Analysis of the Impact of the 2019 Capital One Data Breach on Stock Prices

Introduction

On July 29, 2019, Capital One announced a significant data breach, which affected over 100 million customers. This event potentially impacted the company's stock price, as well as investor confidence. In this report, I analyze the impact of the data breach on Capital One's stock returns using a Difference-in-Differences (DiD) methodology. I compared the performance of Capital One's stock (COF) to a control group of other financial institutions as well as the S&P 500 (SPY) index.

Data Collection

Daily stock price data for Capital One and the control group was collected from January 1, 2019, to August 19, 2019, using the Yahoo Finance API. The data was then processed to calculate daily returns and prepare it for analysis.

Methodology

Difference-in-Differences (DiD) Model

The Difference-in-Differences model estimates the impact of the data breach by comparing the changes in stock returns of Capital One before and after the event, relative to the control group. The model is specified as:

$$returns = \alpha + \beta_1 treated + \beta_2 treated + \beta_3 (treated \times post) + \epsilon$$

Where:

- '$returns$' is the daily stock return.
- '$treated$' is a binary variable indicating whether the stock is Capital One (1 if COF, 0 otherwise).
- '$post$' is a binary variable indicating whether the observation is after the data breach announcement (1 if after July 30, 2019, 0 otherwise).
- '$treated \times post$' is the interaction term indicating the combined effect of being a treated stock post-event.

Difference-in-Trends (DiT) Model

The Difference-in-Trends model validates the assumption that there were no significant differences in trends between the treated and control groups before the event. The model is specified as:

$$returns = \alpha + \beta_1 treated + \beta_2 treated + \beta_3 (treated \times trend) + \epsilon$$

Where:

- '$trend$' is the number of days before the event.

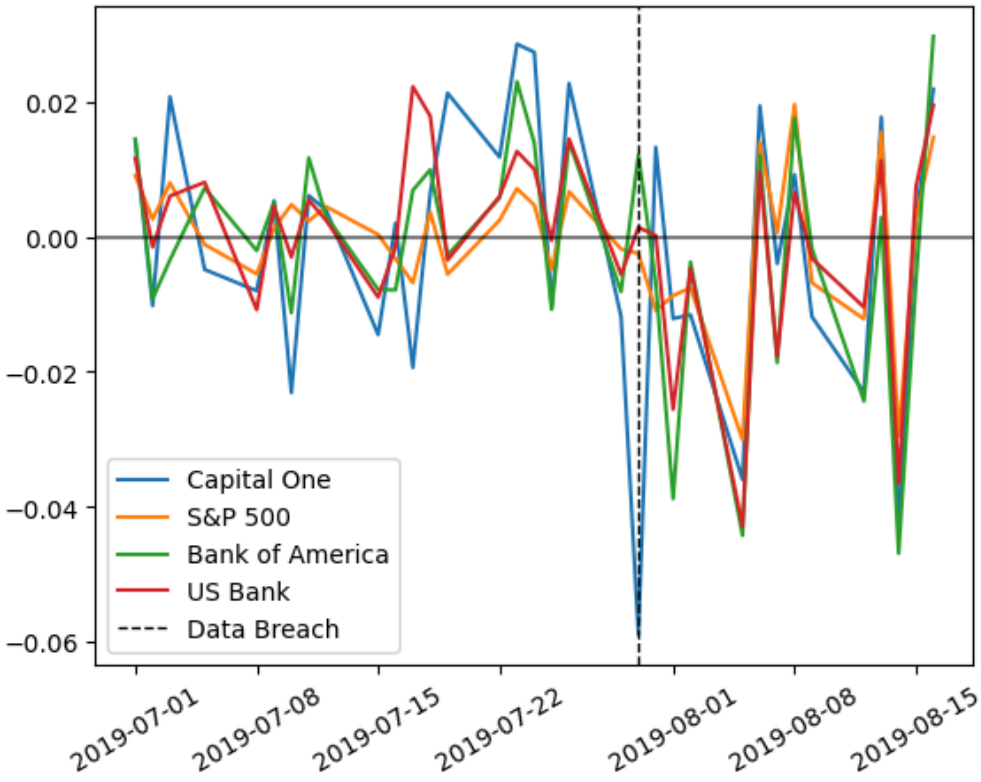
Results

Difference-in-Differences Model

The DiD model produced the following results:

- **Intercept:** 0.0009 (p = 0.028)
- **treated:** 0.0008 (p = 0.450)
- **post:** 0.0010 (p = 0.823)
- **treated_post:** -0.0616 (p = 0.000)

The key coefficient of interest, $treated\_post$, is -0.0616 and statistically significant ($p < 0.05$). This suggests that the data breach announcement resulted in an approximate 6.16% drop in Capital One's stock returns. Visualized below are the stock prices one month before and two weeks after where it can clearly be seen, Capital One's significant drop while both US Bank and Bank of America maintained positive returns.



Validation of Assumptions

No Pre-Event Trend Difference

The Difference-in-Trends model validated the assumption that there were no significant differences in trends between the treated and control groups before the event:

- **treated:** 0.0007 (p = 0.763)
- **trend:** -9.187e-06 (p = 0.219)
- **treated_trend:** 1.731e-06 (p = 0.935)

The $treated\_trend$ coefficient is very close to zero and not statistically significant, indicating no significant pre-event trend differences.

No Bias in the Model

To further validate the model, I performed placebo tests by running the DiD model on pre-event dates and comparing the distribution of the $treated\_post$ coefficients:

- Mean beta: 0.000692
- Mean p-value: 0.646151
- Share of p-values < 0.5: 27.71%

The placebo tests showed that the $treated\_post$ coefficients were centered around zero and not statistically significant, suggesting that the model is not biased.

Conclusion

The analysis indicates that the July 29, 2019, Capital One data breach had a significant negative impact on the company's stock returns, causing an approximate 6.16% drop. The model assumptions were validated through Difference-in-Trends and placebo tests, ensuring the robustness of the results. A repeat offense of such a breach would likely have a larger impact on the company, further damaging the brand and labeling Capital One as a security risk. Given this, it is highly recommended that the company invest into higher levels of privacy and security, as well as additional assurances for current and future potential customers.