

Extended Abstract
for the FTC PrivacyCon 2018

**Soft Disclosure of Data Breach:
A Close Look at the SEC Financial Filings**

Preliminary, please do not cite or quote without author permission

Ginger Zhe Jin
University of Maryland & NBER
Department of Economics

Yi Cao
Ph.D. Candidate
University of Maryland
Robert H. Smith School of Business
Department of Accounting and Information Assurance

November 6, 2017

This study examines how public firms disclose media-reported data breach in their SEC filings (10-K and 10-Q).

Given widespread data breach¹, policymakers have attempted to address it in many ways. On October 13, 2011, the US Securities and Exchange Commission (SEC) issued a guidance that requires public firms disclose material information regarding cybersecurity risks and cyber incidents (SEC 2011). However, the SEC does not define “material information”, does not track how many companies comply with the guidance, and has yet to bring a case under this particular guidance. Ironically, SEC itself was hacked in 2016 and did not disclose the event to the public until September 20, 2017, casting doubt on its own guidance of data breach disclosure.² More broadly, Congress has introduced multiple bills to standardize data breach notification³, but no federal law has passed so far, leaving the issue to local and sector-specific laws.⁴

The fuzzy policy landscape is partly driven by the fact that we have not fully understood firm behavior in data security. Policy makers often believe that firms intentionally hide data breaches because they want to mislead consumers and investors. Following this logic, the stock market should punish firms for publicized data breach, and

¹ According to Privacy Rights Clearinghouse, 7,684 data breaches have been made public since 2005, exposing 1.07 billion records of personal identifiable information (PII) to potential abuse. Source: <https://www.privacyrights.org/data-breaches>, accessed on September 19, 2017.

² With few details, the SEC claims that it has reported the breach to related government agency in 2016, and “the intrusion did not result in unauthorized access to personally identifiable information, jeopardize the operations of the Commission, or result in systemic risk.”(SEC 2017)

³ In 2012, Senator Jay Rockefeller advocated for a cybersecurity legislation that strengthens the requirement to report cybercrimes. In January 2014, the Senate Commerce, Science and Transportation Committee (led by Senator Rockefeller) introduced a bill to create a federal requirement for data breach notification (S. 1976 Data Security and Breach Notification Act of 2014). In his 2015 State of the Union Speech, President Obama proposed new legislation to create a national data breach standard with a 30-day notification requirement for data breach. A related bill was later introduced by the US House of Representatives (H.R. 1770L Data Security and Breach Notification Act of 2015).

⁴ The Gramm-Leach-Bliley Act requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. The Health Insurance Portability and Accountability Act (HIPPA) requires health care institutions to provide data privacy and security provisions for safeguarding medical information.

a mandate for data breach disclosure will motivate firms to adopt tougher data security measures to avoid future breach. However, the stock market penalty is found to be small and temporary, if negative at all (Acquisti et al. 2016). Firms also argue that they are victims themselves, and providing too many details too soon could tip criminals and harm police investigation. It is difficult to evaluate these arguments until we know how firms handle the disclosure after data breach.

In this study, we investigate how public firms disclose media-reported data breach in their SEC filings (10-K and 10-Q). We combine textual analysis with the standard differences-in-differences approach (DID), using a panel data set of breached and non-breached firms. Contrary to the common criticism, preliminary results suggest that firms do not completely hide the bad news of data breach. Rather, they engage in “soft” disclosure, where they use weaker tones, more negative words, and more litigious jargons in the SEC filing as early as one quarter after the media report of data breach, but most of them do not disclose details of the specific data breach event. We believe these findings have significant implications for data breach notification policies.

References:

Acquisti, Alessandro; Curtis Taylor and Liad Wagman (2016) “The Economics of Privacy”, *Journal of Economic Literature*, 54(2): 442-92.

SEC (2011): *CF Disclosure Guidance, Topic No. 2: Cybersecurity* (Oct. 13,

2011), accessed at www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

SEC (2017): *SEC Statement on Cybersecurity* by the SEC Chairman Jay Clayton,

September 20, 2017, accessed at [https://www.sec.gov/news/public-](https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20)

[statement/statement-clayton-2017-09-20](https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20)