reputation

Public trust of the accounting profession is important for efficient capital markets. Big 4 audit firms strive to provide high quality audits to establish a reputation that allows them to charge higher audit fees and attract/retain clients (Krishnamurthy, et al. 2006; Skinner and Srinivasan 2012; Weber et al. 2008). However, when a Big 4 auditor reports an audit failure (e.g., missed fraud), it creates uncertainty about the quality of all of its audits as well as the accuracy of its clients' financial statements (Krishnamurthy, Zhou, and Zhou 2006). This uncertainty translates into an information transfer, or a negative market reaction, for the clients of the "failing" Big 4 audit firm.

For example, Weber et al. (2008) study the ComROAD fraud where the German company reported large amounts of fictitious revenue (63% to 97%), which went undetected for years by its auditor, KPMG. They find that KPMG's clients experience a negative 3% market reaction, especially for companies with higher demands for audit quality. Similarly, Gao, Jamal, Liu and Luo (2011) document negative abnormal returns of 4.4% for Deloitte's clients after its client Kelon Electronical Holdings Co Ltd was investigated by the China Securities Regulatory Commission for fictitious revenues, underestimating expenses, and

misappropriation of funds. This effect even includes affiliated audit groups as demonstrated by negative abnormal return for Pricewaterhouse (PwC)'s clients after its Japanese affiliate (ChuoAoyama) suffered an audit failure at Kanebo (Saito and Takeda 2014).

Auditor Reputation and Security Breaches

We expect a Big 4 security breach to have an impact on Big 4 auditor reputation for several reasons. First, a security breach is a type of operational control risk (i.e., the probability of a weakness in internal control over operations), which provides information about the companies' overall control environment (Lawrence, Minutti-Meza, and Vyas 2018). Therefore, a security breach may reflect a lack of commitment by management to support a strong internal control environment (Lawrence et al. 2018), which provides the basis for carrying out internal control across the organization (COSO 2013). This "tone at the top" attitude not only establishes the importance of internal controls, but "its attitude toward controls has pervasive effects on the actual control procedures throughout the organization also expected standards of conduct" (COSO 2013). So, a lack of attention to controls in cybersecurity (i.e., a weakly setup administrator's account) may indicate a lack of attention to controls and procedures over the entire auditing process, eroding auditor reputation.

Moreover, when a company loses control over its customer information, "it also suffers a loss of trust with its customers" (Pritchard 2018). Accountants, however, just do not serve customers. Rather, they develop relationships with clients and serve as the protectors of the public interest. As part of that responsibility, an accountant must protect the confidentiality of client data and not disclose it to a third party (IFAC 2006). Moreover, audit firm data is "extremely attractive to hackers" (Anonymous 2017). It contains non-public, strategic, financial, and operating data for their clients. If payroll/employment data is included, there is also PII. This information can be used as insider information to generate

profits in the stock market or manipulate the behavior of individuals. Unfortunately, "many CPA firms do not realize that they are at risk and/or do not have anything in place to protect themselves" (Anonymous 2017), indicating that the Deloitte breach may be just the tip of the iceberg for audit firm breaches of client data. A wrong step by one audit firm may negatively impact the entire profession because "[a]ccountants will lose their legitimacy as protectors of public interest if there is no public trust" (Jui and Wong 2013). The Deloitte breach highlighted the lack of cyber security investment by audit firms, which may negatively affect auditor reputation in this interconnected world.

Auditor Market Effects

We first examine the audit market effects of a Big 4 security breach. Audit market effects are usually evaluated by studying auditor dismissals and audit fees.

Auditor Dismissals/Engagements

If an audit client dismisses an auditor for any reason, the Securities and Exchange Commission (SEC) requires the company to file a Form 8-K Item 4.01 within four days of the dismissal. Audit clients dismiss auditors for a variety of reasons including: disagreements with the auditors, changes in operations, audit opinion shopping, or a desire to reduce audit fees (see Pacheco-Paredes, Rama, and Wheatley (2017) for a discussion).

Prior literature examines how the uncertainty around audit failures affect client retention. This literature builds on DeAngelo's (1981) work, that if a high-quality auditor is caught cheating by providing a low quality audit then it should be "punished" by its clients. In other words, market forces penalize audit firms associated with low quality audits (Swanquist and Whited 2015). Thus, if an audit firm is perceived to be executing lower quality audits, audit clients may dismiss the "failing" auditor (or potential clients may not engage the "failing" auditor). For example, Swanquist and Whited (2015) find that local audit offices have difficulty retaining and attracting clients after one of their existing audit

clients has a restatement. In addition, Weber et al. (2008) reports that KPMG's attrition rate doubled after the ComROAD audit failure (15.7% versus 7.7%). Similarly, Gao et al. (2011) find that Deliotte not only lost audit clients to local (not Big 4) audit firms, but all Big 4 firms also lost market share in the IPO market.

We build on this literature by examining whether (1) current audit clients dismissed Deloitte after the breach announcement and (2) Deloitte's rate of new client engagements changed after the breach announcement. If audit clients are worried about the confidentiality of auditor-client information after the breach, they may dismiss or are reluctant to appoint Deloitte as their independent auditor. However, as the complexity and size of an audit client increases, the cost of switching auditors also increases because the new auditor does not possess audit client specific knowledge and cannot have the same audit efficiencies (initially) as the incumbent auditor (Hennes, Leone, and Miller 2014). So, audit clients may not dismiss Deloitte as their auditor after the breach if they judge the switching costs too high. Given the competing arguments, we do not make a prediction about client retention for Deloitte after the breach announcement. We also examine whether the breach affected Deloitte's ability to attract new clients. If the breach affected Deloitte's reputation, new clients would be less likely to engage Deloitte as their auditor following the breach. Our first hypotheses are:

H1A: The likelihood of audit clients of Deloitte dismissing the auditor did not change after the breach announcement.

H1B: The likelihood of new clients engaging Deloitte decreased after the breach announcement.

Audit Fees

Extant literature examines audit fees from the client firm perspective. It generally supports the idea that auditors reduce the first couple years of audit fees (a.k.a., "low-

balling") to attract new audit clients (Ettredge, Scholz, and Li 2007). Big 4 auditors, on average, reduce initial audit fees by four percent (Ghosh and Lustgarten 2010). Research also finds that Big 4 auditors risk-adjust their audit fees. So, risky clients pay higher audit fees than less risky clients even in the initial engagement year (see Elliott, Ghosh, and Peltier 2013 for a discussion of the literature). Risky clients, on average, pay 23 percent more for the initial audit engagement than less risky clients (Elliott et al. 2013). Thus, Big 4 firms charge risky firms more for audits.

In the context of our topic, extant research finds that audit clients with cyber breaches are generally associated with higher audit fees due to increased client business risk and increased audit (control) risk (Higgs, Pinsker, and Smith 2018; Lawrence et al. 2018; Li, No, and Boritz 2017; Yen, Lim, Wang, and Han 2018). Once again, we flip the focus of the research and examine how the auditor's risky behavior affects their audit fee revenues. If Deloitte's security breach negatively affected its (high) quality reputation, then Deloitte may have to reduce its audit fees to attract new clients and/or keep current clients. Thus, total audit fee revenue for Deloitte clients may be reduced after the breach. This reasoning leads to the following hypothesis:

H2: Audit fee revenue for Deloitte is lower after the data breach.

Stock Market Effects

We next examine the stock market effects of the clients of Deloitte. First, there is a cost associated with data breaches. The highest costs correlate to the amount and sensitive nature of information accessed by the hackers in the cyber-security breach. Any communication between a client and auditor is normally considered privileged and sensitive information. Typical information that auditors received from clients in the process of an audit engagement will include for example copies of loans, leases and material contracts, copies of merger agreements, and lists of all bank accounts, including bank name, account

number and authorized signers. This is sensitive and important information that if made public can affect the competitive advantage of the target firm. If investors believe that the breach exposed sensitive client information that could potentially be used by the hackers to the disadvantage of the target firms, then the investors will react negatively to the disclosure of the breach.

Second, disclosure theory (Kasznik and Lev 1995; Amir et al. 2018) suggests one way to mitigate information asymmetry among market participants is by increasing transparency through how the breach notification is made. When investors know management had possessed and withhold negative information like the discovery of a data breach, they may reduce share price to reflect the worst possible news. As suggested earlier, Deloitte's email system was first hacked in late 2016, Deloitte discovered the breach in March 2017, and a third party, *The Guardian*, subsequently disclosed it in September 2017. Based on disclosure theory, we will investors will reduce stock prices assuming bad news was withheld. Thus, our last hypothesis is:

H3: Deloitte clients experienced a negative stock market price reaction around the disclosure of the data security breach.

III. DATA AND METHOD

Sample

Our sample consists of all clients of Big 4 audit firms with complete auditor-related data in Audit Analytics between 2004 and 2018. We focus only on Big 4 auditors because Deloitte, the audit firm that experienced the data breach, is a Big 4 audit firm and as such is fundamentally different from non-Big 4 in terms of the reputation, audit fee structure, client composition, and litigation risk (Dopuch and Simunic 1980; DeAngelo 1981). We merge the auditor related data from Audit Analytics with financial statement data from Compustat North America. Our final sample is 35,499 firm-year observations.

Model to Examine Auditor Changes and Audit Fees

Our first test examines whether the data breach disclosure is associated with the likelihood of the engagement or dismissal of Deloitte. Were audit clients more or less likely to dismiss or appoint Deloitte following the disclosure of the data breach? The second research question examines whether the disclosure of the data breach subsequently affected audit fees paid by clients of Deloitte. We use the following difference-in-difference logistic regression model to examine the relation between the disclosure of the data breach by Deloitte and the likelihood of the engagement or dismissal of Deloitte.

$$Dismissal = \beta_0 + \beta_1 Post + \beta_2 Dismissal\_Deloitte + \beta_3 (Post\ X\ Dismissal\_Deloitte) + \beta_4 Ln(Assets) + \beta_5 Ret\_Std + \beta_6 Ocf\_Std + \beta_7 Revt\_Std + \beta_8 Zmijewski\_Z + \beta_9 Roa + \beta_{10} Leverage + \beta_{11} Btm + \beta_{12} Revgrowth + \beta_{13} Ocf + \beta_{14} Ar\_Invt + \beta_{15} Icw + \beta_{16} Restate + \beta_{17} Gc + \beta_{18} Replag + \beta_{19} BusyYrEnd + Industry\ Effects \quad (1)$$

$$Engagement = \beta_0 + \beta_1 Post + \beta_2 Engagement\_Deloitte + \beta_3 (Post\ X\ Engagement\_Deloitte) + \beta_4 Ln(Assets) + \beta_5 Ret\_Std + \beta_6 Ocf\_Std + \beta_7 Revt\_Std + \beta_8 Zmijewski\_Z + \beta_9 Roa + \beta_{10} Leverage + \beta_{11} Btm + \beta_{12} Revgrowth + \beta_{13} Ocf + \beta_{14} Ar\_Invt + \beta_{15} Icw + \beta_{16} Restate + \beta_{17} Gc + \beta_{18} Replag + \beta_{19} BusyYrEnd + Industry\ Effects \quad (2)$$

The dependent variable in Equation 1, *Dismissal*, equals 1 if the firm's independent auditor changes from year t to year $t+1$, 0 otherwise. In Equation 2, *Engagement* equals 1 if the firm's independent auditor changes from year $t-1$ to year t, 0 otherwise. Therefore, we are examining whether a client dismisses or appoints a new auditor with the year t as the point of reference. *Dismissal_Deloitte* is 1 if the dismissed auditor in year t is Deloitte, 0 otherwise. *Engagement_Deloitte* equals 1 if the appointed auditor in year t is Deloitte, 0 otherwise. The independent variable, *Post*, equals 1 for the period after the announcement of the data breach, 0 otherwise. Our primary independent variables of interest are the interactions *Post X Dismissal_Deloitte* and *Post X Engagement_Deloitte*. The coefficient

β_3 in Equation 1 and Equation 2 indicates whether there is a significant difference in the likelihood of the dismissals or engagement of Deloitte pre- and post- the announcement of the data breach.

We also use the following difference-in-difference OLS regression model to examine whether there is any significant difference in the total audit fees paid by clients of Deloitte before and after the disclosure of the data breach using Equation 3.

$$\text{Ln}\ (Audfees) = \beta_0 + \beta_1 Post + \beta_2 Deloitte + \beta_3 (Post\ \text{X}\ Deloitte) + \beta_4 \text{Ln}(Assets) + \beta_5 Ret\_Std + \beta_6 Ocf\_Std + \beta_7 Revt\_Std + \beta_8 Zmijewski\_Z + \beta_9 Roa + \beta_{10} Leverage + \beta_{11} Btm + \beta_{12} Revgrowth + \beta_{13} Ocf + \beta_{14} Ar\_Invt + \beta_{15} Icw + \beta_{16} Restate + \beta_{17} Gc + \beta_{18} Replag + \beta_{19} Busy YrEnd + Industry\ Effects \quad (3)$$

The dependent variable in Equation 3 is the natural logarithm of total audit fees paid by client to the auditor in year t. The independent variable, *Deloitte,* equals 1 if the client's independent auditor in year t is Deloitte, 0 otherwise. The independent variable, *Post*, equals 1 for the period after the announcement of the data breach, 0 otherwise. The significance of the interaction variable, *Post X Deloitte,* captures the effect of the data breach on the total audit fees (*AudFees*) paid to Deloitte.

We control for the same independent variables in Equations 1, 2, and 3. We expect similar client and auditor specific factors that capture the overall risks associated with the audit engagement to influence auditor-client realignment and audit fee-pricing decisions (Ettredge and Greenberg 1990; Abbott, Parker, and Peters 2006; Schwartz and Soo 1996; Mande and Son 2012). We include several control variables shown in prior research to correlate with auditor changes and audit fees (Nichols and Smith 1983; Schwartz and Menon 1985; Francis and Wilson 1988; Johnson and Lys 1990; DeFond 1992; Ettredge and Greenberg 1990; Abbott et al. 2006; Schwartz and Soo 1996; Mande and Son 2012). We control for client by including the total assets (*Assets*). Evidence from prior accounting research suggests complexity can be associated with auditor-client realignment and audit

pricing decisions (Ettredge and Greenberg 1990; Sankaraguruswamy and Whisenant 2004). As a client's operational complexity increases (decreases), the number of agency relationships increases (decreases) making it difficult (easier) for external stakeholders to monitor managerial discretions.

We control for the company's financial condition by including variables that capture the profitability and solvency of the client (Nichols and Smith 1983; Schwartz and Menon 1985). Prior research suggest that auditors consider companies that are in good financial condition to have low audit risk. Hence, auditors will continue to seek a relationship with these clients or charge a higher audit fee premium to compensate for this risk. We control for the volatility of the stock returns (*Ret_Std*), volatility of cash flow from operations (*Ocf_Std*), and volatility of sales revenue (*Revt_Std*). We control for probability of bankruptcy (*Zmijewski_Z*), profitability (*Roa*), level of cash flow from operations (*OCF*), financial leverage (*Leverage*), growth opportunity (*Btm* and *Revgrowth*), and the proportion of total assets in receivables and inventory (*Ar_Invt*).

Following existing research on audit pricing and auditor changes (e.g., Raghunandan and Rama 2006; Ettredge et al. 2007; Huang, Raghunandan, and Rama 2009; Mande and Son 2012), we control for the quality of the client's financial reporting. We include indicator variables for material weakness in internal control over financial reporting (*Icw*) and the disclosure of an accounting misstatement in previously issued financial statements (*Restate*). We also include an indicator variable for modified going-concern opinion (*Gc*) following prior research on audit opinion shopping (Lu 2006; Krishnan and Stephens 1995). Finally, we control for audit report lag (*Replag*) and busy year-end audits (*BusyYrEnd*).

Model to Examine Market Reaction

In the second part of our analyses, we examine the market reaction to announcement of the data breach by Deloitte. We use a standard event study methodology to evaluate the

effects of the breach on Deloitte clients compared to non-Deloitte clients. We use the market model with a value-weighted index to estimate the abnormal returns around the announcement of the data breach on September 25, 2017. Assuming a firm's common stock returns follow a single factor market model, the return on firm *j*'s common stock on day *t*, is computed using the following equation:

$$R_{ut} = \alpha_j + \beta_j R_{mt} + \varepsilon_{jt},$$

where, R_{jt} is the rate of return of firm *j*'s common stock on day *t*; R_{mt} is rate of return of a CRSP's value weighted market index on day *t*, ε_{jt} is the random error that by construction, must have an expected value of 0, and is not correlated R_{mt}. We estimate the *daily abnormal returns* for firm *j*'s common stock on day *t* as the residual of the market model:

$$A_{jt} = R_{jt} - (\hat{\alpha}_j + \hat{\beta}_{j*} R_{mt})$$

We estimate daily abnormal returns over a long window and a short window. The long window includes 150 days before the announcement of the data breach and 30 days after the announcement. The short window includes three days before the announcement of the data breach and three days after the announcement. Though, the data breach was reported to the public on September 25, 2017, Deloitte had discovered the hack in March of that year. Following the discovery of the hack, Deloitte had pursued a number of actions that potentially could be suggestive of a data breach to the public even before the subsequent announcement. For example, according to the website Krebs on Security, the company had sent out a mandatory password reset email on to its employees in the United States. The notice stated that all employee passwords and personal identification numbers (PINs) must be changed, and any employees who failed to do so may not be to access their email or other Deloitte applications. On 27 April 27, 2017, *The Guardian* reports that Deloitte had retained the U.S. law firm Hogan Lovells on "special assignment" to review what it called "a possible cybersecurity incident" (Hopkins 2017). In the days and weeks

after the breach disclosure, there were a number media reports explaining the extent of the hack. The long event window enables us to capture any abnormal returns for any news worthy event around the announcement of the breach. To examine market reaction to the announcement of the data breach by Deloitte, we estimate the following OLS regression:

$$\textit{Cumulative Abnormal Returns} = \beta_0 + \beta_1 \textit{Deloitte} + \beta_3 \textit{Ln(Mkvl)} + \beta_4 \textit{Btm} + \beta_5 \textit{Momentum} + \textit{Industry Effect} \quad (5)$$

The dependent variable *Cumulative Abnormal Returns* is the cumulative abnormal returns over the long event window (-150, +30) and over the short event window (-3, +3). The independent variable of interest *Deloitte* is an indicator variable that takes the value 1 for a Deloitte client, 0 otherwise.

We also examine market reaction to 8-K filings disclosing the dismissal or engagement of Deloitte pre- and post- the announcement of data breach. We estimate we estimate the following difference-in-difference OLS regression:

$$\textit{Cumulative Abnormal Returns} = \beta_0 + \beta_1 \textit{Post} + \beta_2 \textit{Dismissal\_Deloitte} + \beta_3 (\textit{Post X Dismissal\_Deloitte}) + \beta_4 \textit{Engagement\_Deloitte} + \beta_5 (\textit{Post X Engagement\_Deloitte}) + \beta_6 \textit{Ln(Mkvl)} + \beta_7 \textit{Btm} + \beta_8 \textit{Momentum} + \textit{Industry Effect} \quad (6)$$

The dependent variable, *Cumulative Abnormal Returns* is the 3-day (-1, +1) or 7-day (-3, +3) cumulative abnormal returns around the filing of the Form 8–K that announces the dismissal or appointment of the auditor. Our primary independent variables of interest are the interactions *Post X Dismissal_Deloitte* and *Post X Engagement_Deloitte*. The coefficient β_3 and β_4 in Equation 6 indicates whether there is a significant difference in the market reaction to the dismissal or engagement of Deloitte pre- and post- the announcement of the data breach. Following prior event studies (e.g., Davidson, Xie, and Xu 2004; DeFond, Hann, and Hu 2005), we control in Equations 5 and 6 a number of other variables that may influence market reaction to events. We control for firm size (*Mkvl*), measured as the natural logarithm of the market value of equity; book to market value (*Btm*), measured as book

value per share scaled by market price per share; and the momentum (*Momentum*) of the firm's share price in the period before the event announcement. We make no predictions on the sign of the coefficients.

IV. EMPIRICAL RESULTS

Table 1 reports the summary statistics of variables used to estimate client dismissals/engagements of Deloitte and total audit fees paid to Deloitte pre- and post-announcement of data breach. Approximately, six percent of the firm-year observations are in the post data breach period. Deloitte clients represent about 24 percent of observations in the sample. Approximately, 10 percent (0.0042/0.0414) and 28 percent (0.0081/0.0288) of the auditor dismissals and engagements observations over the period 2004 to 2018 involve the dismissal and engagement of Deloitte, respectively.

[Insert Table 1 about here.]

Auditor Dismissals and Engagements Analyses

We present the results of the logistic regression model examining the effect of the data breach on Deloitte's dismissals and engagements in the first and second columns of Table 2, respectively. Both logistic regressions are estimated with industry fixed effects to control for industry-specific factors potentially correlated with auditor-client realignment decisions. The Chi-sq. statistics are estimated based on clustered standard errors. Both models are significant at the 1 percent level. In the first column of Table 2, the dependent variable, *Dismissals* equals 1 if the client dismissed the external auditor in year t and appoints a new auditor in year $t+1$, 0 otherwise. The independent variable of interest, *Post* X *Dismissals_Deloitte,* is not significant suggesting that the announcement of the data breach did not affect the likelihood of a client dismissing Deloitte. Many control variables load consistently with prior research. For example, we find a significantly positive association

between auditor dismissals and the following independent variables: internal control issues, restatements, going-concerns, and longer report audit report lag.

[Insert Table 2 about here.]

In the second column of Table 2, the dependent variable, *Engagements* equals 1 if the client dismissed an auditor in year *t-1* and appoints a new external auditor in year *t*, 0 otherwise. The independent variable of interest, *Post* X *Engagements_Deloitte* is negative and significant, suggesting that the announcement of the data breach is associated with a decrease in the likelihood of a client appointing Deloitte as its auditor in the post data breach period.

Auditor Fee Analyses

We present the results of the OLS regression model that examine the effect of the data breach on audits fees paid by clients of Deloitte in Table 3. The dependent variable is the natural logarithm of total audit fees paid by clients (*AudFees*). The independent variable *Deloitte* is an indicator variable that takes the value 1 for Deloitte clients, 0 otherwise. The independent variable of interest, *Post* X *Deloitte*, captures the significance of the audit fees earned by Deloitte in the post data breach period. In the first column of Table 3, we estimate the OLS model for the full sample. However, because clients have a stronger bargaining power over the audit fees paid to the independent auditor when it comes to negotiating first year audits compared ongoing audit engagements (Simon and Francis 1988; Ettredge and Greenberg 1990; and Deis and Giroux 1996), we separate the sample in to continuing audit engagements (column 2) and first year audit engagements (column 3).

[Insert Table 3 about here.]

In the first column of Table 3, the coefficient of *Post* X *Deloitte* is negative, but not significant; suggesting that the data breach did not affect the bargaining power of Deloitte with respect to the total audits fees associated with its audit engagements in the post data

breach period. In the second column of Table 3 where we only consider the effect of data breach on continuing engagements, the coefficient of *Post* X *Deloitte* is also negative, but not also significant. However, in the third column (first year audits), the coefficient of the interaction variable, *Post X Deloitte* is negative and significant, indicating that first year audit clients of Deloitte paid significantly lower total audit fees after the data breach disclosure.

In a related sensitivity analysis, we also estimate a "changes" regression model that examines the effect of the data breach on changes in total audit fees as in addition to the "levels" model in Table 3. The total audit fees paid by a client is jointly determined with many other firm- and industry-related attributes, suggesting that a cross-sectional approach based on variable levels alone mixes the antecedents and consequences of changes in audit fees (Vafeas and Waegalein 2007). To address this problem, we re-estimate an OLS regression model that examines the effect of the data breach on changes in total audit fees and controlling for changes in other potential determinants of changes in audit fees. We present the results of this analysis in Table 4. Similar to the Table 3 results, the coefficient of *Post* X *Deloitte* is insignificant for All engagements (column 1) and continuing engagements (column 2), but significantly negative for first year audit engagements (column 3). This result is consistent with the "levels" analysis and suggests that in the post data breach period, new Deloitte clients experience a significant reduction in audit fees.

[Insert Table 4 about here.]

Market Reaction Analyses

In this section, we examine market reaction to the disclosure of the data breach. Examining the market reaction to the disclosure of the breach enables us to evaluate investors' assessment of the economic impact of the breach from concerns regarding confidentiality, integrity and accessibility of audit client information that potentially could

be exposed (and used) by bad actors. Figure 2 presents a graph of the long-window daily cumulative abnormal returns beginning 150 before the disclosure of the breach and ending 30 days after the disclosure of the data breach. The graph shows that over this long-event window, clients of Deloitte had lower cumulative abnormal returns compared to other non-Deloitte Big 4 clients. In Panel A, Table 5, we compare the mean cumulative abnormal returns around the event window between Deloitte and other non-Deloitte Big 4 clients. We find that there is a significant difference in the mean cumulative abnormal returns between the two groups at 1 percent level of significance.

[Insert Figure 2 about here.]

[Insert Table 5 about here.]

In Panel B, Table 5, we report the descriptive statistics of the variables in the OLS regression model to examine market reaction to the event disclosure after controlling for other variables. The two dependent variable are the long-window cumulative abnormal returns (-150, +30) and the short event window (-3, +3). The average cumulative abnormal returns for the long and short window for observations in the sample are -1.07 and 1.88 percent respectively. Approximately, 21.23 percent of observations in this sample is Deloitte clients.

We present the results of the OLS analysis in Table 6. The dependent variable is the cumulative abnormal market returns estimated over a long window and over a short window around the disclosure date of the breach using the market model with a value-weighted index. The independent variable of interest, *Deloitte* is an indicator variable that takes the value 1 for Deloitte clients, 0 otherwise. We find that market reaction to the disclosure of the breach is negative, marginally significant for the long event window, and significantly negative for the short event window. Overall, this signals that the market perceives the breach as potentially having negative consequences for the clients of Deloitte.

[Insert Table 6 about here.]

The second part of the market reaction analysis compares the market reaction to dismissal and engagement of Deloitte as the independent auditor before and after disclosure of the breach. We use the market model with a value-weighted index to estimate the cumulative abnormal return around: (1) the dates of announcement of the dismissal of Deloitte and other Big 4 audit firms between 2004 and 2018, and (2) the dates of announcement of the engagement of Deloitte and other Big 4 audit between 2004 and 2018. Table 7 presents the descriptive statistics of the variables in the model to examine market reaction to the announcement of the dismissal or appointment of Deloitte as independent auditor pre- and post- the disclosure. *A priori*, we would suggest that the market might interpret the dismissal of Deloitte as auditor following the disclosure of the breach as potentially signaling that unfavorable confidential client information may have been compromised in the breach leading the client to dismiss Deloitte. The potential leakage of sensitive client information obtained from communications between client and auditor may lead to a loss of competitive edge. Hence, such concerns can cause investors to react negatively dismissal of the Deloitte. However, it also possible that the dismissal of Deloitte gives the client an opportunity to seek another auditor with better data security. This could elicit a positive market reaction from shareholders. Investors may have concerns about data security and information confidentiality when a company appoints Deloitte as their auditor. Therefore, we may expect an adverse market reaction to the appointment of Deloitte as auditor following the breach.

[Insert Table 7 about here.]

Table 8 presents the results of the difference-in-difference OLS regression that examines market reaction to the dismissal or appointment of Deloitte before and after the disclosure of the data breach. The dependent variable is the market reaction 3-day (-1, +1)

and 7-day (-3, +3) cumulative abnormal market reaction around the dates of announcements of the dismissal or appointment of Big 4 audit firms between 2004 and 2018. We estimate the abnormal returns on the day of those announcements using the market model with a value-weighted index. The independent variable *Dismissals_Deloitte* is an indicator variable that equals 1 if the departing auditor is Deloitte, 0 otherwise. *Engagements_Deloitte* is an indicator variable that equals 1 if the incoming auditor is Deloitte, 0 otherwise. Overall, the coefficient of *Post X Dismissals_Deloitte* is positive and significant, suggesting that investors react positively to the dismissal of Deloitte in the post data breach period. On the other hand, the coefficient of *Post X Engagements_Deloitte* is negative and significant. Taken together these findings suggest that investors react positively (negatively) to the dismissal (appointment) of Deloitte in the post data breach period compared to the pre data breach period.

[Insert Table 8 about here.]

V. CONCLUSION

We examine whether a security breach may negatively influence the reputation of an auditor. Specifically, we examine how audit clients and investors respond to a breach of confidential client data by Deloitte. On the one hand, we find that Deloitte's audit clients at the time of the breach did not experience a change in audit fees, nor were they more likely to dismiss Deloitte. This finding indicates that Deloitte's relationship with its current clients was able to mitigate any negative impact of the cyber-security breach. On the other hand, prospective clients were less likely to appoint Deloitte as their independent auditor after the breach. In addition, we show that the disclosure of the breach is associated with lower audit fees for new Deloitte clients. Thus, the security breach did have a negative

impact on Deloitte's reputation in the new audit client market. This is significant as the audit market is increasingly competitive with (increasing) downward pressure of audit fees.

Analyzing market reaction to the breach, we find an overall significant negative market reaction to the disclosure of the data security breach. Second, we find a positive (negative) market reaction when clients dismissed (appointed) Deloitte as their independent auditor after the breach. This result is consistent with the market viewing the security breach as potential having negative consequences for current clients of Deloitte as well as future concerns of the confidential relationship between an auditor and its new clients.

REFERENCES

Abbott, L. J., S. Parker, and G. F. Peters. 2006. Earnings management, litigation risk, and asymmetric audit fee responses. *Auditing: A Journal of Practice & Theory* 25(1): 85-98.

Anonymous. 2017. 2017 Top 100 people extra: Accounting's biggest issues. *Accounting Today* (September 8). Available on-line on 1/2/2018 at: https://www.accountingtoday.com/news/2017-top-100-people-extra-accountings-biggest-issues

Acquisti, A., A. Friedman, and R. Telang. 2006. Is there a cost to privacy breaches? An event study." *ICIS 2006 Proceedings*: 94.

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

Blouin, J., B. M. Grein, and B. R. Rountree. 2007. An analysis of forced auditor change: The case of former Arthur Andersen clients. *The Accounting Review* 82 (3): 621-650.

Cahan, S., W. Zhang, and D. Veenman. 2011. Did the Waste Management Audit Failures Signal Lower Firm-Wide Audit Quality at Arthur Andersen? *Contemporary Accounting Research* 28 (3): 859-891.

Campbell K., L. A. Gordon, M. P. Loeb, and L. Zhou. 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security* 11(3): 431-48.

Cavusoglu, H., B. Mishra, and S. Raghunathan. 2004. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce* 9(1): 69-104.

Chaney, P. K., and K. L. Philipich. 2012. Shredded reputation: The cost of audit failure. *Journal of Accounting Research* 40 (4): 1221-1245.

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

Dark Reading Staff. 2016. Survey: Customers lose trust in brands after a data breach. *Dark Reading* (5/18). Available on-line on 1/2/2018 at: https://www.darkreading.com/vulnerabilities---threats/survey-customers-lose-trust-in-brands-after-a-data-breach/d/d-id/1325570

Davidson, W. N., B. Xie, and W. Xu. 2004. Market reaction to voluntary announcements of audit committee appointments: The effect of financial expertise. *Journal of Accounting and Public Policy* 23(4): 279-293.

Davis, J. 2017. Deloitte breach tied to lack of multifactor authentication for admin account. Healthcare IT News. Available on-line on 11/08/2019 at:

https://www.healthcareitnews.com/news/deloitte-breach-tied-lack-multifactor-authentication-admin-account

DeAngelo, L. 1981. Auditor size and audit quality. *Journal of Accounting & Economics* 3: 183-199.

DeFond, M. L. 1992. The association between changes in client firm agency costs and auditor switching. *Auditing: A Journal of Practice & Theory* 1 (1): 16-31.

DeFond, M. L., R. N. Hann, and X. Hu. 2005. Does the market value financial expertise on audit committees of boards of directors? *Journal of Accounting Research* 43(2): 153-193.

Deis, D. R., and G. Giroux. 1996. The effect of auditor changes on audit fees, audit hours, and audit quality. *Journal of Accounting and Public Policy* 15(1): 55-76.

Deloitte. 2016. Deloitte recognized as No. 1 in Global Business Consulting by ALM Intelligence, ranked #1 in Consulting Service Providers by Market Share, Worldwide 2015 by Gartner, and named a Leader by IDC MarketScape. Available on-line on 11/08/2019 at: https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-number-one-global-business-consulting.html

Dopuch, N., and D. Simunic. 1980. The nature of competition in the auditing profession: a descriptive and normative view. *Regulation and the Accounting Profession* 34(2): 283-289.

Elliott, J. A., A. Ghosh, and E. Peltier. 2013. Pricing of risky initial audit engagements. *Auditing: A Journal of Practice & Theory* 32(4): 25-43.

Ettredge, M., and R. Greenberg. 1990. Determinants of fee cutting on initial audit engagements. *Journal of Accounting Research* 28(1): 198-210.

Ettredge, M., S. Scholz, and C. Li. 2007. Audit fees and auditor dismissals in the Sarbanes-Oxley era. *Accounting Horizons* 21(4): 371-386.

Ettredge, M. and V. J. Richardson. 2003. Information transfer among Internet firms: The case of hacker attacks. *Journal of Information Systems* 17(2): 71-82.

Foltyn, T. 2017. ISF predicts increasing impact of data breaches next year. *welivesecurity* (December 5). Available on-line on 1/2/2018 at: https://www.welivesecurity.com/2017/12/05/isf-predicts-data-breaches-2018/

Francis, J. R., and E. R. Wilson. 1988. Auditor changes: A joint test of theories relating to agency costs and auditor differentiation. *The Accounting Review* 63(4): 663-682.

Gao, Y., K. Jamal, Q. Liu, and L. Luo. 2011. Does reputation discipline Big 4 auditors? CAAA Annual Conference 2011. University of Alberta School of Business Research Paper No. 2013-1006. Available on-line on 1/25/2018: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1633724

Garg, A., J. Curtis, and H. Halper. 2003. The real cost of being hacked. *The Journal of Corporate Accounting & Finance* (Jul/Aug): 49-52.

Gatzlaff, K. M., and K. A. McCullough. 2010. The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review* 13 (1): 61-83.

Ghosh, A. ad S. Lustgarten. 2006. Pricing of initial audit engagements by large and small audit firms. *Contemporary Accounting Research* 23(2): 333-368.

Gordon, L. A., M. P. Loeb, and L. Zhou. 2011. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security* 19 (1): 33-56.

Hammer, D., and J. Zuckerman. 2018. Protections and rewards for cybersecurity whistleblowers. February 7. Accessed on March 30, 2018 from: https://www.zuckermanlaw.com/protections-and-rewards-for-cybersecurity-whistleblowers/

Hennes, K. M., A. J. Leone, and B. P. Miller. 2014. Determinants and market consequences of auditor dismissals after accounting restatements. *The Accounting Review* 89(3): 1051-1082.

Higgs, J. L., R. Pinsker, and T. J. Smith. 2018. Do auditors price breach risk in their audit fees? Forthcoming, *Journal of Information Systems*.

Hopkins, N. 2017. Deloitte hit by cyber-attack revealing clients' secret emails. *The Guardian* (September 25). Available on-line on 1/24/2018 at: https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

Huang, H-W, K. Raghunandan, and D. Rama. 2009. Audit fees for initial audit engagements before and after SOX. *Auditing: A Journal of Practice & Theory* 28(1): 171-190.

IFAC. 2006. Code of ethics for professional accountants. Available on-line on 1/26/2018: https://www.ifac.org/system/files/publications/files/ifac-code-of-ethics-for.pdf

Johnson, W. B., and T. Lys. 1990. The market for audit services: Evidence from voluntary auditor changes. *Journal of Accounting and Economics* 12(1-3): 281-308.

Jui, L. and J. Wong. 2013. Roles and importance of Professional Accountants in business. Available on-line on 1/24/2018 at: https://www.ifac.org/news-events/2013-10/roles-and-importance-professional-accountants-business

Kannan, K., J. Rees, and S. Sridhar. 2007. Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce* 12, (1): 69-91.

Kasznik, R., and B. Lev. 1995. To warn or not to warn: Management disclosures in the face of an earnings surprise. *The Accounting Review* 70 (1): 113-134.

Krishnamurthy, S., J. Zhou, and N. Zhou. 2006. Auditor reputation, auditor independence, and the stock-market impact of Andersen's indictment on its client firms. *Contemporary Accounting Research* 23(2): 465-490.

Krishnan, J., and R. G. Stephens. 1995. Evidence on opinion shopping from audit opinion conservatism. *Journal of Accounting and Public Policy* 14(3): 179-201.

Kvochko, Elena, and Rajiv Pant. 2015. Why data breaches don't hurt stock prices. *Harvard Business Review* 31.

Layton, R., and P. A. Watters. 2014. A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications* 19 (6): 321-330.

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

Li, H., W. G. No, and J. E. Boritz. 2017. Are external auditors concerned about cyber incidents? Evidence from audit fees? Working paper, Rutgers and University of Waterloo. Available on-line on 1/25/2018 at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2880928

Lord, N. 2018. The history of data breaches. *Digital Guardian* (January 15). Available on-line on 1/20/2018 at: https://digitalguardian.com/blog/history-data-breaches

Lu, T. 2006. Does opinion shopping impair auditor independence and audit quality? *Journal of Accounting Research* 44(3): 561-583.

Mande, V., and M. Son. 2012. Do financial restatements lead to auditor changes? *Auditing: A Journal of Practice & Theory* 32(2): 119-145.

Morgan, S. 2018. Top cybersecurity facts, figures, and statistics for 2018. *CSO from IDG* (January 23). Available on-line on 1/28/2018 at: https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

Nichols, D. R., and D. B. Smith. 1983. Auditor credibility and auditor changes. *Journal of Accounting Research* 21(2): 534-544.

Oyedele, A. 2017. BUFFETT: This is 'the number one problem with mankind' (May 6). Available on-line on 1/2/2018: http://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5

Pacheco-Paredes, A. A., D. V. Rama, and C. M Wheatley. 2017. The timing of auditor hiring: Determinants and consequences. *Accounting Horizons* 31(3): 85-103.

Puzas, D. 2016. Ten reasons average data breach costs $7 million. Available on-line on 11/10/2016 at: https://www.secureworks.com/blog/ten-reasons-average-data-breach-costs-7-million

Pritchard, S. 2018. Top seven data loss issues. Available on-line on 1/24/2018 at: http://www.computerweekly.com/feature/Top-seven-data-loss-issues

Public Company Accounting Oversight Board (PCAOB). 2017a. PCAOB publishes staff inspection brief Previewing 2016 inspection findings. Accessed on March 29, 2018

at: https://pcaobus.org/News/Releases/Pages/staff-inspection-brief-2016-preview-11-9-17.aspx

Public Company Accounting Oversight Board (PCAOB). 2017b. Staff inspection brief (August). Available on-line on 1/22/2018: https://pcaobus.org/Inspections/Documents/inspection-brief-2017-3-issuer-scope.pdf

Public Company Accounting Oversight Board (PCAOB). 2004. Auditing Standard No. 3, Audit Documentation. PCAOB Release 2004-006 https://pcaobus.org/Standards/Archived/Pages/AU339b.aspx

Raghunandan, K., and D. V. Rama. 2006. SOX Section 404 material weakness disclosures and audit fees. *Auditing: A Journal of Practice & Theory* 25(1): 99-114.

Richardson, V. J., M. W. Watson, and R. Smith. 2018. Much Ado about Nothing: The (lack of) economic impact of data privacy breaches. Forthcoming, Journal of Information Systems.

Saito, Y and F. Takeda. 2014. Global audit firm networks and their reputational risk. *Journal of Accounting, Auditing & Finance* 29(3): 203-237.

Sankaraguruswamy, S., and J. S. Whisenant. 2004. An empirical analysis of voluntarily supplied client-auditor realignment reasons. *Auditing: A Journal of Practice & Theory* 23(1): 107-121.

Schwartz, K. B., and K. Menon. 1985. Auditor switches by failing firms. *The Accounting Review* 60(2): 248-261.

Schwartz, K. B., and B. S. Soo. 1996. The association between auditor changes and reporting lags. *Contemporary Accounting Research* 13(1): 353-370.

Simon, D. T., and J. R. Francis. 1988. The effects of auditor change on audit fees: Tests of price cutting and price recovery. *The Accounting Review* 63(2): 255-269.

Skinner, D. J., and S. Srinivasan. 2012. Audit quality and auditor reputation: Evidence from Japan. *The Accounting Review* 87 (5): 1737-1765.

Spanos, G., and L. Angelis. 2016. The impact of information security events to the stock market: A systematic literature review. *Computers & Security* (2016): 216-229.

Swanquist, Q. T., and R. L. Whited. 2015. Do clients avoid "Contaminated" offices? The economic consequences of low-quality audits. *The Accounting Review* 90(6): 2537-2570.

Weber, J., M. Willenborg, and J. Zhang. 2008. Does auditor reputation matter? The case of KPMG Germany and ComROAD AG. *Journal of Accounting Research* 46(4): 941-972.

Vafeas, N., and J. F. Waegelein. 2007. The association between audit committees, compensation incentives, and corporate audit fees. *Review of Quantitative Finance and Accounting* 28(3): 241-255.

Yen, J-C., J-H. Lim, T. Wang, and C. Han. 2018. The impact of audit firms' characteristics on audit fees following information security breaches. Forthcoming, *Journal of Accounting and Public Policy*.

Appendix A: Variable Definitions

Post	1 for the period after the data breach is disclosed to the public, 0 otherwise;
Deloitte	1 for Deloitte audit client, 0 otherwise;
Dismissals	1 if the client changes independent auditor from year *t* to year *t+1*, 0 otherwise;
Dismissals_Deloitte	1 if the client switches from Deloitte from year *t* to year *t+1*, 0 otherwise;
Engagements	1 if the client changes independent auditor from year *t-1* to year *t*, 0 otherwise;
Engagements_Deloitte	1 if the client switches to Deloitte from year *t-1* to year *t*, 0 otherwise;
Audfees	Total fees paid to audit firm in year *t*;
Assets	Client's total assets at the beginning of year *t*;
Ret_Std	The standard deviation of monthly stock returns in year *t*;
Ocf_Std	The standard deviation of cash flows from operations over the most recent 5-year period including year *t*;
Revt_Std	The standard deviation of sales revenues scaled by total assets over the most recent 5-year period including year *t*;
Zmijewski_Z	Probability of bankruptcy in year *t* calculated using Zmijewski (1984's) bankruptcy prediction model;
Roa	Income before tax scaled by total assets at the beginning of year *t*;
Leverage	Total long-term debt scaled by total assets in year *t*;

Btm	Book value per share divided market price per share at the beginning of year *t*;
Revgrowth	Change in total sales revenue from year *t-1* to year *t*;
Ocf	Cash flow from operations in year *t* divided by total assets at the beginning of year *t*;
Ar_Invt	The sum of total inventory and receivables divided by total assets at the beginning of year *t*;
Icw	1 if the company reported material weakness in internal controls over financial reporting in year *t*;
Restate	1 if the company reported an accounting restatement in year *t*;
Gc	1 if the company received a modified going concern opinion in year *t*;
Replag	the total number of days between the end of the fiscal year and audit report date;
BusyYrEnd	1 if the company's fiscal year ends in December or January, 0 otherwise;
Cumulative Abnormal Returns (*-150, +30*)	The cumulative abnormal returns over the period 150 days before the announcement of the breach and 30 days after the announcement;
Cumulative Abnormal Returns (*-3, +3*)	The cumulative abnormal returns over the period 3 days before the announcement of the breach and 3 days after the announcement;
Momentum	The trailing 3-year return on the firm's stock

Figure 1: Timeline of Deloitte Data breach

Figure 2: Cumulative Abnormal Returns around the Data Breach Disclosure (Market Model with Value-Weighted Index)

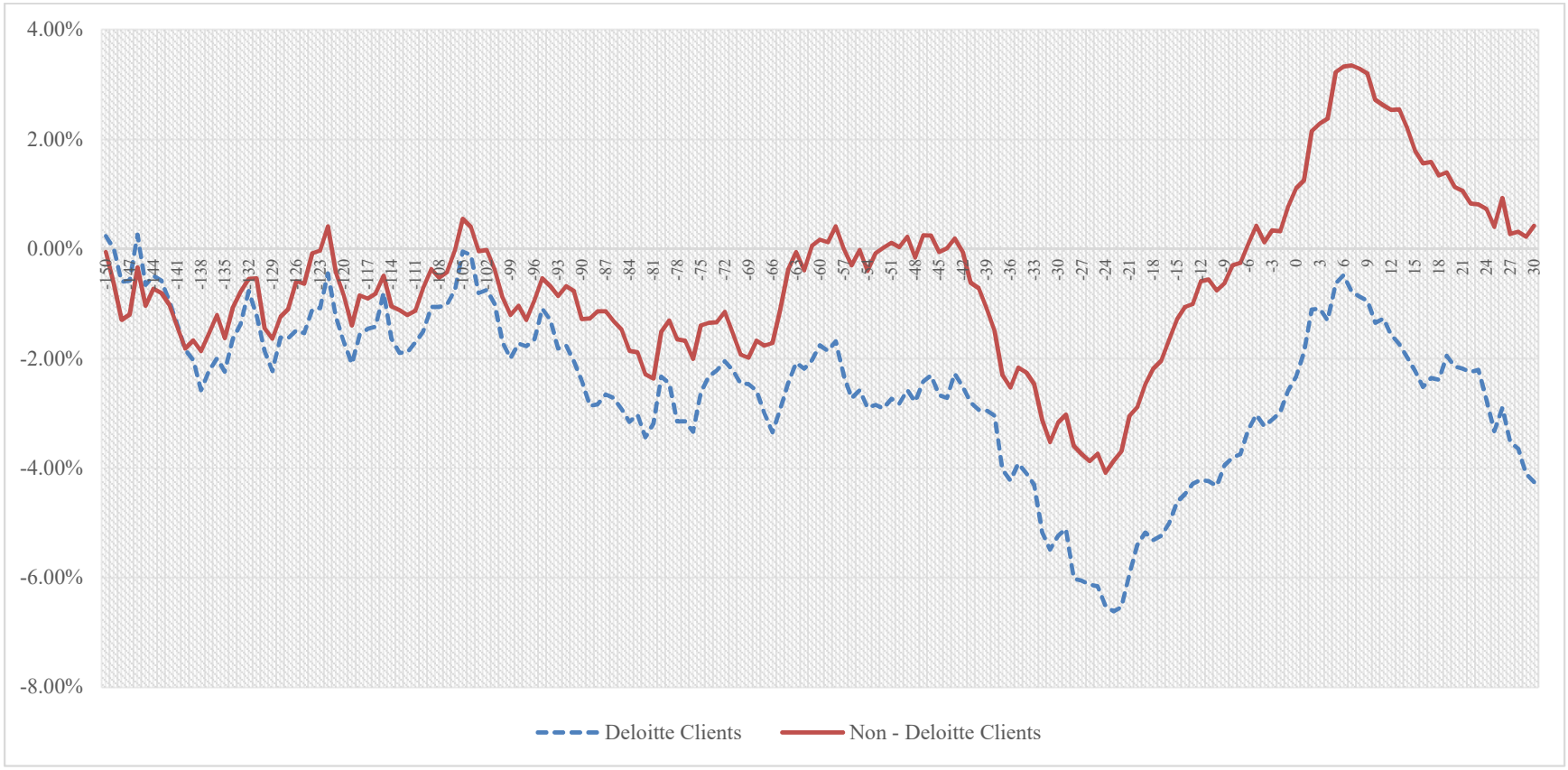

Table 1: Summary Statistics

	N	Mean	Median	Lower Quartile	Upper Quartile	Std Dev
Post	35,499	0.0552	0.0000	0.0000	0.0000	0.2283
Deloitte	35,499	0.2363	0.0000	0.0000	0.0000	0.4248
Dismissals	35,499	0.0414	0.0000	0.0000	0.0000	0.1993
Dismissals_Deloitte	35,499	0.0042	0.0000	0.0000	0.0000	0.0649
Engagements	35,499	0.0288	0.0000	0.0000	0.0000	0.0948
Engagements_Deloitte	35,499	0.0081	0.0000	0.0000	0.0000	0.0897
Audfees ($)	35,499	2,564,777.56	1,352,500.00	718,702.00	2,740,000.00	3,966,563.43
Assets ($)	35,499	5,595,388,275	987,988,000	269,562,000	3,606,784,000	18,154,437,499
Ret_Std	35,499	0.7010	0.3268	0.1772	0.5744	2.4423
Ocf_Std	35,499	0.0973	0.0342	0.0170	0.0690	0.5533
Revt_Std	35,499	0.1806	0.0934	0.0398	0.2012	0.3609
Zmijewski_Z	35,499	-0.8800	-1.2739	-2.3528	-0.2727	5.6860
Roa	35,499	-0.0457	0.0323	-0.0257	0.0720	0.5241
Leverage	35,499	0.2254	0.1817	0.0060	0.3371	0.2430
Btm	35,499	0.3900	0.3922	0.2134	0.6439	1.2161
Revgrowth	35,499	0.1647	0.0701	-0.0155	0.1863	0.6825
Ocf	35,499	0.0375	0.0855	0.0342	0.1406	0.3880
Ar_Invt	35,499	0.2118	0.1766	0.0728	0.3107	0.1683
Icw	35,499	0.0508	0.0000	0.0000	0.0000	0.2197
Restate	35,499	0.0902	0.0000	0.0000	0.0000	0.2864
Gc	35,499	0.0286	0.0000	0.0000	0.0000	0.1668
Replag (days)	35,499	64.23	60.00	55.00	72.00	30.04
BusyYrEnd	35,499	0.7804	1.0000	1.0000	1.0000	0.4140

Table 2: The Dismissal and Engagement of Deloitte Pre and Post Data Breach

Variables	*Dismissals*		*Engagements*	
Intercept	1.8477	***	-4.9677	***
	(7.07)		(30.57)	
Post	-2.9798	***	-0.6439	***
	(17.67)		(5.93)	
Dismissals_Deloitte	0.3671			
	(0.04)			
Post X Dismissals_Deloitte	**0.0157**			
	(0.18)			
Engagements_Deloitte			0.9698	***
			(99.08)	
Post X Engagements_Deloitte			**-1.0044**	***
			(5.96)	
Ln (*Assets*)	-0.4234	***	-0.1085	***
	(331.55)		(15.41)	
Ret_Std	0.0124		0.0106	
	(1.30)		(0.64)	
Ocf_Std	0.3924	**	-0.1606	**
	(4.33)		(6.00)	
Revt_Std	0.0562		0.0500	
	(0.33)		(0.48)	
Zmijewski_Z	-0.0001		0.0003	
	(0.01)		(0.02)	
Roa	0.0018		0.0136	
	(0.03)		(0.05)	
Leverage	0.2060		0.3747	*
	(1.85)		(3.47)	
Btm	0.0796	***	0.0879	*
	(6.88)		(3.65)	
Revgrowth	-0.0593		0.1576	***
	(1.57)		(15.73)	
Ocf	0.1250		0.1623	
	(0.77)		(0.78)	
Ar_Invt	0.4420	**	0.0903	
	(5.52)		(0.13)	

Icw	0.9314	***	-0.4677	***
	(80.10)		(10.72)	
Restate	0.2279	**	-0.7046	***
	(5.09)		(38.70)	
Gc	0.4247	***	-0.0991	
	(8.27)		(0.15)	
Ln (*Replag*)	0.7579	***	0.7036	***
	(52.75)		(27.46)	
BusyYrEnd	-0.2482	***	0.0320	
	(11.35)		(0.10)	
Industry Fixed Effects	Yes		Yes	
Pseudo R-Square	0.09		0.0613	
Likelihood Ratio Chi-Sq	2795.86	***	1927.60	***
Obs.	35,499		35,499	

This table presents the results of the difference in difference logistic regression to estimate the likelihood of dismissing and engaging Deloitte pre- and post the data breach. The dependent variables are in the first and second columns are *Dismissals* and *Engagements*. All specifications include industry fixed effects. Models are estimated with standard errors that are robust to heteroskedasticity and clustered by client (Petersen 2009). Chi-sq. statistics are presented in parentheses below the coefficients. *, **, and *** indicate significance at the 0.10, 0.05, and 0.01 levels, respectively (based on two-tailed tests). All variables are defined in Appendix 1. Bold denotes variables of interest.

Table 3: Audit Fees Paid by Deloitte Clients Pre and Post Data Breach

	(1) All Cients		(2) Continuing		(3) Initial	
Variables	Ln (*Audfees*)					
Intercept	1.7719	***	1.7761	***	1.7786	***
	(3.54)		(3.57)		(3.53)	
Post	0.1541	***	0.1533	***	0.1558	
	(10.72)		(10.65)		(1.00)	
Deloitte	-0.0445	***	-0.0449	***	-0.0073	
	(6.14)		(6.12)		(0.15)	
Post X Deloitte	**-0.0278**		**-0.0305**		**-0.1995**	***
	(0.96)		**(1.03)**		**(4.01)**	
Ln (*Assets*)	0.5497	***	0.5503	***	0.5062	***
	(272.43)		(269.91)		(31.53)	
Ret_Std	0.0066	***	0.0065	***	0.0138	
	(5.51)		(5.31)		(1.39)	
Ocf_Std	0.0196	**	0.0679	***	0.0085	
	(2.46)		(5.36)		(0.66)	
Revt_Std	0.0850	***	0.1039	***	0.0310	
	(9.30)		(10.40)		(0.77)	
Zmijewski_Z	0.0089	***	0.0102	***	0.0020	
	(5.88)		(6.45)		(0.17)	
Roa	-0.0479	***	-0.0441	***	-0.0472	
	(3.17)		(2.90)		(0.30)	
Leverage	0.0368	**	0.0262		0.1754	
	(2.32)		(1.62)		(1.49)	

Btm	-0.0089	***	-0.0071	***	-0.0845	***
	(3.47)		(2.76)		(3.72)	
Revgrowth	-0.0227	***	-0.0222	***	-0.0190	
	(5.05)		(4.82)		(0.81)	
Ocf	-0.2754	***	-0.2908	***	-0.2494	***
	(16.92)		(17.10)		(3.26)	
Ar_Invt	0.6821	***	0.6750	***	0.6994	***
	(29.29)		(28.62)		(4.28)	
Icw	0.3295	***	0.3174	***	0.5094	***
	(25.00)		(23.44)		(7.98)	
Restate	0.0821	***	0.0760	***	0.1874	***
	(7.98)		(7.23)		(3.42)	
Gc	0.1526	***	0.1588	***	-0.1329	
	(7.31)		(7.46)		(1.12)	
Ln (*Replag*)	0.4170	***	0.4155	***	0.4100	***
	(32.37)		(31.51)		(6.22)	
BusyYrEnd	0.0935	***	0.0925	***	0.1285	**
	(13.18)		(12.93)		(2.53)	
Industry Fixed Effects	Yes		Yes		Yes	
Adjusted R-Square	0.78		0.78		0.72	
F Value	2795.86	***	1190.13	***	23.41	***
Obs.	35,499		34,477		1,022	

This table presents the results of the OLS regression to estimate the audit fees paid by Deloitte clients pre- and post the data breach. The dependent variable is the natural logarithm of total audit fees. All specifications include industry fixed effects. Models are estimated with standard errors that are robust to heteroskedasticity and clustered by client (Petersen 2009). T-statistics are presented in parentheses below the coefficients. *, **, and *** indicate significance at the 0.10, 0.05, and 0.01 levels, respectively (based on two-tailed tests). All variables are defined in Appendix 1. Bold denotes variables of interest.

Table 4: Audit Fees Paid by Deloitte Clients Pre and Post Data Breach (Changes OLS Regression)

	(1) All Clients		(2) Continuing		(3) Initial	
Variables	*Chg_Audfees*					
Intercept	-1.4597	*	-1.3419	**	-1.3853	*
	(1.68)		(2.24)		(1.74)	
Post	0.0860	***	0.0879	***	0.3887	
	(3.34)		(4.92)		(0.68)	
Deloitte	-0.0158		-0.0013		-0.0265	
	(1.22)		(0.14)		(0.15)	
Post X Deloitte	**0.0177**		**-0.0029**		**-0.5091**	**
	(0.34)		**(0.08)**		**(2.17)**	
Chg_Ln_Assets	-0.3820	***	-0.3815	***	-0.3117	*
	(21.28)		(29.71)		(1.78)	
Chg_Ret_Std	-0.0002		0.0001	*	0.0008	
	(1.34)		(1.72)		(0.66)	
Chg_Ocf_Std	0.0625	***	-0.0013		5.9548	***
	(7.06)		(0.21)		(11.38)	
Chg_Revt_Std	0.0514	***	-0.0013		0.7907	***
	(10.04)		(0.38)		(3.75)	
Chg_Zmijewski_Z	0.0143	***	0.0047	***	0.1711	***
	(6.23)		(2.92)		(4.33)	
Chg_Roa	-0.1871	***	-0.0863	***	2.5012	***
	(7.35)		(4.87)		(4.32)	

Chg_Leverage	0.3917	**	-0.1214	***	4.0993	***
	(9.76)		(4.30)		(6.97)	
Chg_Btm	-0.0001	***	-0.0005	***	-0.1963	***
	(3.04)		(3.17)		(7.47)	
Chg_Revgrowth	-0.0002		-0.0001		-0.2024	***
	(0.65)		(0.49)		(3.88)	
Chg_Ocf	-0.0613	**	-0.0086		0.6048	
	(2.03)		(0.41)		(1.12)	
Chg_Ar_Invt	0.0963		0.3207	***	4.2422	***
	(0.89)		(4.20)		(3.04)	
Chg_Icw	0.7009	***	0.6854	***	1.1287	***
	(24.11)		(33.23)		(3.67)	
Chg_Restate	0.2062	***	0.1979	***	0.2132	***
	(8.07)		(10.95)		(0.75)	
Chg_Gc	0.0369		-0.0195		-0.4203	
	(1.01)		(0.76)		(0.94)	
Chg_Ln_Replag	-0.8749	***	-0.8718	***	-1.0977	***
	(43.36)		(60.93)		(5.15)	
Industry Fixed Effects	Yes		Yes		Yes	
Adjusted R-Square	0.13		0.21		0.76	
F Value	48.18	***	83.33	***	28.07	***
Obs.	35,499		34,477		1,022	

This table presents the results of the OLS regression to estimate changes in audit fees paid by Deloitte clients pre- and post the data breach. The dependent variable is the change in total audit fees from year *t-1* to year *t*. All specifications include industry fixed effects. Models are estimated with standard errors that are robust to heteroskedasticity and clustered by client (Petersen 2009). T-statistics are presented in parentheses below the coefficients. *, **, and *** indicate significance at the 0.10, 0.05, and 0.01 levels, respectively (based on two-tailed tests). All variables are defined in Appendix 1. Bold denotes variables of interest.

Table 5: Market Reaction to the Disclosure of the Data Breach – Summary Statistics

Panel A: Univariate Analysis of Market Reaction

Deloitte Clients			Non- Deloitte Clients				
Days	Obs.	Cumulative Abnormal Returns	Days	Obs.	Cumulative Abnormal Returns	t-value	
(-150,+30)	418	-4.26%	(-150,+30)	1,545	0.20%	13.88	***

Panel B: Market Reaction to the Disclosure of the Data Breach – Summary Statistics

	N	Mean	Median	Lower Quartile	Upper Quartile	Std Dev
Cumulative Abnormal Returns (-150, +30)	1,963	-0.0107	-0.0409	-0.2304	0.1550	0.4820
Cumulative Abnormal Returns (-3, +3)	1,963	0.0188	0.0160	-0.0135	0.0450	0.0692
Deloitte	1,963	0.2129	0.0000	0.0000	0.0000	0.4095
Mkvl	1,963	12,211.31	2,120.13	658.76	7258.07	43,626.67
Btm	1,963	0.1807	0.3067	0.1546	0.5310	7.4399
Momentum	1,963	0.2539	0.1278	-0.1058	0.3841	1.0034

Table 6: Market Reaction to the Disclosure of the Data Breach

Variables	*Cumulative Abnormal Returns* (*-150, +30*)		*Cumulative Abnormal Returns* (*-3, +3*)	
Intercept	-0.1166	**	0.0628	***
	(2.12)		(6.81)	
Deloitte	**-0.0412**	*	**-0.0009**	**
	(1.71)		**(2.27)**	
Ln (*Mkvl*)	0.0065		-0.0059	***
	(0.99)		(5.59)	
Btm	-0.0005		0.0003	***
	(1.28)		(7.32)	
Momentum	0.1777	***	0.0074	*
	(3.07)		(1.96)	
Industry Fixed Effects	Yes		Yes	
Adjusted R-Square	0.145		0.036	
F Value	7.46	***	17.98	***
Obs.	1,963		1,963	

This table presents the results of the OLS regression to examine market reaction to the announcement of the breach. The dependent variable is the cumulative abnormal returns around the day of the disclosure of the breach calculated using market model with a value-weighted index. All specifications include industry fixed effects. Models are estimated with standard errors that are robust to heteroskedasticity and clustered by client (Petersen 2009). T-statistics are presented in parentheses below the coefficients. *, **, and *** indicate significance at the 0.10, 0.05, and 0.01 levels, respectively (based on two-tailed tests). All variables are defined in Appendix 1. Bold denotes variables of interest.

Table 7: Market Reaction to the Dismissal and Engagement of Deloitte Pre and Post Data Breach – Summary Statistics

	N	Mean	Median	Lower Quartile	Upper Quartile	Std. Dev
Cumulative Abnormal Returns (*-1, +1*)	1,884	-0.0009	-0.0014	-0.0253	0.0225	0.0637
Cumulative Abnormal Returns (*-3, +3*)	1,884	-0.0049	-0.0047	-0.0426	0.0316	0.0926
Post	1,884	0.0435	0.0000	0.0000	0.0000	0.2039
Dismissals_Deloitte	1,884	0.1298	0.0000	0.0000	0.0000	0.3362
Engagements_Deloitte	1,884	0.1953	0.0000	0.0000	0.0000	0.3965
Mkvl	1,884	4,076.44	461.27	130.07	1,909.59	14,816.64
Btm	1,884	0.4376	0.5126	0.2894	0.8459	14.5903
Momentum	1,884	0.1681	-0.0294	-0.3016	0.2814	1.1821

Table 8: Market Reaction to the Dismissal and Engagement of Deloitte Pre and Post Data Breach

	(1)		(2)		(3)		(4)	
Variables	*Cumulative Abnormal Returns (-1, +1)*				*Cumulative Abnormal Returns (-3, +3)*			
Intercept	0.0019	**	-0.0063	**	-0.0191	**	-0.0182	**
	(2.38)		(2.12)		(2.40)		(2.32)	
Post	-0.0038		-0.0037		0.0059		0.0032	
	(0.63)		(0.50)		(0.62)		(0.27)	
Dismissals_Deloitte	-0.0031				-0.0060			
	0.71				(0.92)			
Post X Dismissals_Deloitte	**0.0146**	*			**0.0034**	**		
	(1.95)				**(2.12)**			
Engagements_Deloitte			-0.0048				-0.0074	
			(1.22)				(1.14)	
Post X Engagements_Deloitte			**-0.0139**	**			**-0.0125**	*
			(1.99)				**(1.71)**	
Ln (*Mkvl*)	-0.0004		0.0009		0.0022	**	0.0021	**
	(0.58)		(1.18)		(2.04)		(2.00)	
Btm	0.0001		0.0001		0.0009	***	0.0009	***
	(0.51)		(0.63)		(34.17)		(33.87)	
Momentum	0.0024	**	0.0035	***	0.0059	***	0.0057	***
	(2.44)		(2.82)		(2.99)		(2.92)	
Industry Fixed Effects	Yes		Yes		Yes		Yes	
Adjusted R-Square	0.006		0.006		0.031		0.031	
F Value	2.34	**	2.19	**	245.48	***	238.79	***
Obs.	1,755		1,755		1,755		1,755	

This table presents the results of the OLS regression to examine market reaction to the announcement of 8-K disclosure of the dismissal and engagement of Deloitte. The dependent variable is the cumulative abnormal return around the date of the 8-K disclosure using market model with a value-weighted index. All specifications include industry fixed effects. Models are estimated with standard errors that are robust to heteroskedasticity and clustered by client (Petersen 2009). T-statistics are presented in parentheses below the coefficients. *, **, and *** indicate significance at the 0.10, 0.05, and 0.01 levels, respectively (based on two-tailed tests). All variables are defined in Appendix 1. Bold denotes variables of interest.