What Works?:

Quasi-experiments in Cybersecurity Policy Interventions

Karl Grindal, PhD Candidate

June 3, 2021

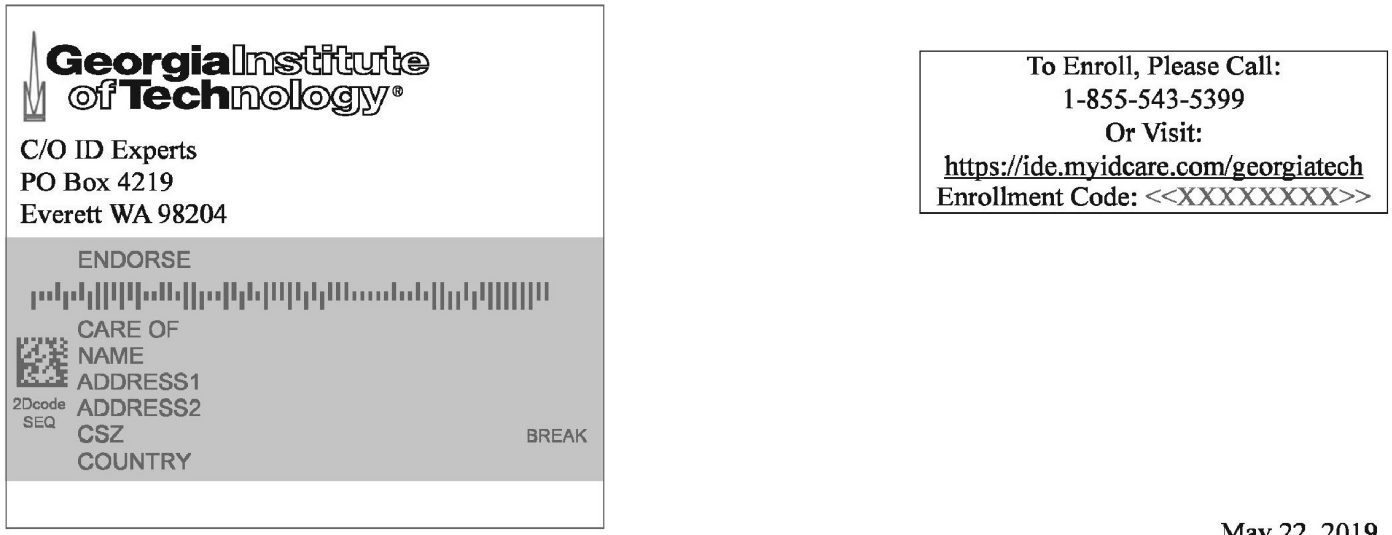
Georgia Institute of Technology

Introduction

1. Introduction
2. Data Collection
3. Methodology
4. Findings
    - Minor Findings
    - Major Findings
5. Implications

Introduction

What is a breach notification letter?



Georgia Institute of Technology®

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE
CARE OF
NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY
2Dcode SEQ
BREAK

To Enroll, Please Call:
1-855-543-5399
Or Visit:
https://ide.myidcare.com/georgiatech
Enrollment Code: <<XXXXXXXX>>

May 22, 2019

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>,

The Georgia Institute of Technology ("Georgia Tech") is committed to protecting personal information. We are writing to provide an update on the security incident that we disclosed on April 2, 2019. This notice explains the incident, measures we have taken, and some steps you can take in response.

What Happened?
In late March 2019, Georgia Tech identified signs that an unauthorized person had found a way to send queries through a Georgia Tech web server to an internal database. Georgia Tech immediately implemented its incident response protocol, took steps to secure the web server, and began an investigation to determine what records in the database were accessed. The U.S. Department of Education was notified, and Georgia Tech set up a dedicated website on April 2, 2019 that shared its preliminary findings.

What Information Was Involved?
Leading forensic firms were engaged to assist in the investigation and help determine the specific information that was accessed. The investigation determined that access to the database may have occurred between December 14, 2018 and March 22, 2019. The information about you in the database that may have been accessed includes your name, address,

Policy Literature

Policy Evaluation

- Romanosky et al. (2011) connected data breach notification laws to a 2% reduction in identity theft. [5]
- Kesari (2020) noted that updates in 2016 to California data breach notification suggest ".1 fewer reports per 100,000 people" for reported medical identity theft. [3]
- Liu (2020) found that state anti-phishing or credit freeze legislation did not impact annual identity theft reports. [4]

The economics of information security is more fully developed, with the annual World Economics of Information Security (WEIS) conference serving as a focal point.

Motivation

One promising technique for the evaluation of some cyber-security programs is the use of natural and quasi-natural experiments.

Using a difference-in-differences methodology, one could conduct a quasi-natural experiment to determine the impact of mandatory data breach notification laws and regulations in the United States.

-Benjamin Dean, 2016 [1]

Research Question and Hypothesis

Research Question: Have regulatory cyber policy interventions effectively reduced the frequency of data breach incidents *ceteris paribus*?

Research Question and Hypothesis

Research Question: Have regulatory cyber policy interventions reduced the frequency of data breach incidents *ceteris paribus*?

- **Hypothesis 1:** The NY Department of Financial Services cybersecurity regulations reduced the frequency of reported data breaches in the New York financial sector.

Research Question and Hypothesis

Research Question: Have regulatory cyber policy interventions reduced the frequency of data breach incidents *ceteris paribus*?

- **Hypothesis 1:** The NY Department of Financial Services cybersecurity regulations reduced the frequency of reported data breaches in the New York financial sector.
- **Hypothesis 2:** The Massachusetts Data Security Law reduced the frequency of reported data breaches in Massachusetts.

Research Question and Hypothesis

Research Question: Have regulatory cyber policy interventions reduced the frequency of data breach incidents *ceteris paribus*?

- **Hypothesis 1:** The NY Department of Financial Services cybersecurity regulations reduced the frequency of reported data breaches in the New York financial sector.
- **Hypothesis 2:** The Massachusetts Data Security Law reduced the frequency of reported data breaches in Massachusetts.
- **Hypothesis 3:** The HITECH Act reduced the frequency of reported data breaches in the healthcare sector.

Research Question and Hypothesis

Research Question: Have regulatory cyber policy interventions reduced the frequency of data breach incidents *ceteris paribus*?

- **Hypothesis 1:** The NY Department of Financial Services cybersecurity regulations reduced the frequency of reported data breaches in the New York financial sector.
- **Hypothesis 2:** The Massachusetts Data Security Law reduced the frequency of reported data breaches in Massachusetts.
- **Hypothesis 3:** The HITECH Act reduced the frequency of reported data breaches in the healthcare sector.
- **Hypothesis 4:** The expansion of FTC Section 5 enforcement authority with the Wyndham Hotels suit reduced the frequency of reported data breaches nationally.

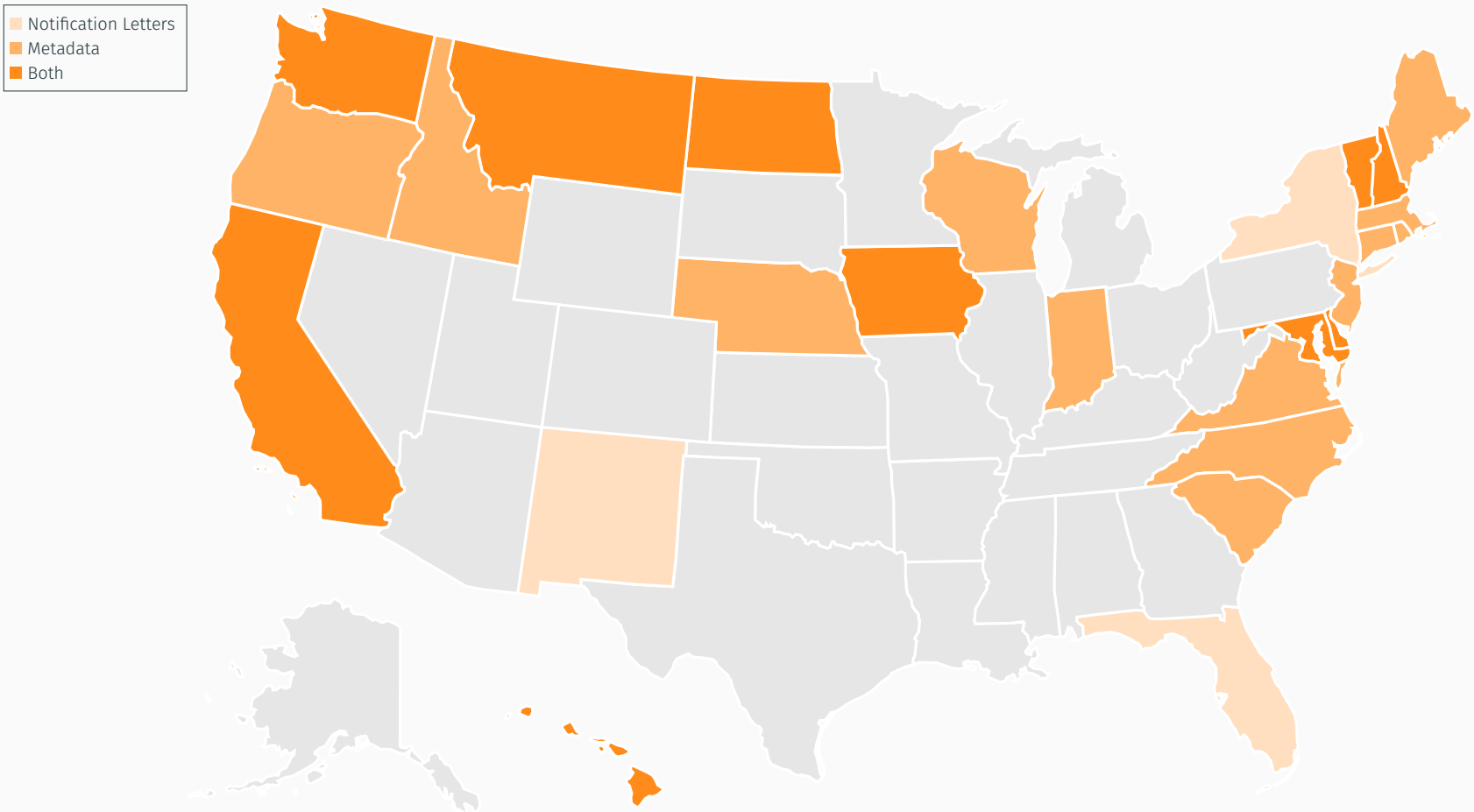
Case Selection

	State Level	National Level
Industry Wide Regulations	NY DFS cybersecurity regulation (March 1, 2017)	HITECH Act, part of the ARRA (February 17, 2009)
Economy Wide Regulations	Massachusetts Data Security Standard - 201 C.M.R. 17 (March 1, 2010)	FTC Section 5: Unfair or Deceptive Acts or Practices (Enforcement 2005-2020)

Data Collection

States with Breach Data Available

Figure 1: States with Collected Data Breach Notification Information



State Data - Percent of Collection for each Year

State	’05	’06	’07	’08	’09	’10	’11	’12	’13	’14	’15	’16	’17	’18	’19	’20
North Carolina	85	100	100	100	100	100	100	100	100	100	100	100	100	90		
New Hampshire		53	100	100	100	100	100	100	100	100	100	100	100	100	100	83
Hawaii			47	100	100	100	100	100	100	100	100	100	100	100	100	30
Massachusetts			46	100	100	100	100	100	100	100	100	100	100	100	100	69
South Carolina				43	100	100	100	100	100	100	100	100	100	100	48	
Maine				42	100	100	100	100	100	100	100	100	100	100	100	70
Iowa							80	100	100	100	100	100	100	100	100	67
California								95	100	100	100	100	100	100	100	70
Wisconsin								69	100	100	100	100	100	100	100	54
Connecticut								25	100	100	100	100	100	100	77	
Virginia									99	100	100	100	100	91		
Indiana									72	100	100	100	100	100	100	67
Maryland											99	100	100	100	100	50
Montana											65	100	100	100	100	69
Washington											39	100	100	100	100	70
Oregon											17	100	100	100	100	71
Rhode Island												24	100	100	100	73
Vermont													87	100	100	63
New Jersey													58	100	42	
Delaware														72	100	66
North Dakota															99	71

Descriptive Statistics for Collected

Descriptive Statistics of Captured Incidents

Statistics	Measure
Number of captured incidents	54,340
Incidents dropped for No Reported Date	559
Incidents dropped for Amended Submission	45
Incidents dropped for Unclear Org Name	14
Incidents remaining after drops	53,722
Breaches after incident matching	19,592

Comparable Datasets

Datasets Used in Academic Research

Dataset	Public	Collection Years	Comprehensive	Incidents	State
Advisen Ltd	N	’90-’19	N	150,000 [1]	N/A
Dataloss DB	Y	’05-’15	N	1,078	N
Hackmageddon	Y	’11-’20	N	613[2]	N
HHS Breaches	Y	’09-’20	Y	3,654[3]	Y
Privacy Rights Clearinghouse	Y	’05-’19	N	9,015[3]	Y
SAS® OpRisk Global Data	N	’95-’14	N	26,541	N/A
Veris Community	Y	’98-’20	N	7,833[3]	Y/N

New Breach Data

Dataset	Public	Collection Years	Comprehensive	Incidents	State
My State Breach Data	Y	’05-’20	Y	19,592	Y

[1] Hogan et al. (2020) [2]
[2] Werner et al (2017) used 10 months in 2016 [7]
[3] Updated December 12, 2020

Methodology

Diagram of Factor Relationships

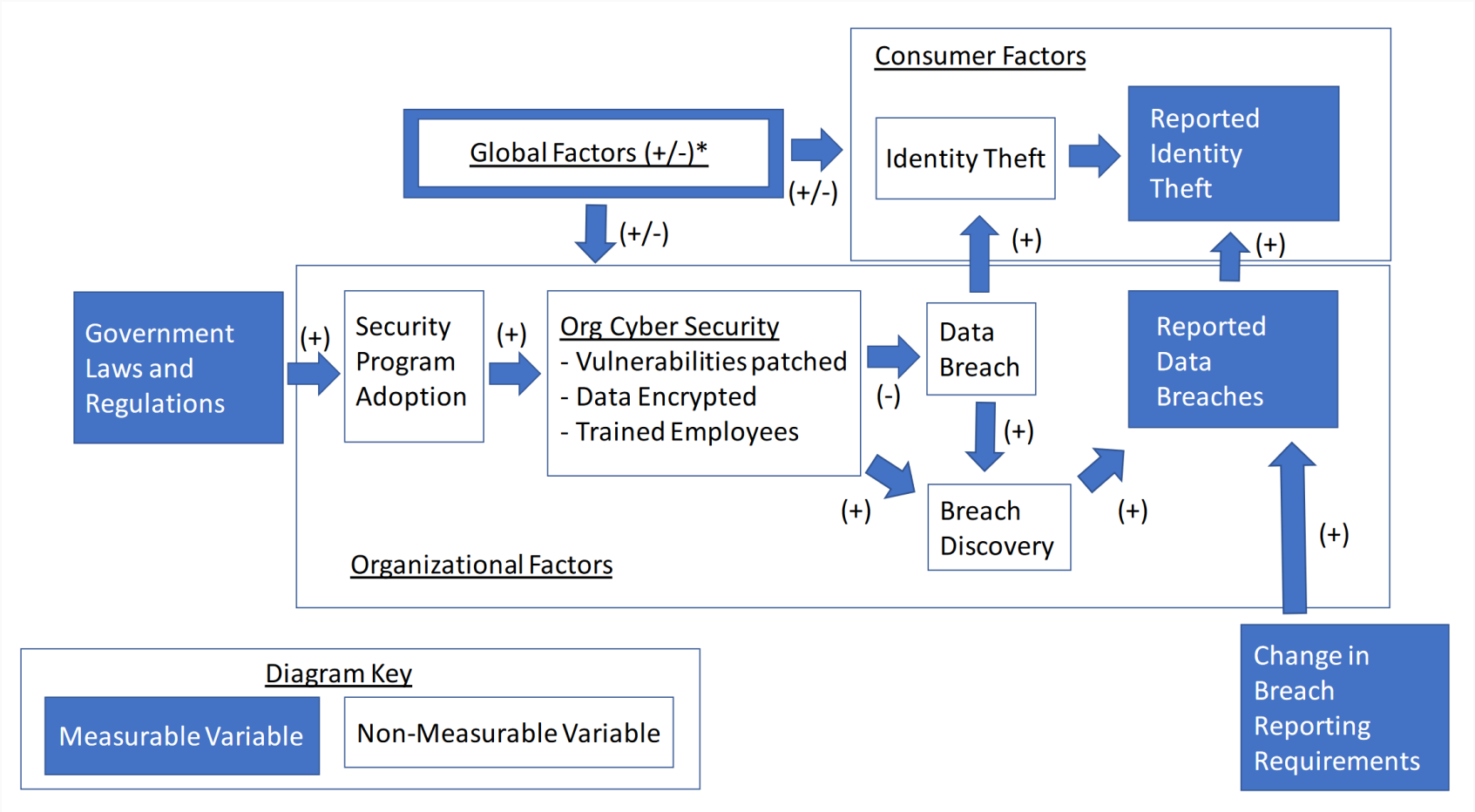


Figure 2: * includes Cyber Hygine, Government Capability, Vulnerabilities, etc.

Regulatory Enforcement

Table 1: First Regulatory Enforcement

State Law	Massachusetts Data Security Law	HITECH Act	NY DFS cyber regulations
First Enforcement	Briar Group	Blue Cross Blue Shield of Tennessee	Residential Mortgage Inc.
Scope of Incident	Hack lasted 8 months, took credit card data.	Theft of hard drives over 1 million individuals affected	Phishing attack accessed mailing list (unreported)
Penalty	$110,000	$1,500,000	$1,500,000
Days Since Regulation Has Been Enforced	372 days	1,017 days	1,112 days

Quasi-Experimental Research

Experimental Research

- The “gold-standard” of research is randomized controlled trials
- Random assignment helps to achieve identical treatment and control groups
- Can be costly to implement and is sometimes unethical

Quasi-Experimental Research

- An empirical interventional study with non-random assignment
- Allows for observational data to be used
- Statistical methodologies like interrupted time series and propensity matching can address some of the challenges associated with using nonequivalent groups

Quasi-Experimental Research

Interrupted Time Series (ITS)

- Analysis of time series data (i.e., an outcome measured over time)
- Comparison of the outcome before and after an intervention
- This method is particularly useful for assessing the impact of changes in policy

Group	Pre-Test	Treatment	Post-Test
Experimental Group	$O_1\ O_2\ O_3\ O_4\ O_5\ O_6$	X	$O_7\ O_8\ O_9\ O_{10}\ O_{11}\ O_{12}$

Quasi-Experimental Research

Comparative Design ITS

- Improves on ITS by comparing with a control series (i.e., no intervention)
- Comparative Design ITS has additional pre- and post-treatment measurements
- These additional measurements allow for segmented regression and comparison of changes in both level and slope

Group	Pre-Test	Treatment	Post-Test
Experimental Group	$O_1\ O_2\ O_3\ O_4\ O_5\ O_6$	X	$O_7\ O_8\ O_9\ O_{10}\ O_{11}\ O_{12}$
Control Group	$O_{13}\ O_{14}\ O_{15}\ O_{16}\ O_{17}\ O_{18}$		$O_{19}\ O_{20}\ O_{21}\ O_{22}\ O_{23}\ O_{24}$

Findings

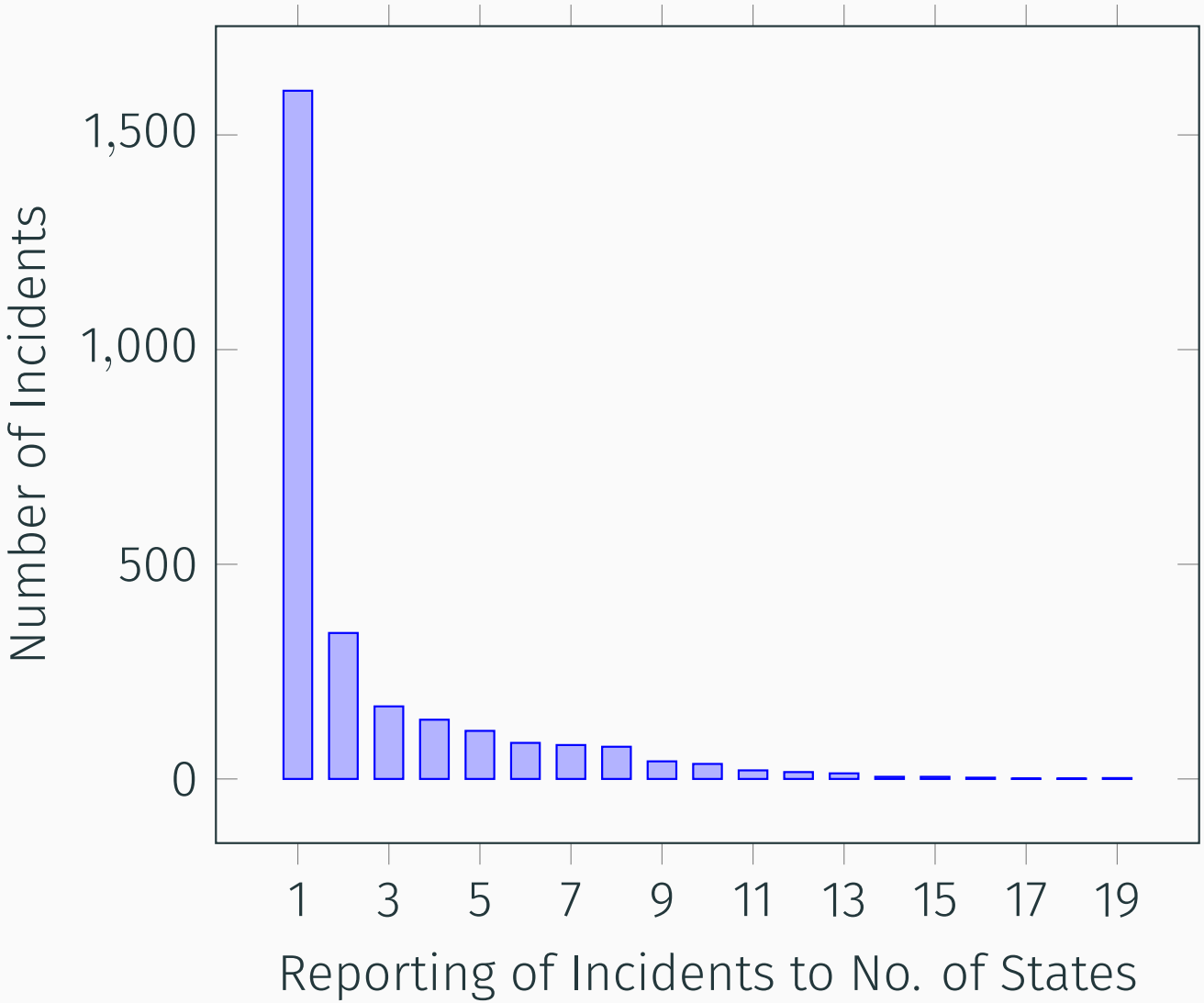
Overview of Minor Findings

Minor Findings

- The majority of reported incidents were localized in their effect.
- The number of individuals affected by a breach has an exponential distribution.
- There is a similar number of breaches per capita in states with similar reporting requirements.
- Across all states, there is a slow but persistent rate of growth in breach incidents at approximately 20% per year.
- The consistent seasonal variation observed in data breach reporting increased in the Spring and decreased in the Fall.

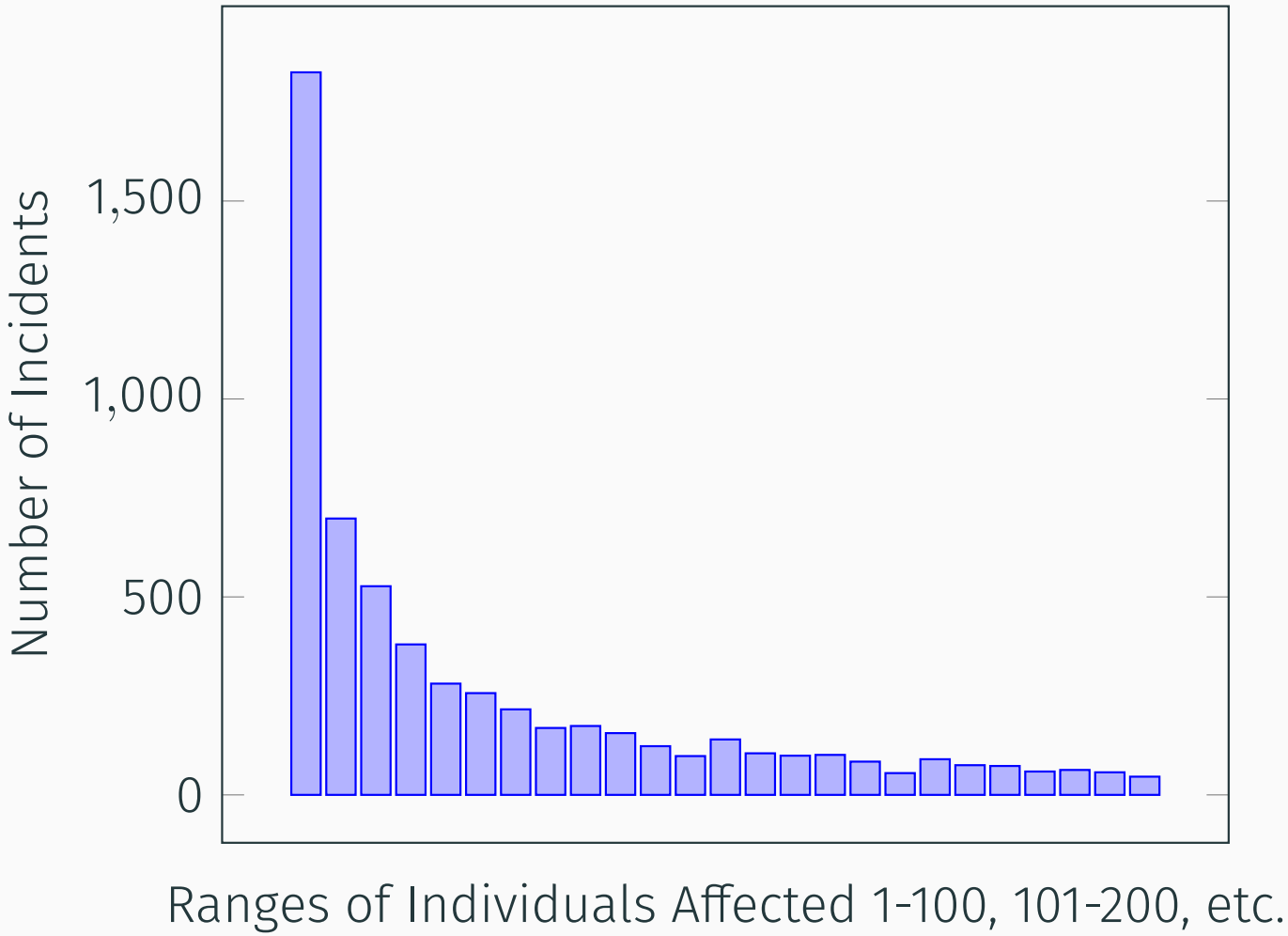
Number of Incidents Reported Across Different States

Figure 3: Number of Incidents Reported Across Different States



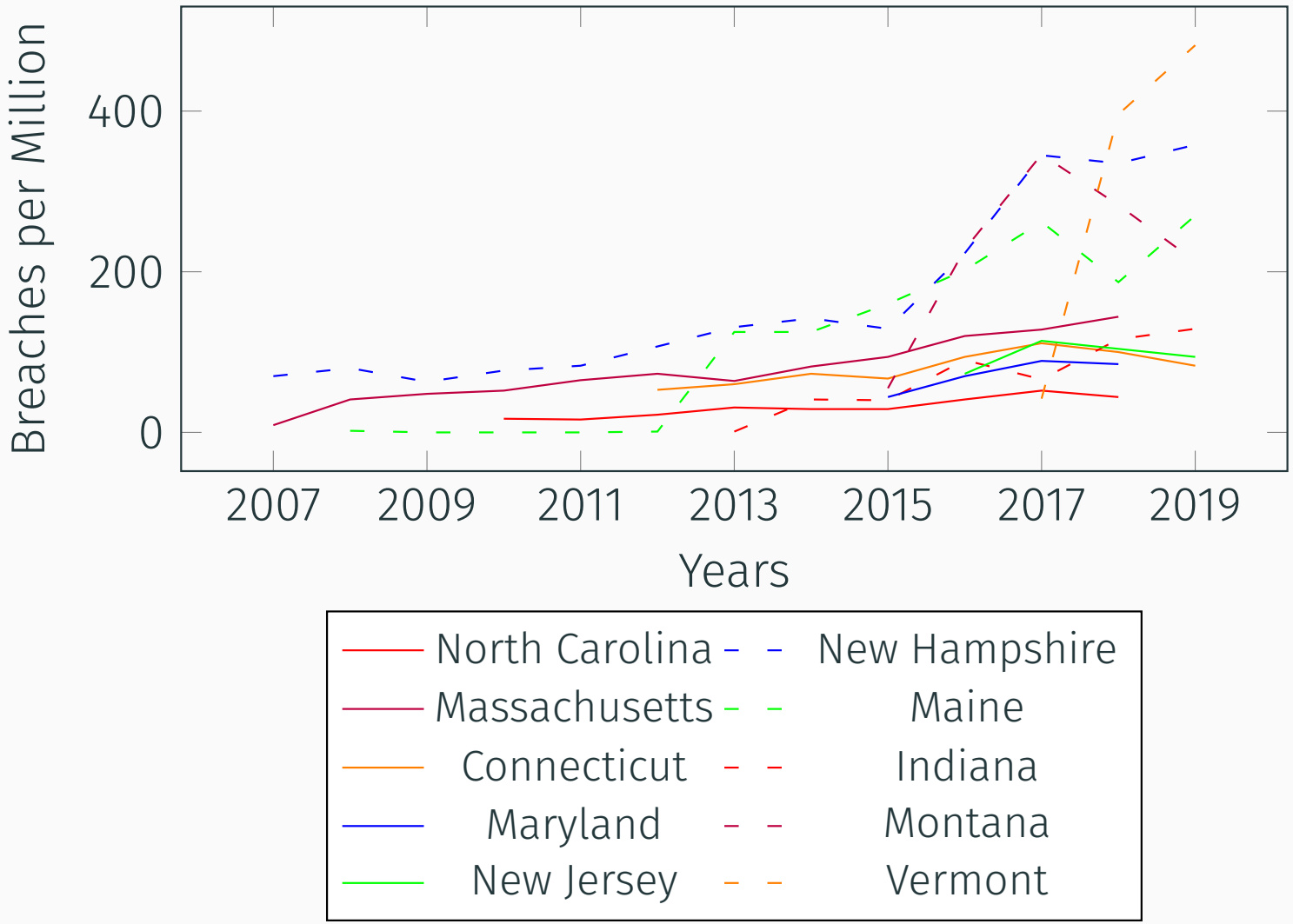
Total Individuals Affected By Breaches

Figure 4: Histogram of Total Individuals Affected



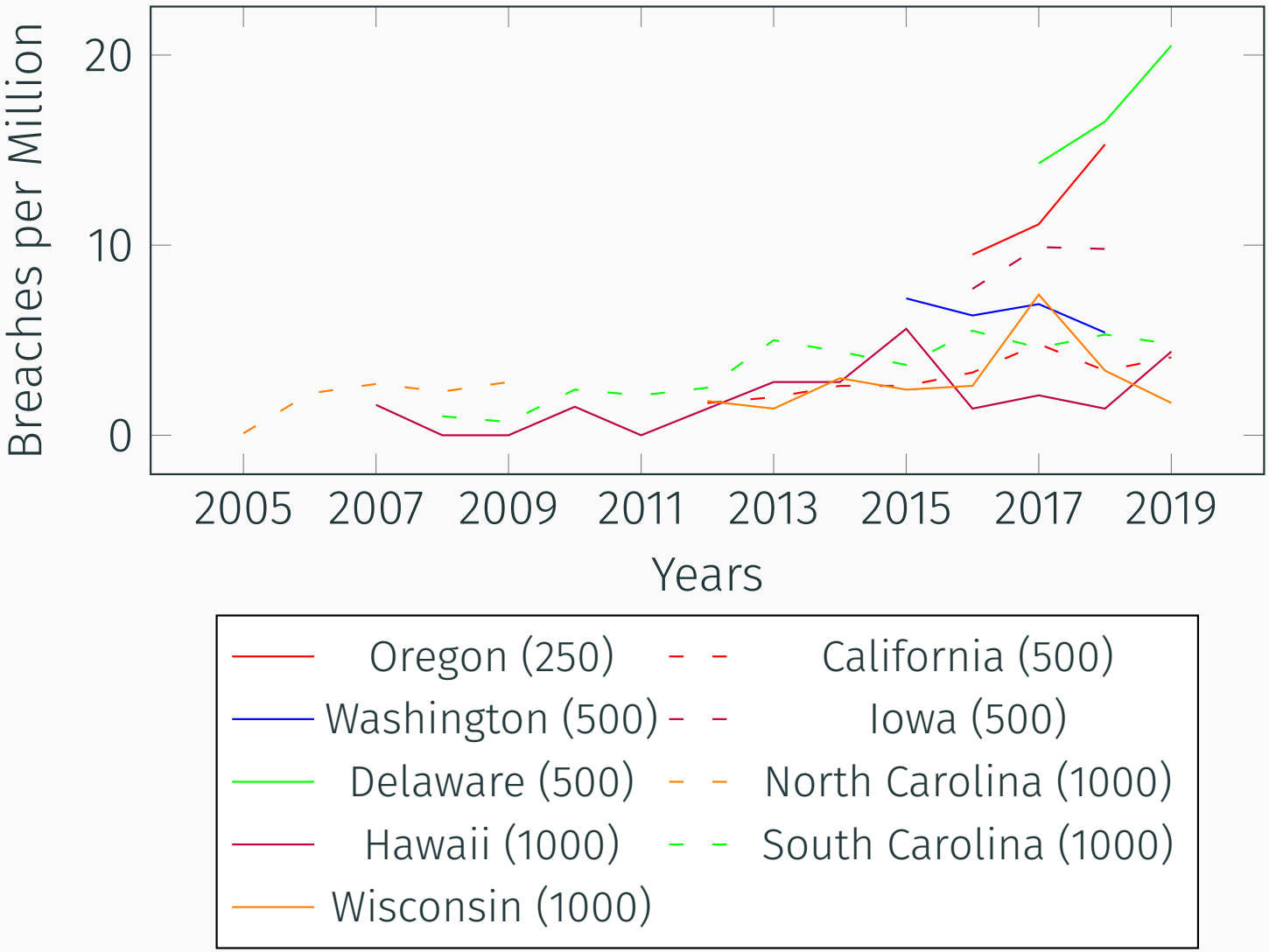
Breaches per Million

Figure 5: Reported Breaches each Year per Million with No Resident Limits



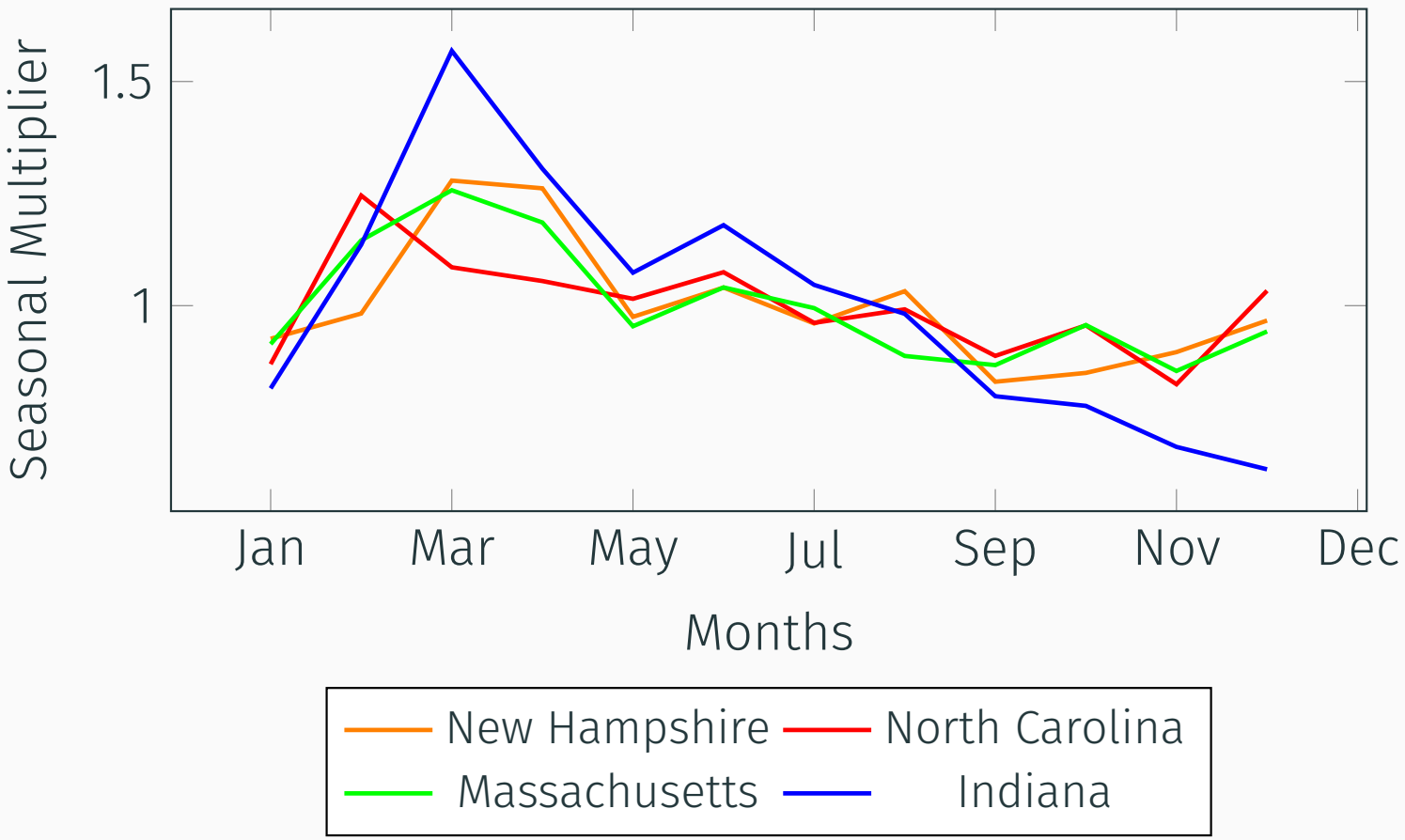
Breaches per Million

Figure 6: Reported Breaches each Year per Million with Resident Limits



Evidence for Seasonal Trends

Figure 7: Seasonal Variation in Breaches per Million



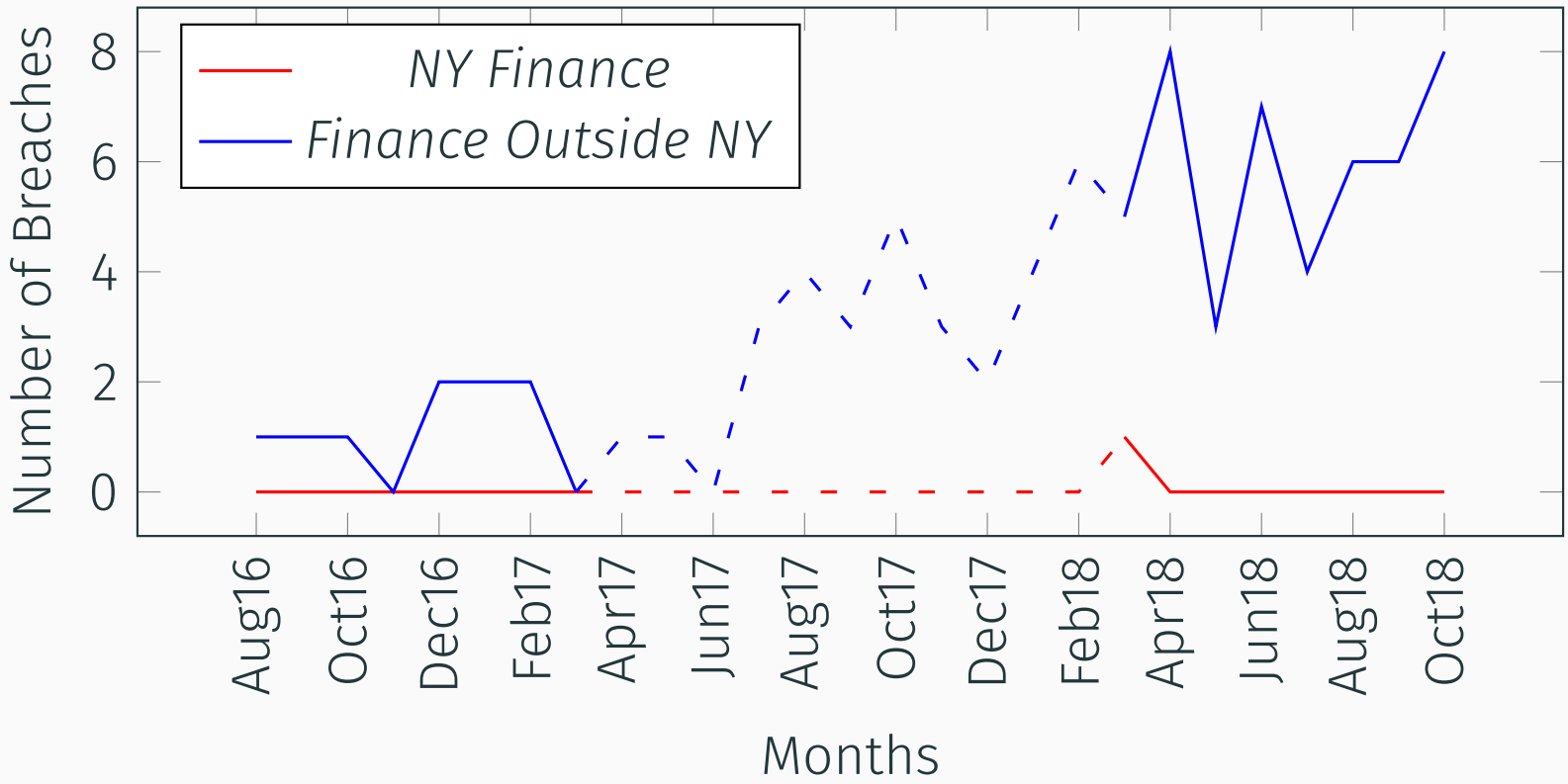
Overview of Major Findings

Major Findings

- The New York Department of Financial Services regulations was shown to be effective. The intervention lead to a reduction in 27 financial sector breaches in New York over the course of a year.
- In contrast, the Massachusetts Data Security Law, the HITECH Act, and FTC's Wyndham's Actions did not demonstrate a reduction in reported data breaches.

Comparing New York Finance to Not-New York Finance with Maine Data

Figure 8: Comparing New York Finance to Not-New York Finance with Maine Data

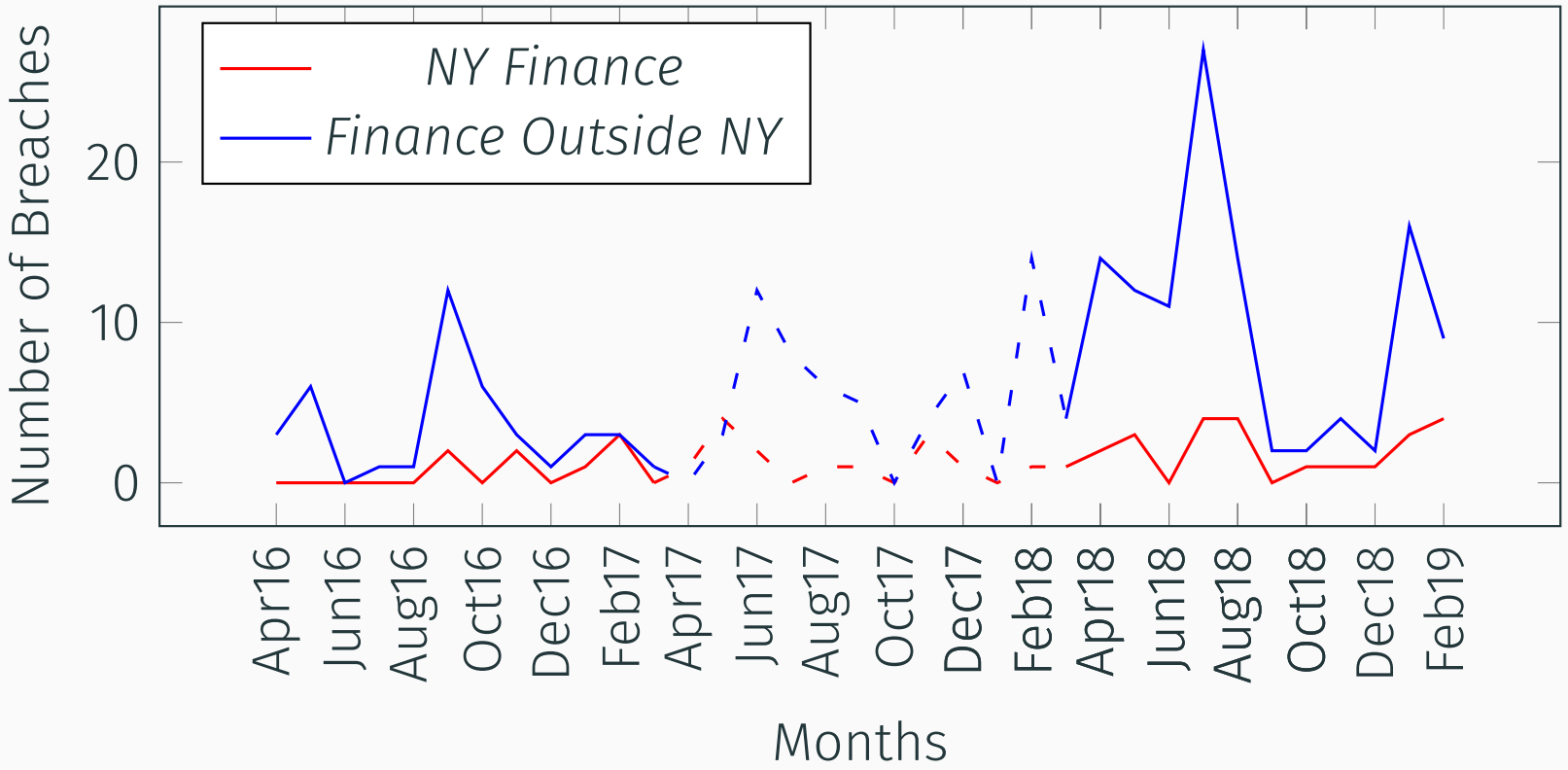


Comparative ITS NY DFS Regulations (NY Finance Compared to Non-NY Finance with Maine Data)

Parameter	Interpretation	Estimate	Std Error	Probability
α	Intercept	1.11	0.81	0.18
β_1	Control Pre-Trend	-0.02	0.16	0.88
β_2	Control Post-Level Change	4.05	1.05	0.00 ***
β_3	Control Post-Trend Change	0.23	0.23	0.34
β_4	Treatment/Control Pre-Level Difference	-1.11	1.14	0.34
β_5	Treatment/Control Pre-Trend Difference	0.02	0.23	0.92
β_6	Treatment/Control Post-Level Difference	-3.55	1.48	0.02 *
β_7	Treatment/Control Change in Slope Difference Pre-to Post-	-0.31	0.31	0.34

Comparing New York Finance to Not-New York Finance with Connecticut Data

Figure 9: Comparing New York Finance to Not-New York Finance with Connecticut Data

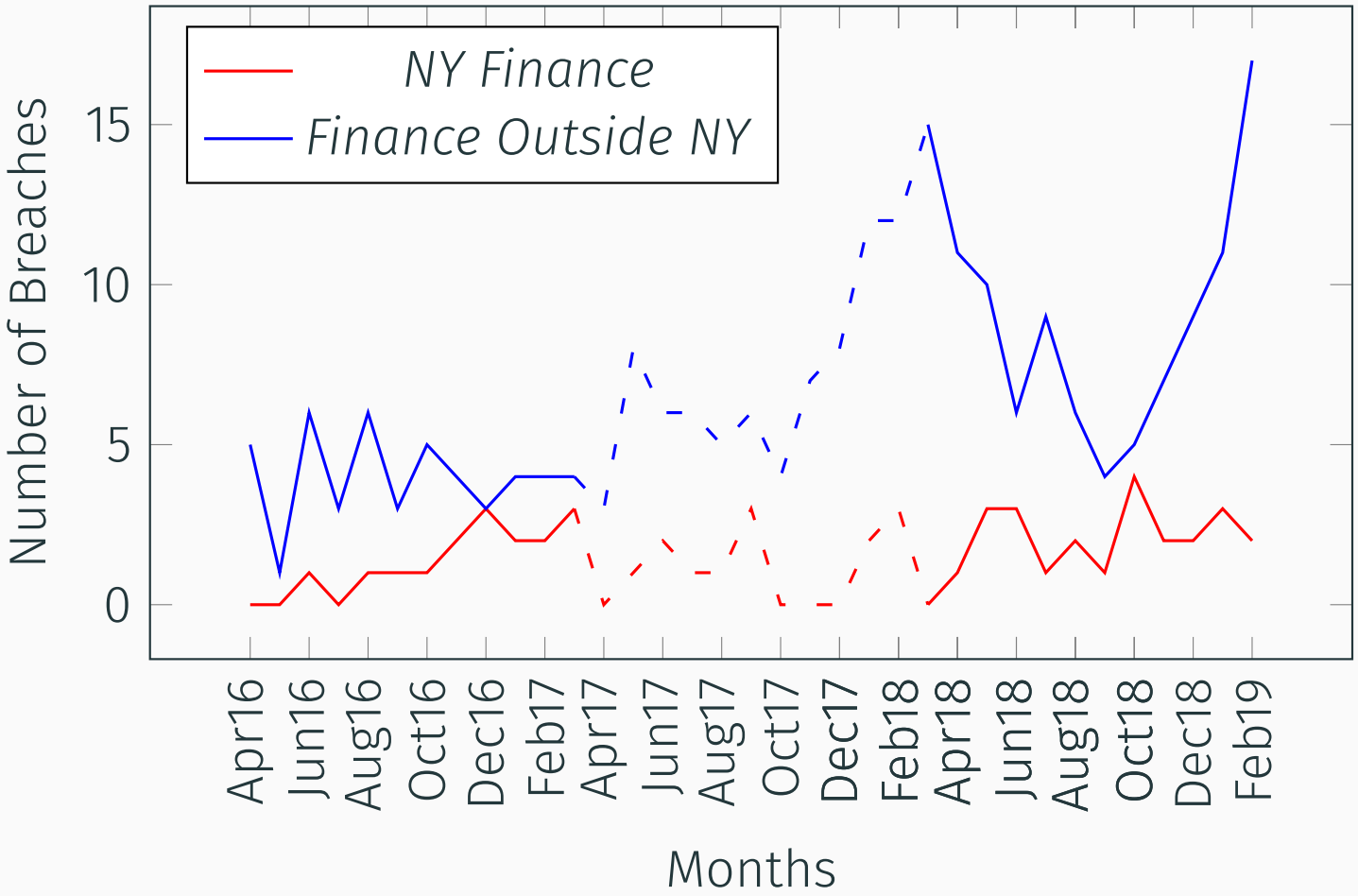


Comparative ITS NY DFS Regulations (NY Finance Compared to NY Not-Finance with Connecticut Data)

Parameter	Interpretation	Estimate	Std Error	Probability
α	Intercept	3.97	2.68	0.15
β_1	Control Pre-Trend	-0.10	0.36	0.79
β_2	Control Post-Level Change	9.66	3.57	0.01 *
β_3	Control Post-Trend Change	-0.32	0.51	0.54
β_4	Treatment/Control Pre-Level Difference	-4.17	3.79	0.28
β_5	Treatment/Control Pre-Trend Difference	0.23	0.51	0.66
β_6	Treatment/Control Post-Level Difference	-9.51	5.05	0.07 .
β_7	Treatment/Control Change in Slope Difference Pre-to Post-	0.26	0.73	0.73

Comparing New York Finance to Not-New York Finance with Connecticut Data (First Date of Breach)

Figure 10: Comparing New York Finance to Not-New York Finance with Connecticut Data (First Date of Breach)

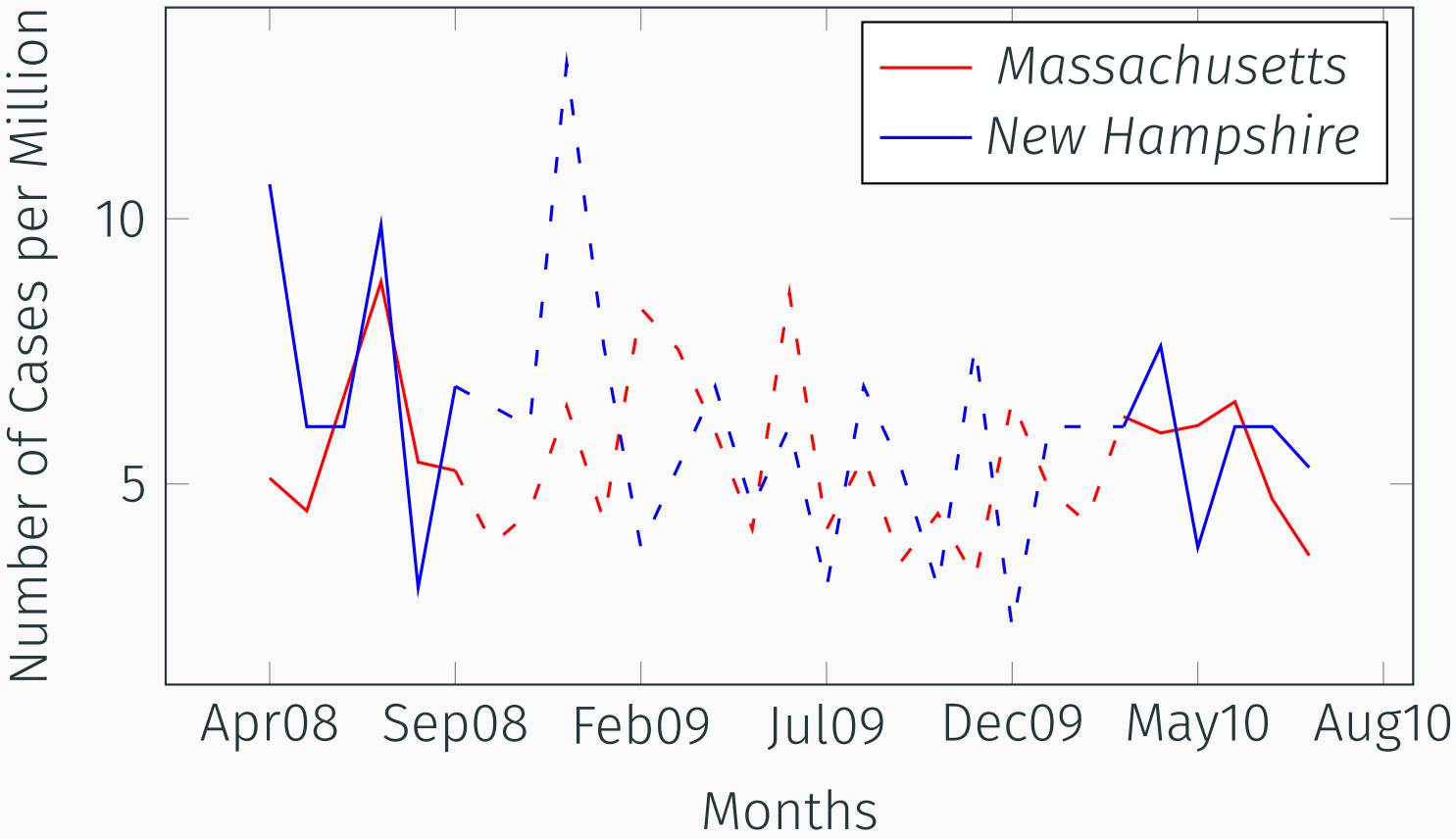


Comparative ITS NY DFS Regulations (NY Finance Compared to NY Not-Finance, Connecticut Robustness Check)

Parameter	Interpretation	Estimate	Std Error	Probability
α	Intercept	4.05	1.40	0.01 **
β_1	Control Pre-Trend	-0.00	0.19	0.97
β_2	Control Post-Level Change	5.07	1.87	0.01 **
β_3	Control Post-Trend Change	0.03	0.27	0.92
β_4	Treatment/Control Pre-Level Difference	-4.44	1.98	0.03 *
β_5	Treatment/Control Pre-Trend Difference	0.27	0.27	0.31
β_6	Treatment/Control Post-Level Difference	-6.68	2.65	0.02 *
β_7	Treatment/Control Change in Slope Difference Pre-to Post-	-0.16	0.38	0.66

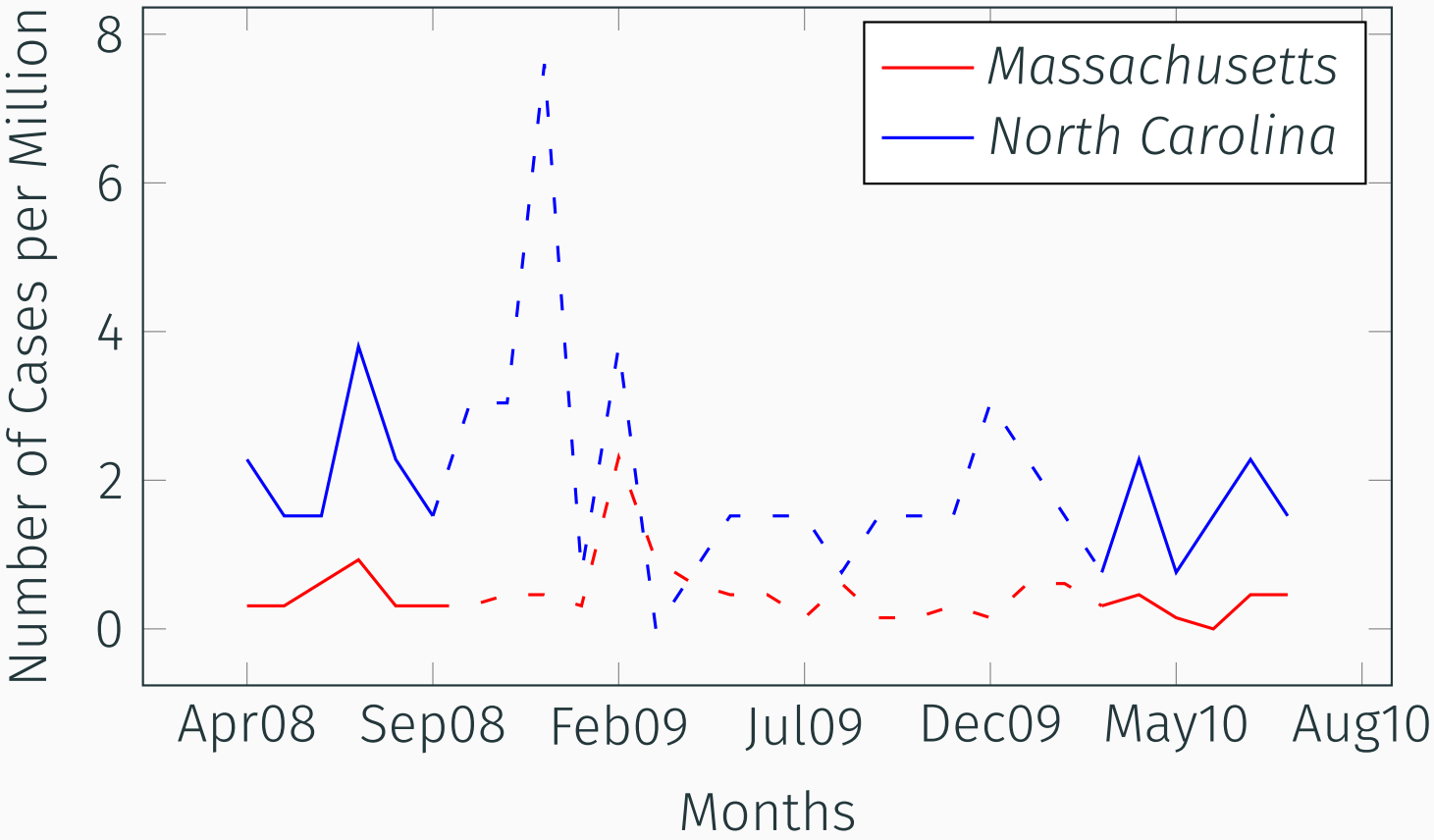
Massachusetts Data Security Law (1 of 2)

Figure 11: Comparing Massachusetts and New Hampshire



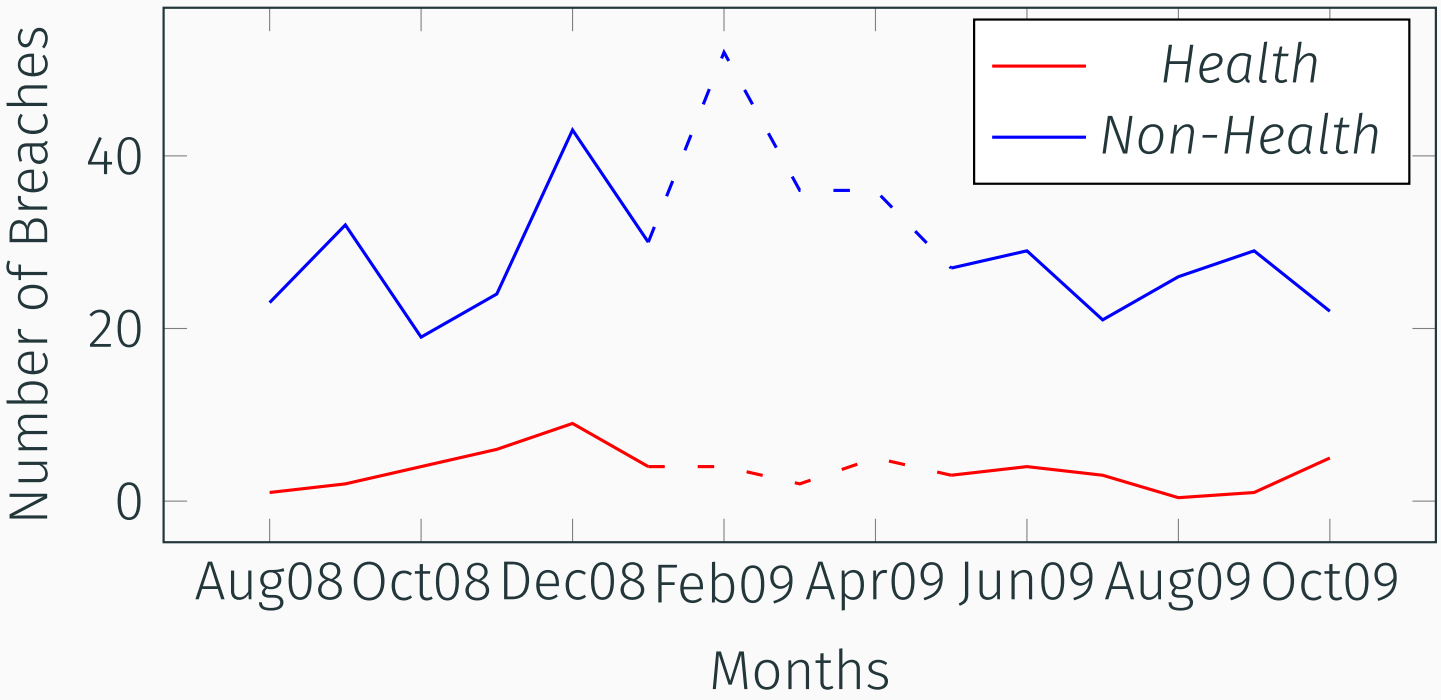
Massachusetts Data Security Law (2 of 2)

Figure 12: Comparing Massachusetts and North Carolina (1000+ residents)



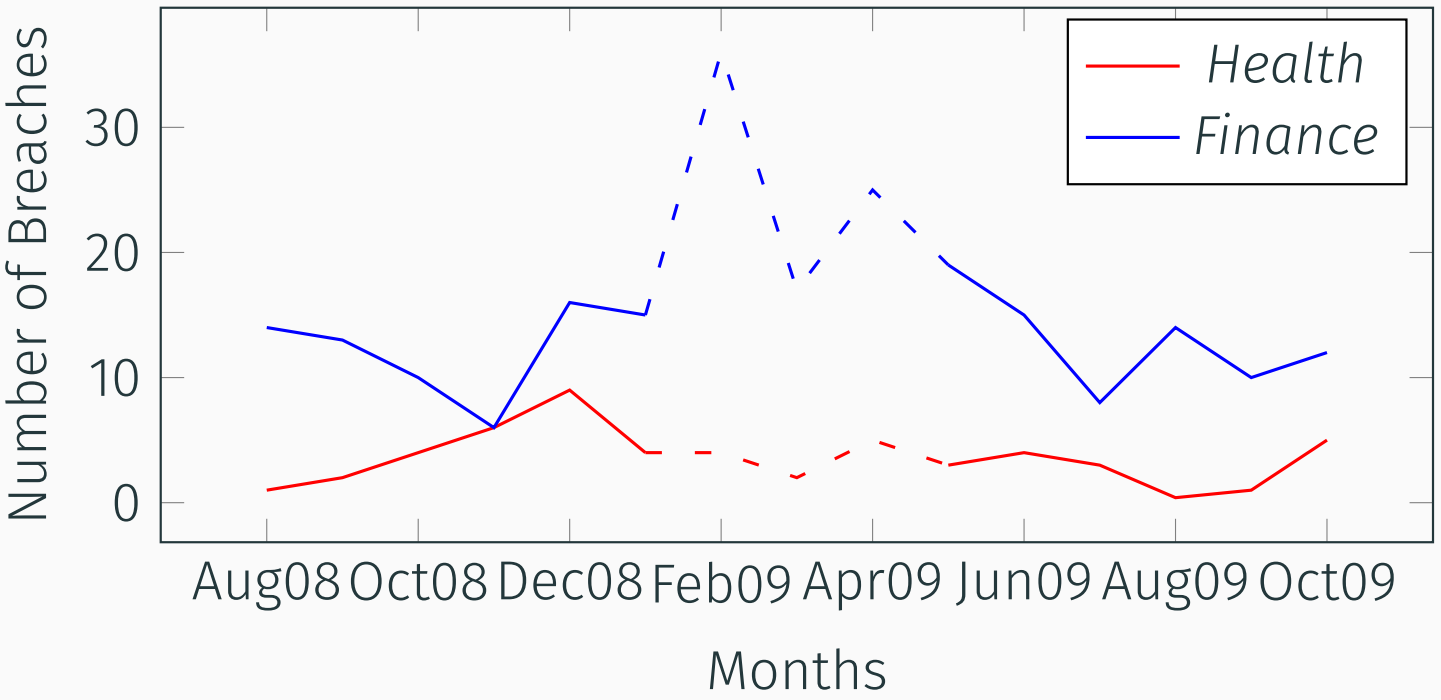
HITECH Act (1 of 2)

Figure 13: Comparing Health vs Non-Health Breaches



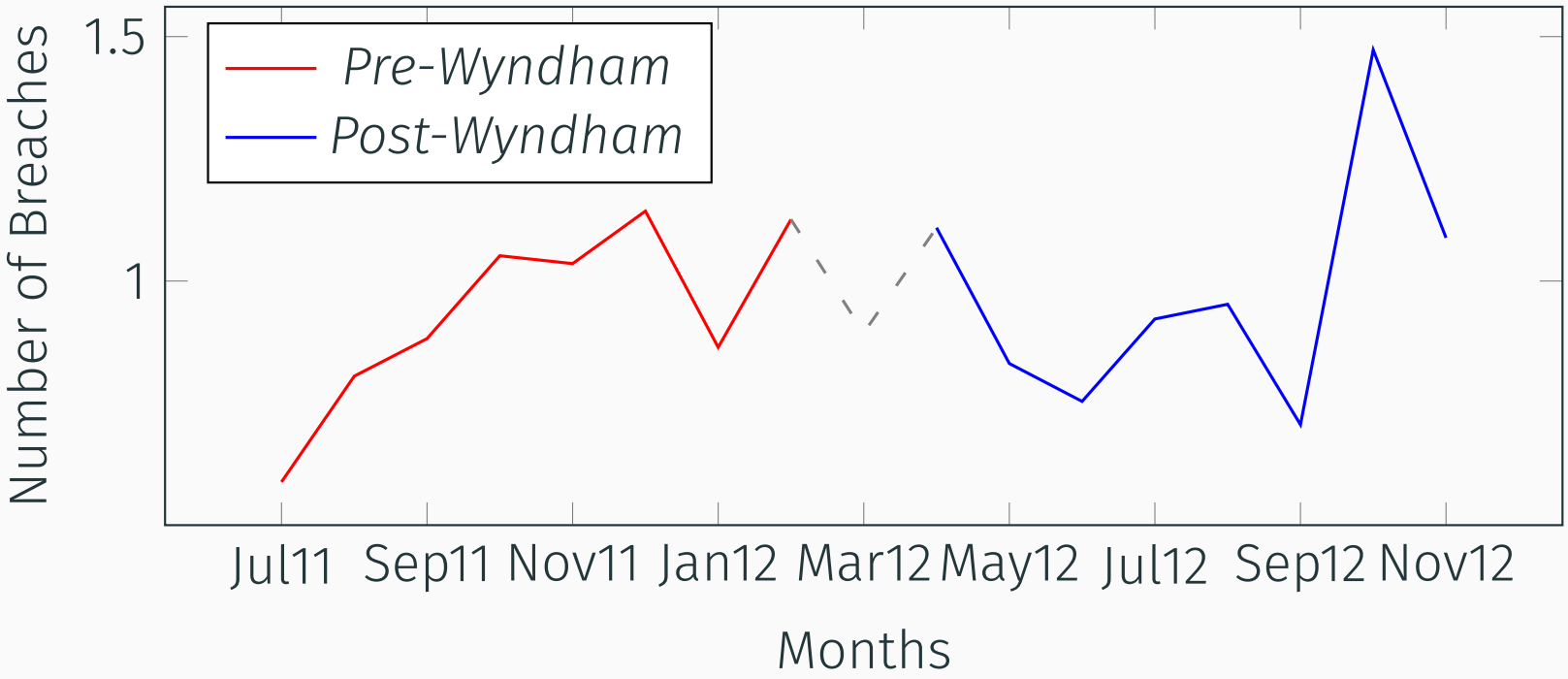
HITECH Act (2 of 2)

Figure 14: Comparing Health vs Finance Breaches



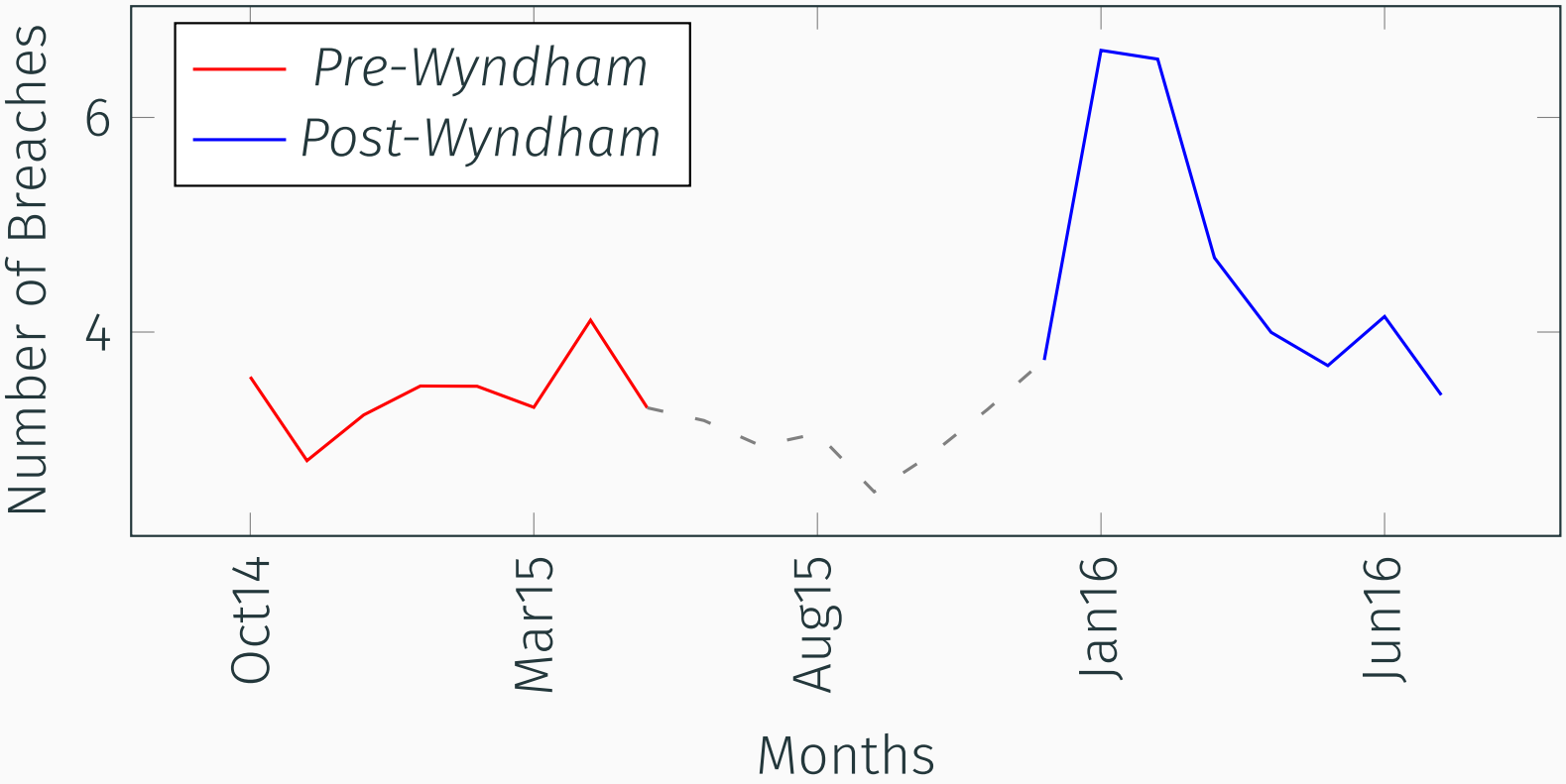
Wyndham FTC Suit Initial Complaint

Figure 15: The Wyndham FTC Suit as Intervention



Wyndham FTC Suit Third Circuit

Figure 16: The Wyndham FTC Suit as Intervention (Third Circuit Decision)



Quasi-Experiment for Wyndham FTC Suit, Third Circuit Decision

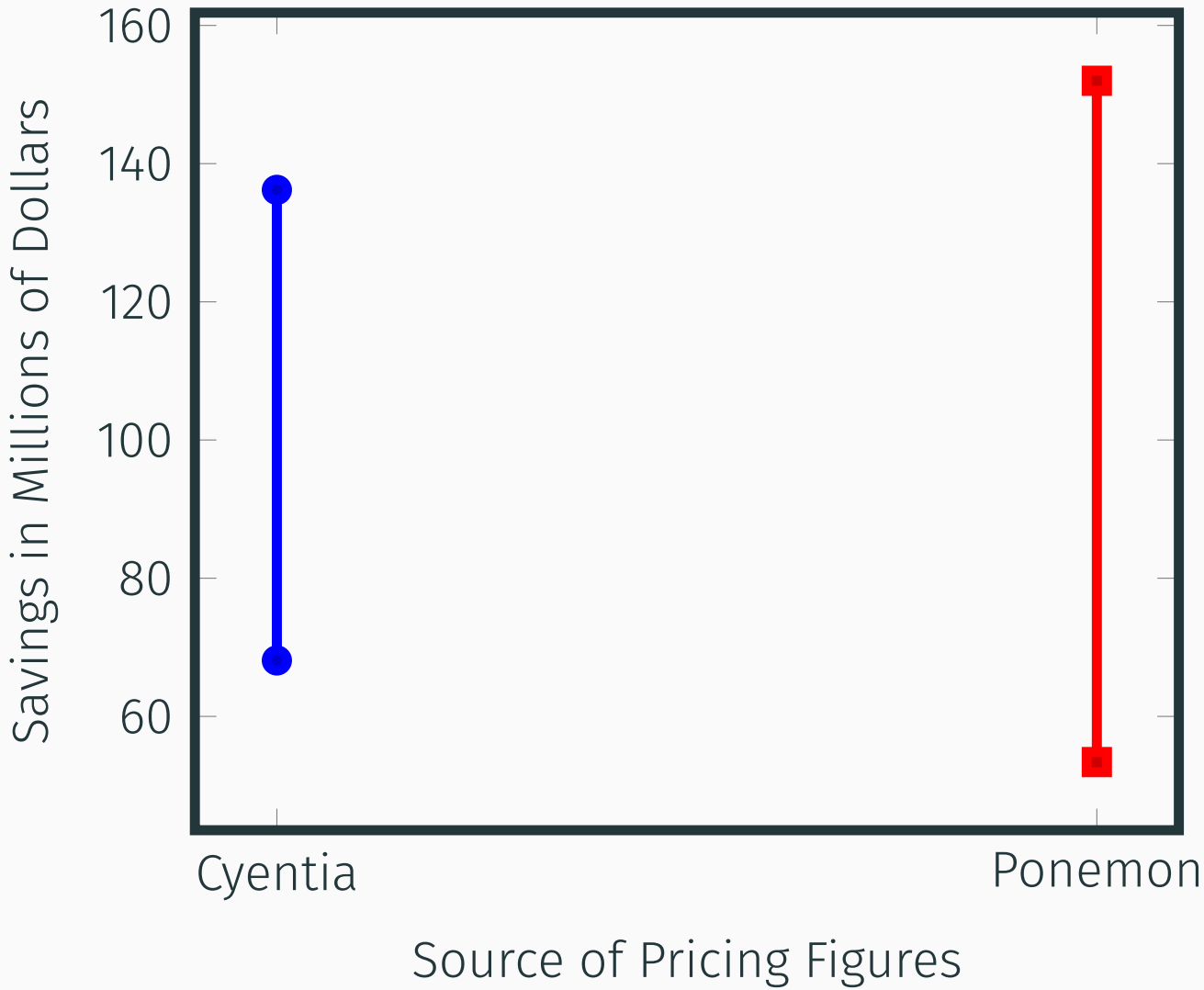
Table 2: Quasi-Experiment for Wyndham FTC Suit, Third Circuit Decision

Parameter	Interpretation	Estimate	Std Error	Probability
α	Intercept	3.16	0.67	0.00 ***
β_1	Pre-Trend	0.06	0.13	0.68
β_2	Post-Level Change	2.28	0.87	0.02 *
β_3	Post-Trend Change	-0.34	0.19	0.09 ·

Implications

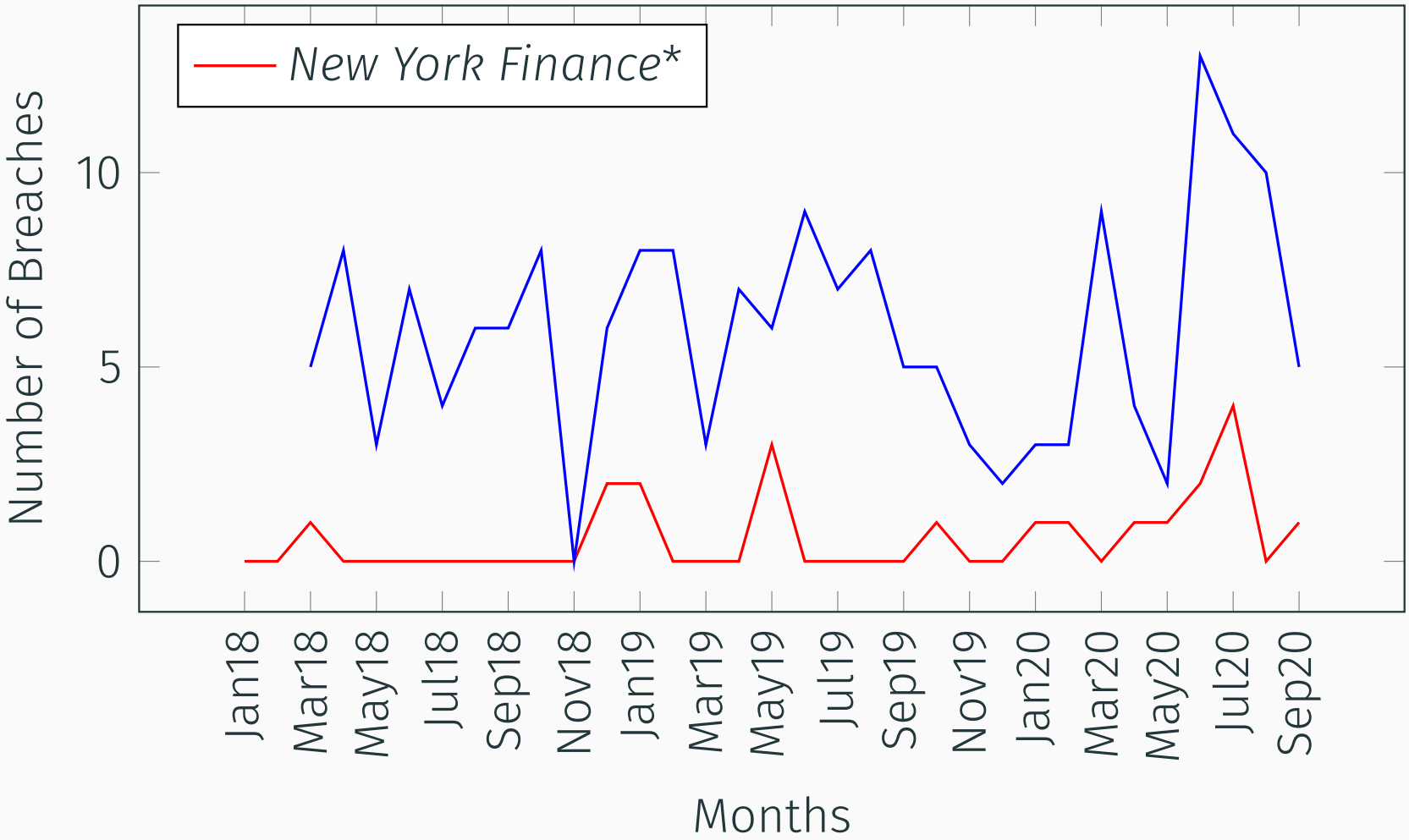
Estimate of Saving from NY DFS Regulations

Figure 17: Savings from Regulation over 1 Year



Question of Persistence of Breach Reduction

Figure 18: New York Financial Breach Growth in 2020



Regulatory Requirements

Table 3: Organizational Regulatory Requirements

	MA Data Security Law	HITECH Act	FTC Section 5 (Wyndham Hotel)	NY Dept of Financial Services
Designation of specific personnel	Yes	No	No	Yes
Education and training of employees	Yes	No	No	Yes
Creation and maintenance of cyber policies	Yes	No	No	Yes
Notification of Breaches	Yes/No[4]	Yes	No	Yes
Certification of compliance	No	No	No	Yes

[4]The initial law included a notification requirement, however the cybersecurity provisions were implemented later.

Computer Security Requirements

Table 4: Computer Security Requirements

	MA Data Security Law	HITECH Act	FTC Section 5 (Wyndham Hotel)	NY Dept of Financial Services
Secure user authentication protocols	Yes	No	Yes/No[5]	Yes
Secure access control measures	Yes	No	Yes/No[5]	Yes
Encryption requirements	Yes	Yes	Yes	Yes
Reasonably up-to-date security software, patches, virus definitions	Yes	No	Yes/No[5]	Yes
Control third-party access to network	Yes	No	Yes	Yes

[5] Cited in the FTC's complaint against Wyndham, but also employed in prior actions

Summary

- The NY DFS cyber regulations had the strictest organizational and technical requirements.
- The NY DFS cyber regulations while effective, may not be persistent.
- Overall, there is mixed to limited evidence for the efficacy of US regulatory cyber policy interventions.
- Tools of policy evaluation, like quasi-experiments, can be applied to cybersecurity policy interventions.

Questions?

Massachusetts Data Security Law

MA Data Security Law

Official Title: (201 CMR 17) Standards for the protection of personal information of residents of the Commonwealth

Policy Impact

- Applies to anyone with personal information about a resident of the Commonwealth
- Mandates companies develop, implement, and maintain a comprehensive information security program

Regulator: Massachusetts Office of Consumer Affairs and Business Regulation

HITECH Act

HITECH Act

Official Title: Health Information Technology for Economic and Clinical Health Act
Part of the American Recovery and Reinvestment Act of 2009

Policy Impact

- Amended the HIPAA Security Rule on personal health data
- Mandates Breach Notification when 500+ individuals affected

Regulator: United States Department of Health and Human Services

NY DFS Regulations

NY DFS Regulations

Official Title: 23 NYCRR 500 - Cybersecurity Requirements for Financial Services Companies

Policy Impact

- Requires certification of compliance with NY State
- Mandates policies, procedures, and risk assessments

Regulator: New York Department of Financial Services

FTC Section 5

FTC Section 5

Official Title: Section 5(a) of the Federal Trade Commission Act (15 USC §45)

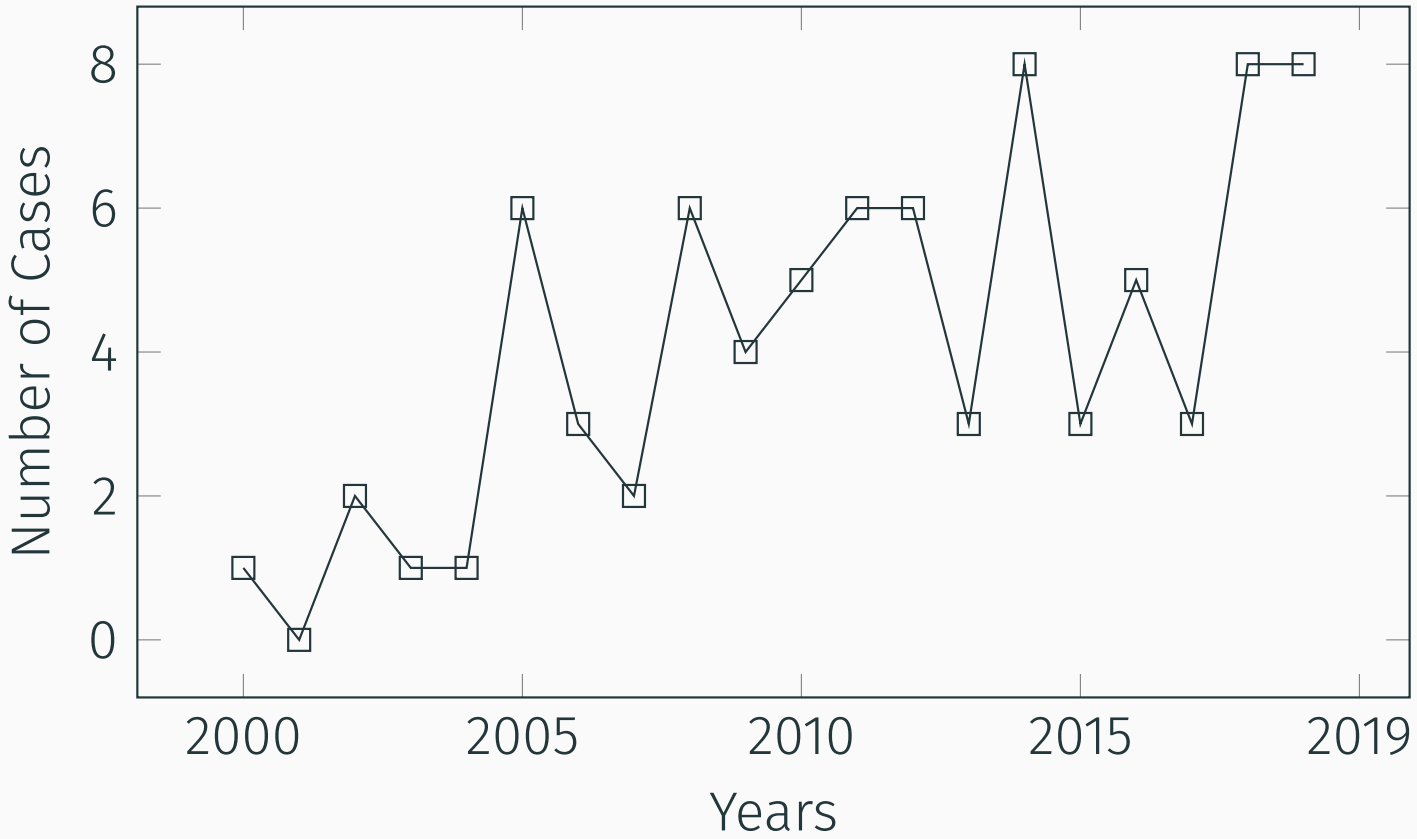
Policy Impact

- Prohibits “unfair or deceptive acts or practices in or affecting commerce.”
- Data security orders require a comprehensive information security program

Regulator: United States Federal Trade Commission

FTC Section 5

Figure 19: FTC Data Breach Enforcement Cases per Year



Source: FTC Cases and Proceedings Advanced Search, Tagged as Data Security Topic

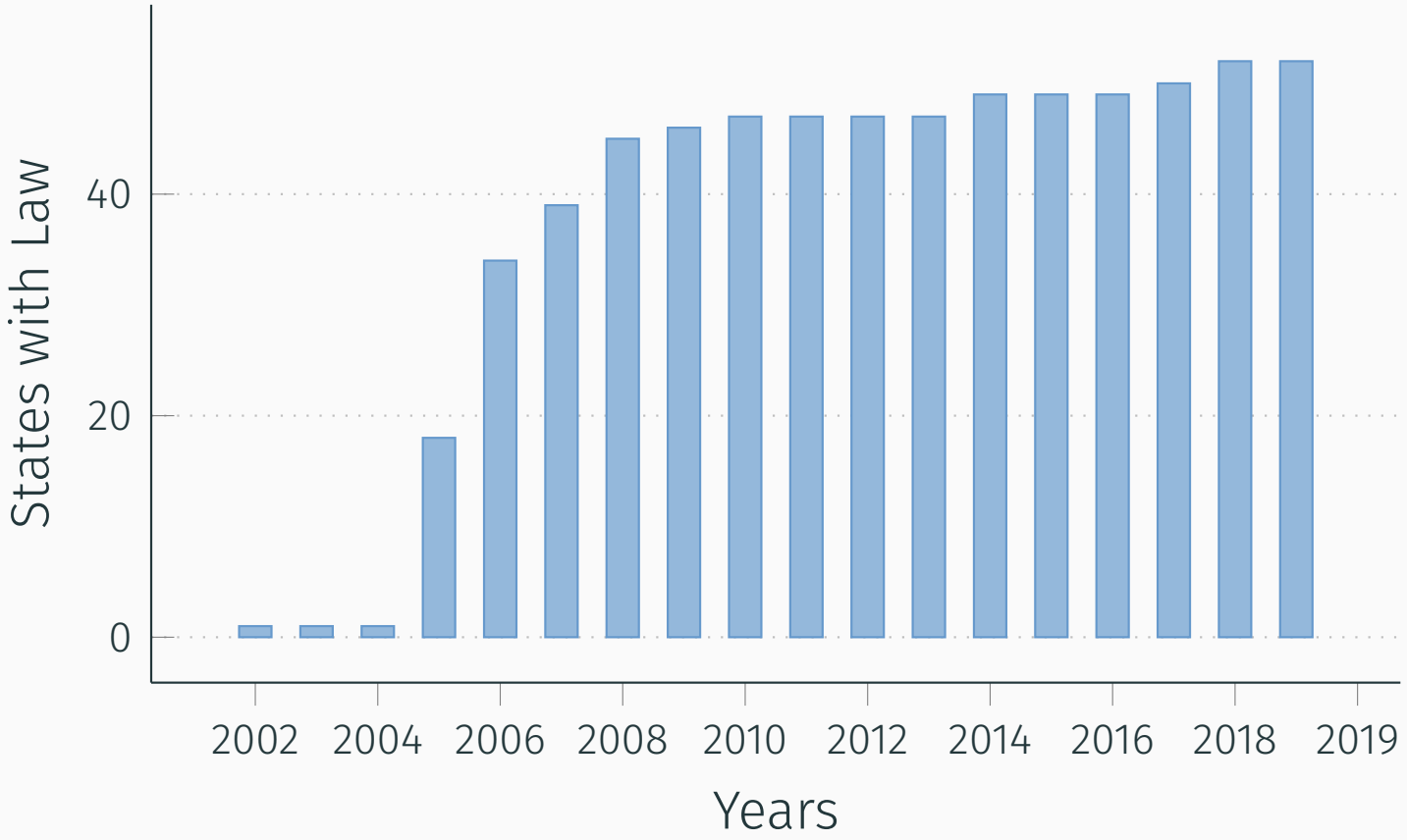
Command and Control vs Meta-Regulations

> *'**Command and control**' regulation, which refers to the prescriptive nature of the regulation (the command) supported by the imposition of some negative action by the regulator (the control) ... If adequately enforced, command and control regulation is dependable; it can specify operational parameters and regulatory obligations with clarity and immediacy.*
>
> *'**Meta-regulation**' has been used to describe regulation for self-regulation in different ways. At its most basic, it relates to corporate self-audits and safety cases where businesses develop their own rules and reporting for the regulator to assess.*

-F.C. Simon, 2017 [6]

Background: Breach Notification Laws

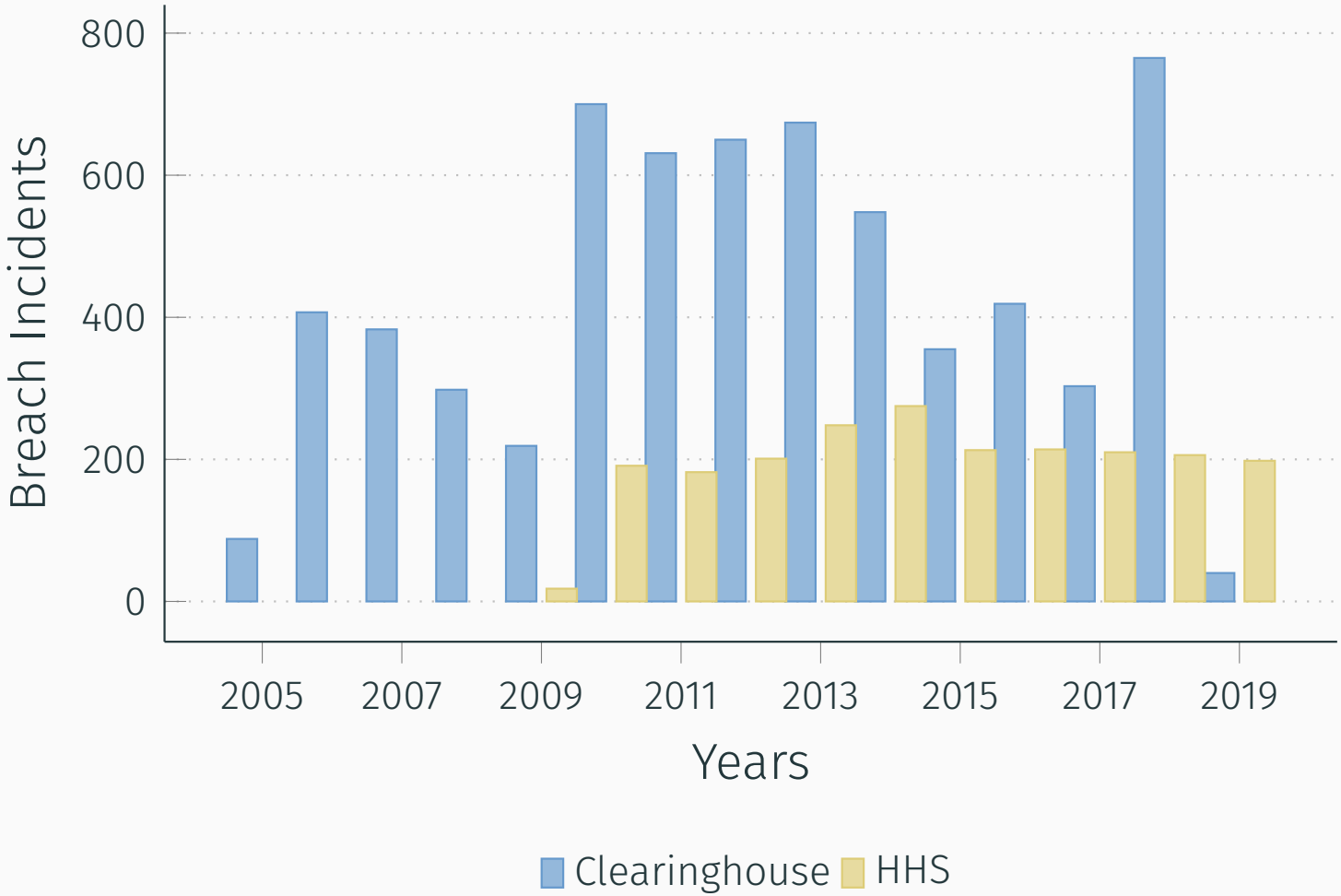
Figure 20: States and Territories with Breach Notification Laws in Place by Year



Source: IT Governance USA Inc

Literature Review: Datasets (Continued)

Figure 21: Data Breach Incidents by Year in Public Datasets

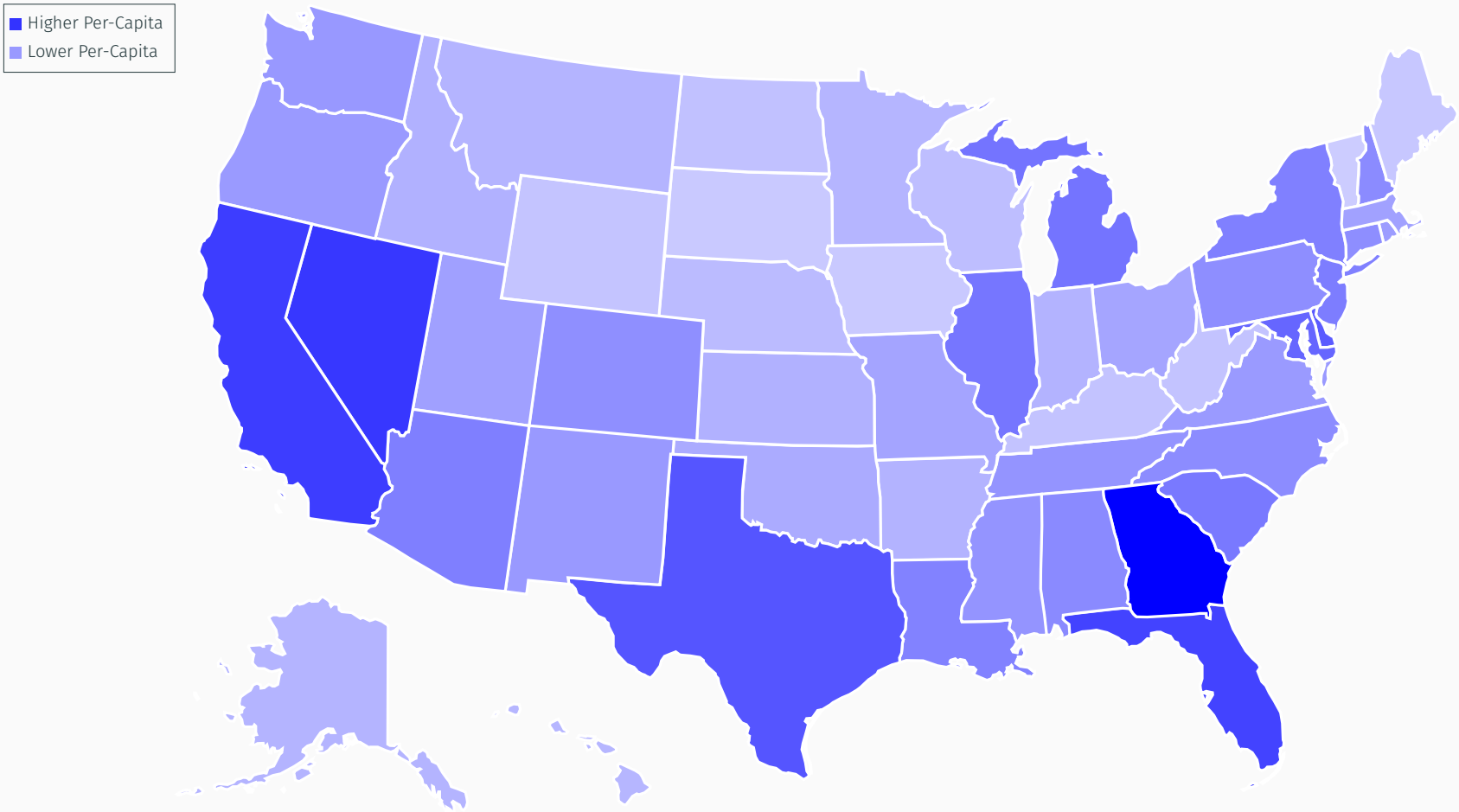


Variables

- Dependent variables
  - Reports of Data Breaches to the States
  - Identity Theft Reports (FTC Consumer Sentinel Network)
  - Cybersecurity Complaints (FBI Internet Crime Complaint Center)
- Independent variables
  - Changes in Breach Reporting Requirements
  - Cyber Hygiene (CyberGreen)
  - Vulnerability (NVD Scores)
  - Cybersecurity Spending (Taxpayers for Commons Sense, OMB)

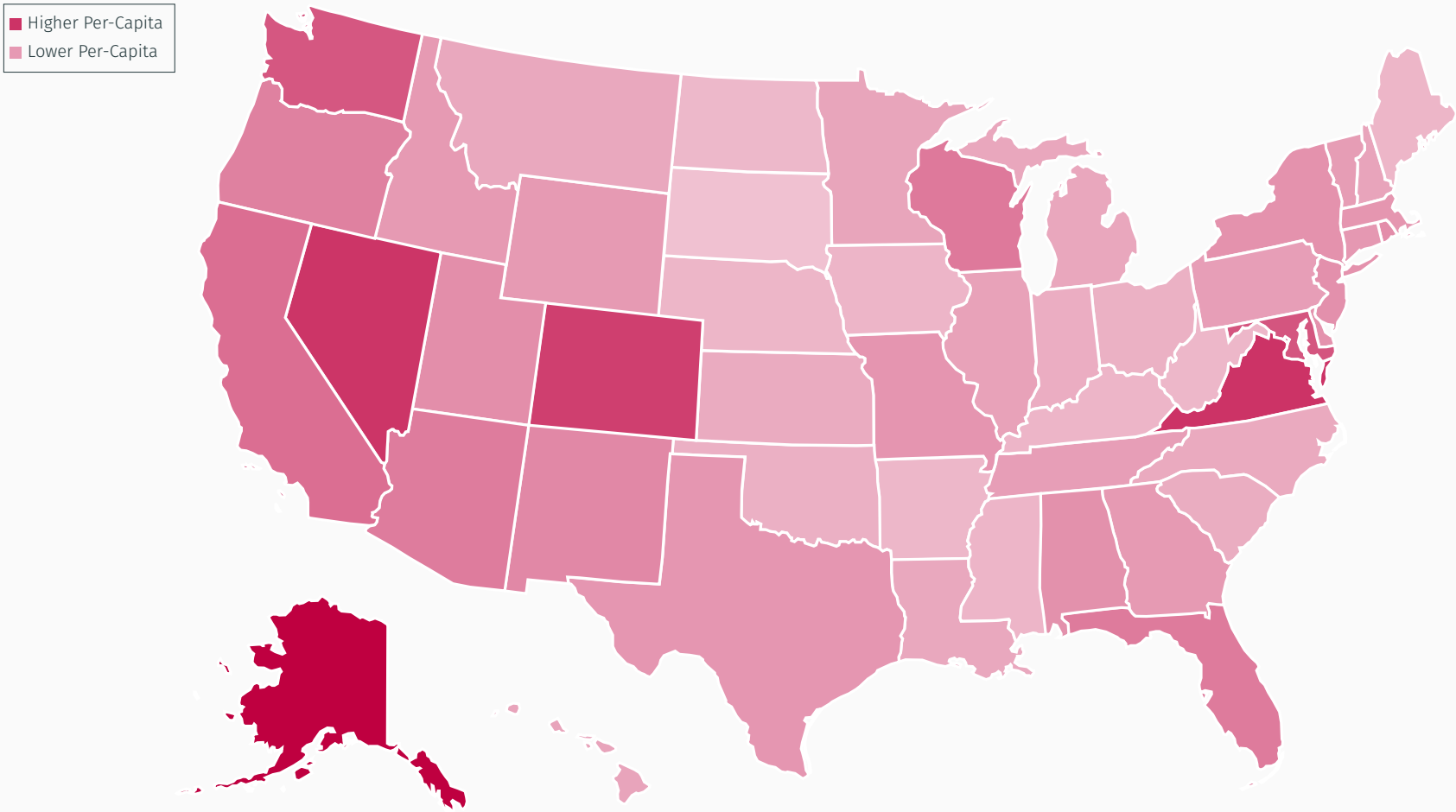
Dependent Variable: Identity Theft

Figure 22: Identity Theft Reports Per Capita in 2018 (FTC)



Dependent Variable: Cybersecurity Complaints

Figure 23: Cybersecurity Complaints Per Capita in 2018 (FBI IC3)



Independent Variable: Changes in Data Breach Laws

Figure 24: Proposed Breach Notification Legislation

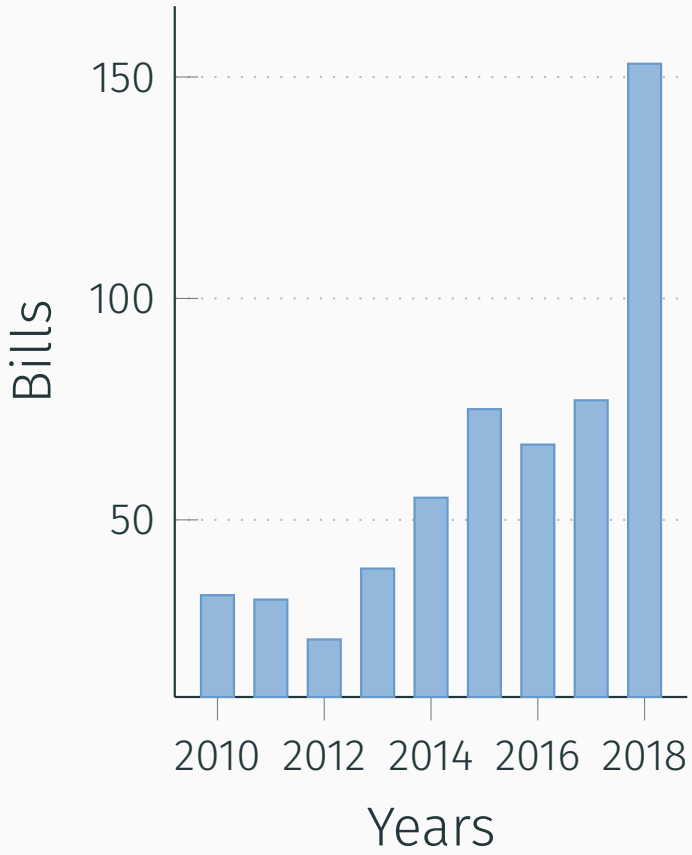
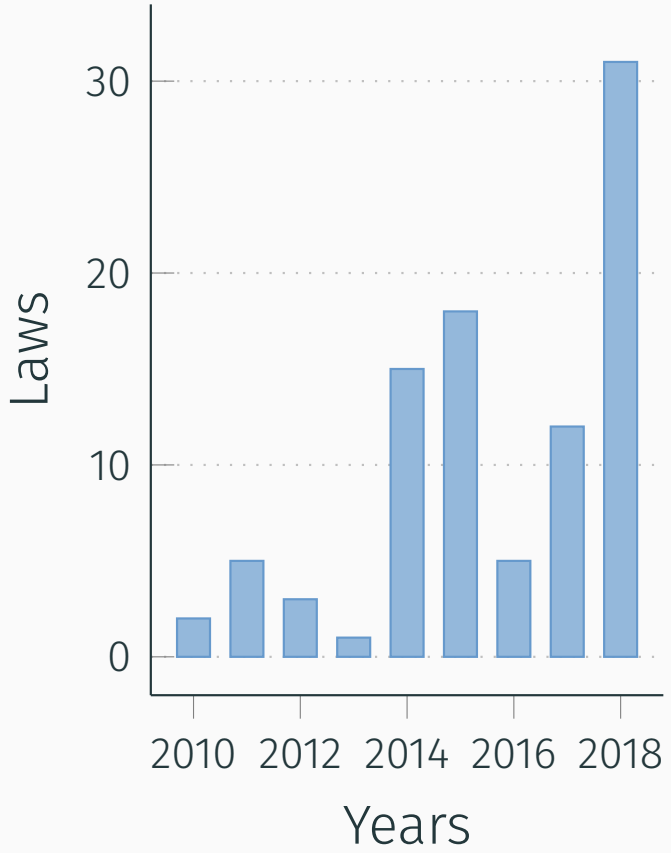
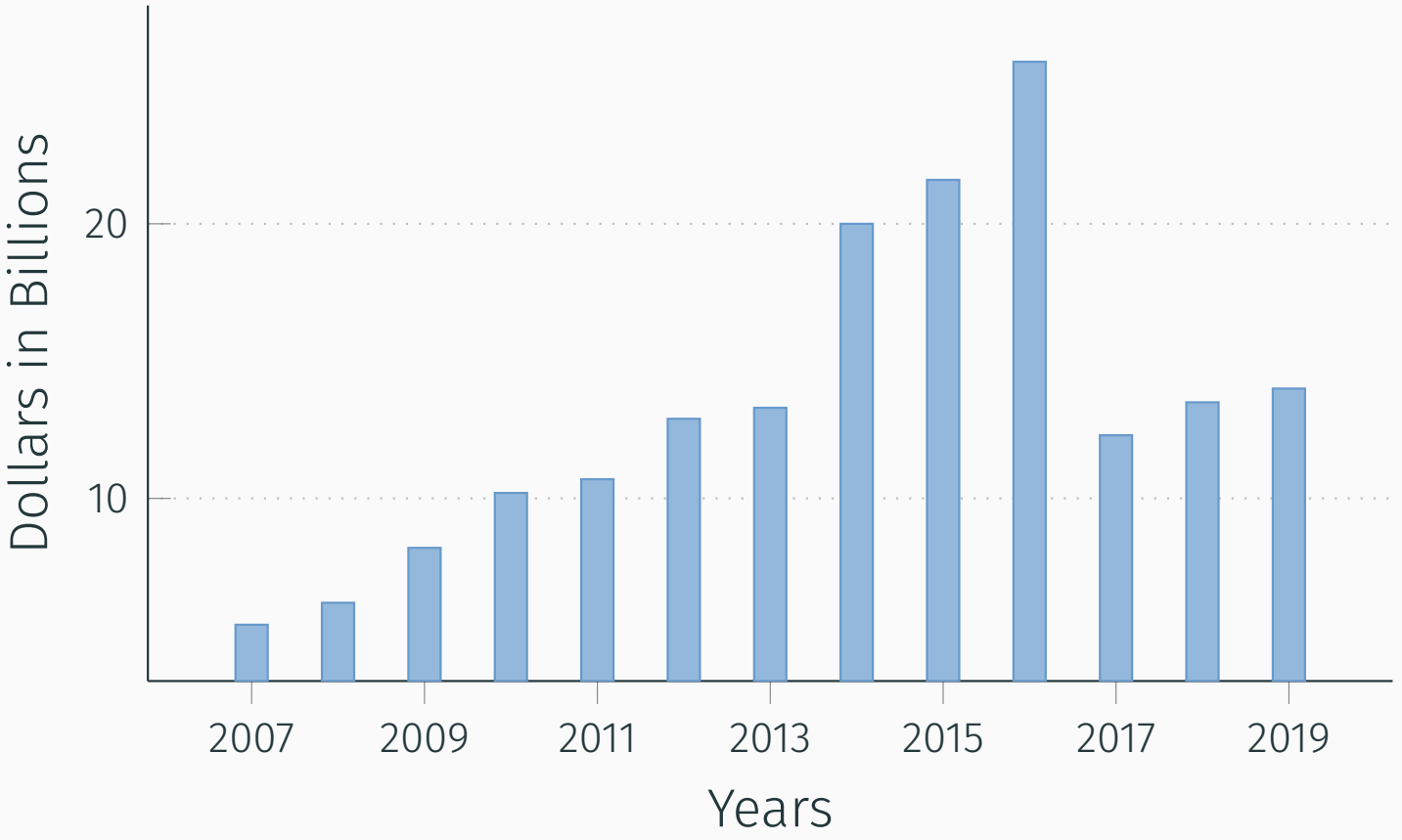


Figure 25: New and Amended Data Breach Notification Laws



Independent Variable: Cybersecurity Spending

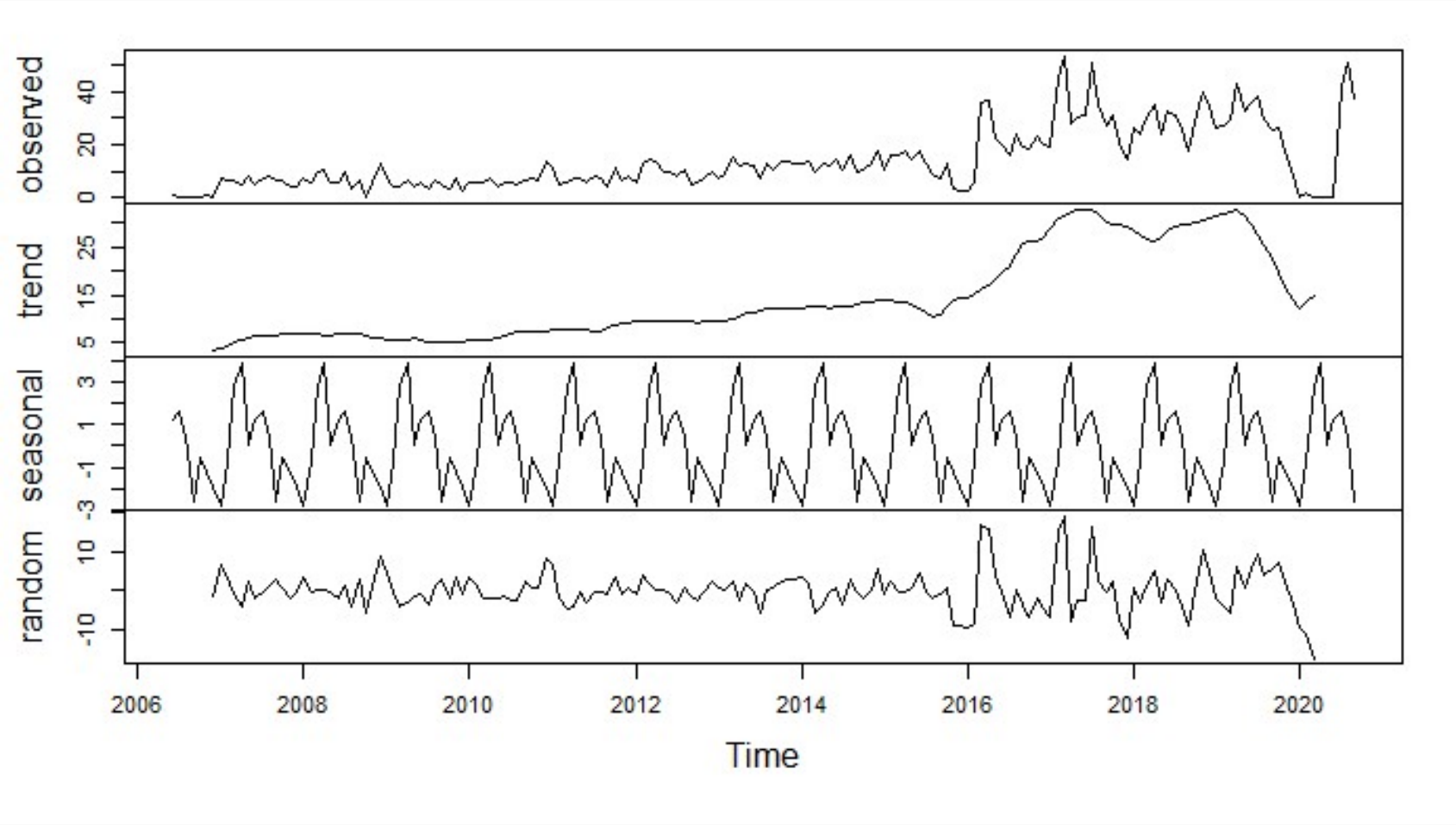
Figure 26: Cybersecurity Dollars Spent by CFO Agencies in Billions per FY



Source: Taxpayers for Common Sense '07-'16, Office of Management and Budget '17-'19

Decomposition of Trends

Figure 27: Sample Decomposition of Additive Time Series for Massachusetts*

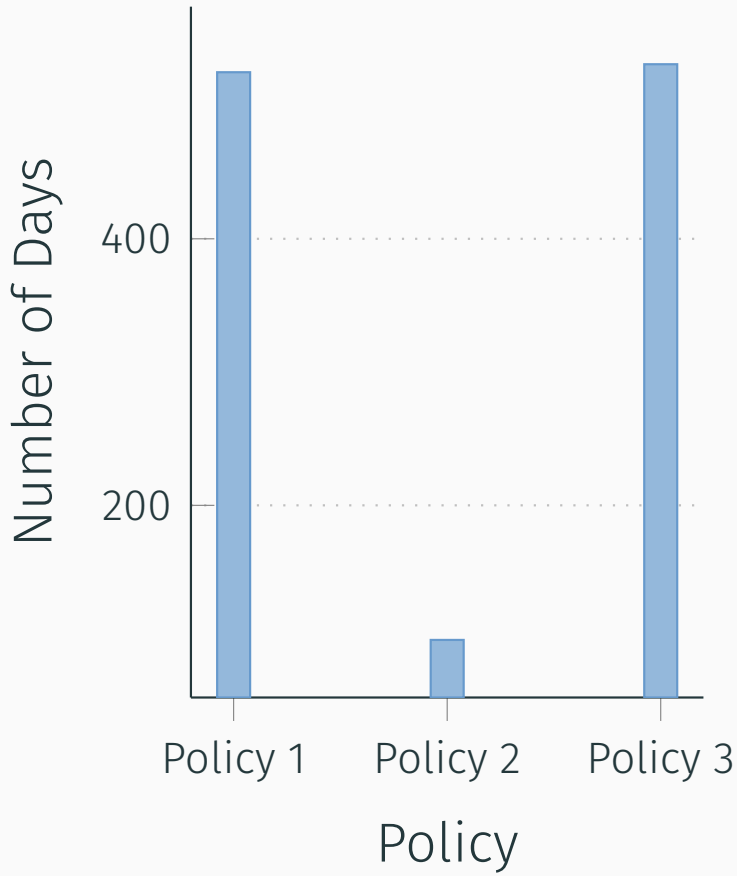


* Data breaches per Million in Massachusetts

Case Implementation Period

1. MA Data Security Law
   - Enacted: September 22, 2008
   - Enforcement: March 1, 2010
2. HITECH Act
   - Enacted: February 17, 2009
   - Enforcement: May 27, 2009
3. NY DFS regulations
   - Enacted: March 1, 2017
   - Enforcement: September 3, 2018 (Third Phase)

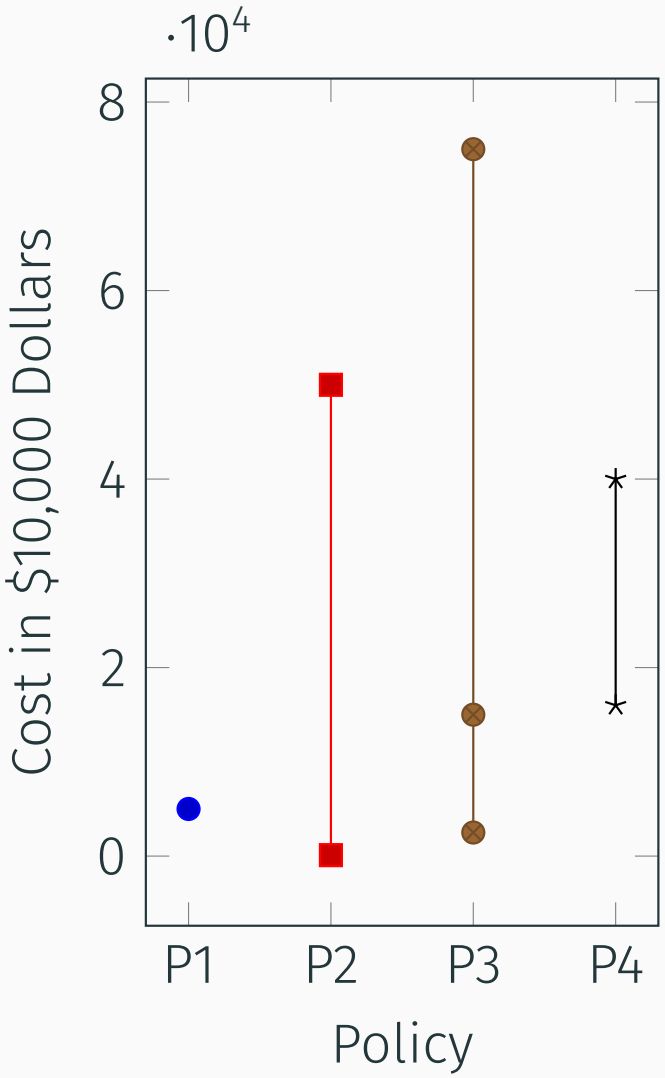
Figure 28: Implementation Days



Comparison of Regulatory Penalties

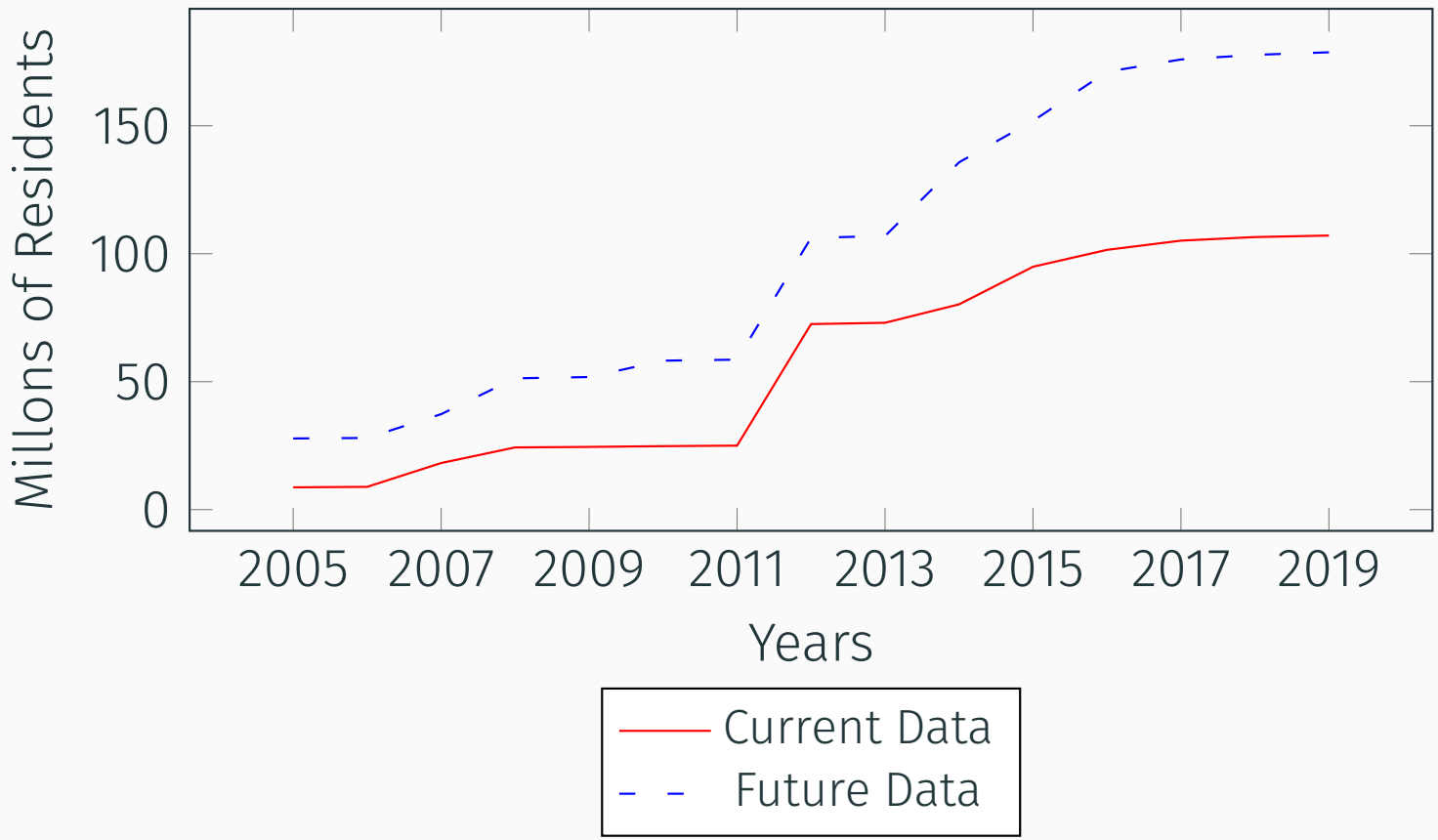
1. MA Data Security Law
    - Penalties have a maximum limit per violation of $5,000
2. HITECH Act
    - Penalties are limited per violation at $100 to $50,000
3. NY DFS regulations
    - Penalties have a maximum limit per day of
        - $2,500 (any-violation)
        - $15,000 (negligence)
        - $75,000 (knowing)
4. FTC Enforcements
    - Penalties have a maximum limit per violation of
        - $16,000 (pre-2016)
        - $40,000 (post-2016)

Figure 29: Maximum Penalty



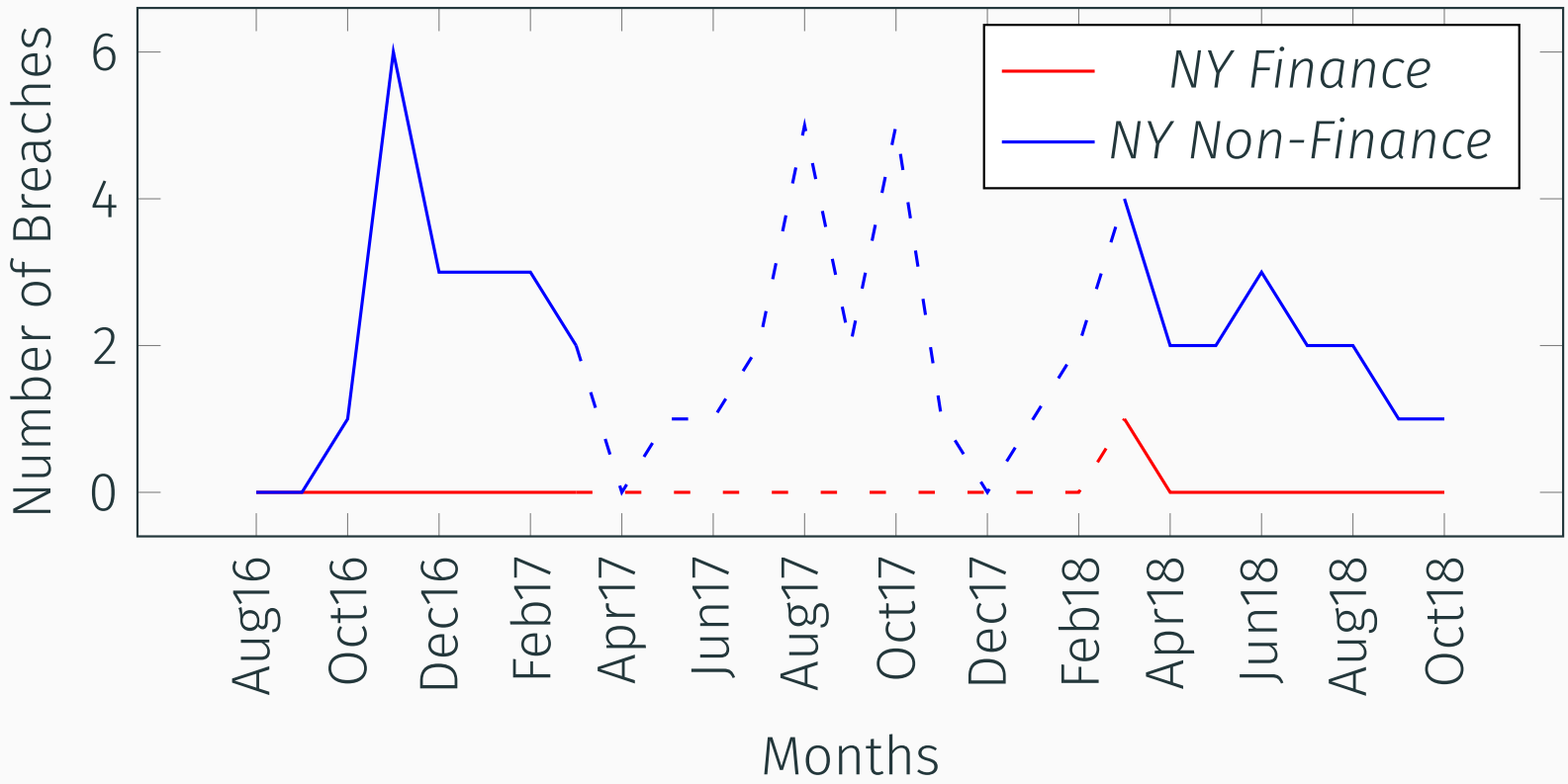
Backup slides

Figure 30: Population of States Reporting Breach Notifications



Comparing New York Finance to New York Not-Finance with Maine Data

Figure 31: Comparing New York Finance to New York Not-Finance



Comparative ITS NY DFS Regulations (NY Finance Compared to NY Not-Finance with Maine Data

Parameter	Interpretation	Estimate	Std Error	Probability
α	Intercept	0.54	0.79	0.50
β_1	Control Pre-Trend	0.38	0.16	0.02 *
β_2	Control Post-Level Change	-0.01	1.02	0.99
β_3	Control Post-Trend Change	-0.70	0.22	0.00 **
β_4	Treatment/Control Pre-Level Difference	-0.54	1.11	0.63
β_5	Treatment/Control Pre-Trend Difference	-0.38	0.22	0.10 .
β_6	Treatment/Control Post-Level Difference	0.51	1.45	0.73
β_7	Treatment/Control Change in Slope Difference Pre-to Post-	0.62	0.31	0.06 .

References i


Benjamin Dean.
Natural and Quasi-Natural Experiments to Evaluate Cybersecurity Policies.
Vol. 70, No. 1:129–160.


K. M. Hogan, G. T. Olson, and M. Angelina.
A Comprehensive Analysis of Cyber Data Breaches and Their Resulting Effects on Shareholder Wealth.


A. Kesari.
The Effect of State Data Breach Notification Laws on Medical Identity Theft.


E. Y. Liu.
The effect of state characteristics and cybercrime legislation on Internet crime.

References ii


S. Romanosky, R. Telang, and A. Acquisti.
Do data breach disclosure laws reduce identity theft?: Do Data Breach Disclosure Laws Reduce Identity Theft?
30(2):256–286.


F. C. Simon.
Meta-Regulation in Practice: Beyond Normative Views of Morality and Rationality.
Routledge Advances in Sociology. Routledge, Taylor & Francis Group.


G. Werner, S. Yang, and K. McConky.
Time series forecasting of cyber attack intensity.
In *Proceedings of the 12th Annual Conference on Cyber and Information Security Research - CISRC '17*, pages 1–3. ACM Press.