CARLSON SCHOOL OF MANAGEMENT
UNIVERSITY OF MINNESOTA

Law School

UNIVERSITY OF MINNESOTA
Driven to Discover℠

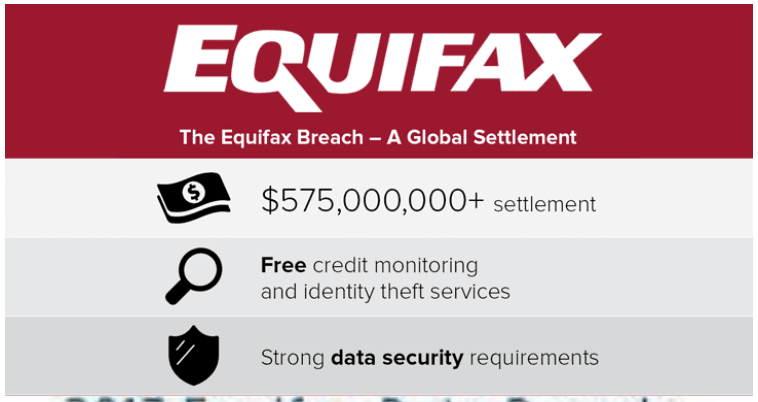
State Breach Notification Laws Aren't Working… But They Could

Paul M. Vaaler
Law School & Carlson School of Management
University of Minnesota

Paul M. Vaaler (vaal0001@umn.edu
13th Annual Cybersecurity Summit
Double Tree Hotel, Bloomington, MN
October 24-26, 2023
3:00-3:30pm
Ballroom

Firm Data Breaches Are a Problem…Everywhere

The 2013 breach of Target customer credit card and related payment systems supplier information leading to the CEO's ouster.



…The 2017 leak and hack of Equifax PII for tens of millions of US customers costing hundreds of millions in damages and related costs…

…The 2021 leak and then hack of PII for VWA owners and potential owners…on top of the "clean diesel" scandal of 2010s.

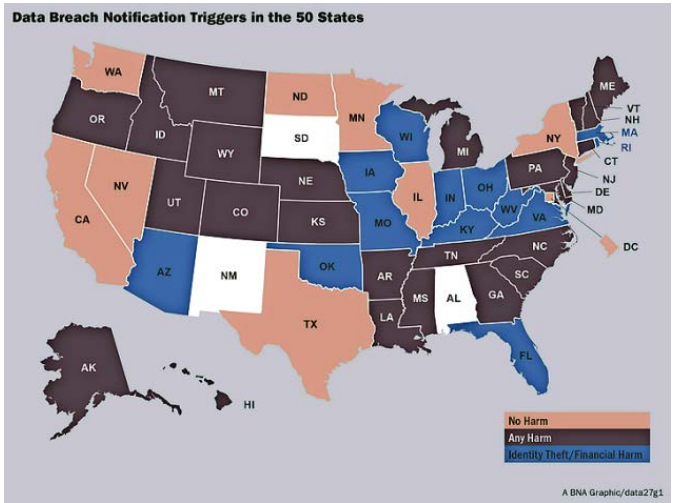
And BNLs Are the Principal Defense

- The US federal data security regime is an uneven patchwork applying to specific industries and groups:

1. Fair and the Accurate Credit Transactions Act (FACT).
2. Health Insurance Portability and Accountability Act (HIPAA).
3. Children's Online Privacy Protection Act (COPPA).
4. Sarbanes-Oxley Act (SOX)

- State BNLs essentially cover the rest of us:

1. California enacted the first BNL in 2003.
2. All 50 states and DC enacted BNLs by 2018.
3. Variations on a state-by-state BNL theme: triggers, notification requirements, public and private rights of action, publication to inform and guide state residents.
4. BNLs generally apply to where firm customers live. Big firms operating (inter)nationally have customers in virtually every state…starting with California.



How BNLs Should Work

- BNL enactment itself should decrease data breaches…and right away:

1. Impose breach search, notification, and mitigation costs on firms.
2. Impose fines as well as public and private liability for untimely notification.
3. Put public officials (*e.g.,* State AG) and residents on notice.

- BNL enactment should prompt broader market developments that decrease data breaches…in the long run (Becker, 1968):

1. See development of data security, breach surveillance, and breach mitigation standards in firms.
2. Let firms position themselves in a "market for data privacy."
3. See development of consumer-accessible information on how firms are doing in their market position.
4. Let consumers choose firms based on their own preference for data security versus cost.

What We "Know" About BNL Effectiveness

- There is substantial logic that that BNLs should work and a little evidence that they do…indirectly:

1. State-by-state approach tailored to local resident and firm preferences…developing markets.
2. Goel & Shawky (2014): Right after BNL enactment, firms incur more financial losses after data breach events.
3. Romanosky *et al.* (2011): BNL enactment decrease "downstream" identity theft.

There is no broad-sample statistical evidence regarding the impact of BNLs on data breach counts and magnitudes.

- But there is a lot of skepticism about BNL effectiveness:

1. Goel & Shawky (2014): BNL effects on firm financial losses after data breaches wane with time.
2. Laube & Böhme (2016): Hard to set optimal penalties for data breaches, even under optimistic assumptions.
3. Winn (2009): BNL penalties are inadequate to deter firms and to compensate consumers.
4. Acquisti *et al.* (2020): Hackers are more sophisticated and dark markets for breached data are more efficient.
5. Collins (2019): Consumers share more data with firms while data breach numbers increase in 2010s.

Research Questions…and Quite Possible Answer

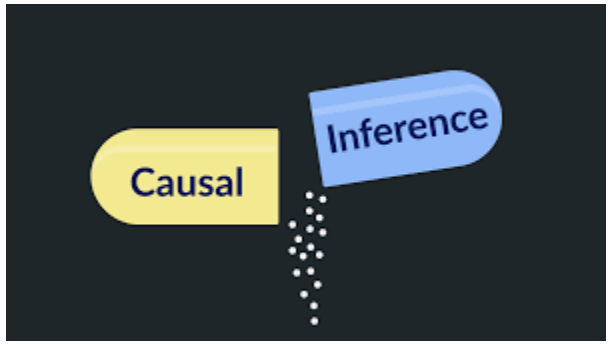
- Do BNLs work: Decrease data breach counts and magnitudes; decrease "downstream" fraud and identity theft.

- There are good reasons to think BNLs <u>won't</u> work:
  - Incentives to invest are weak (Faulkner, 2007; Joerling 2010).
  - There is a lemons problem finding partners with superior data protection (Chellappa & Pavlou, 2002).
  - Firms may be accepting the risk of cyber threats and insuring to avoid liability (Marotta *et al.,* 2017).
  - Companies might be nationalizing the issue through law enforcement (Colonial Pipeline and JBS Food Processing).

Doing a Big Data Study to Answer Those Questions

- Data and Sampling: 1) Data breach counts and magnitudes: Privacy Rights Clearing House (PRC); 2) BNL laws and enactment dates: Solove & Schwartz (2019), National Conference of State Legislatures (NCSL) (2021); 3) State data security and disposal laws: NCSL (2021); 4) Identity theft and fraud counts and magnitudes: US Federal Trade Commission Sentinel Data. Sample all 51 "states" from 2005-2019. 675 state-year observations in balanced panel.

- Model, Variables, and Tests: $y_{jt} = \beta_1 x_1 + \varrho_j + \tau_t + \varepsilon$ The y_{jt} is, the count of data breach events in state j, year t or the magnitude of data breaches (records) in state j, year t. The β_1 is the post-BNL effect on counts (rates) or on magnitudes (elasticities) and should be negative if BNLs work. The ϱ_j **and** τ_t are state j and year t fixed effects.

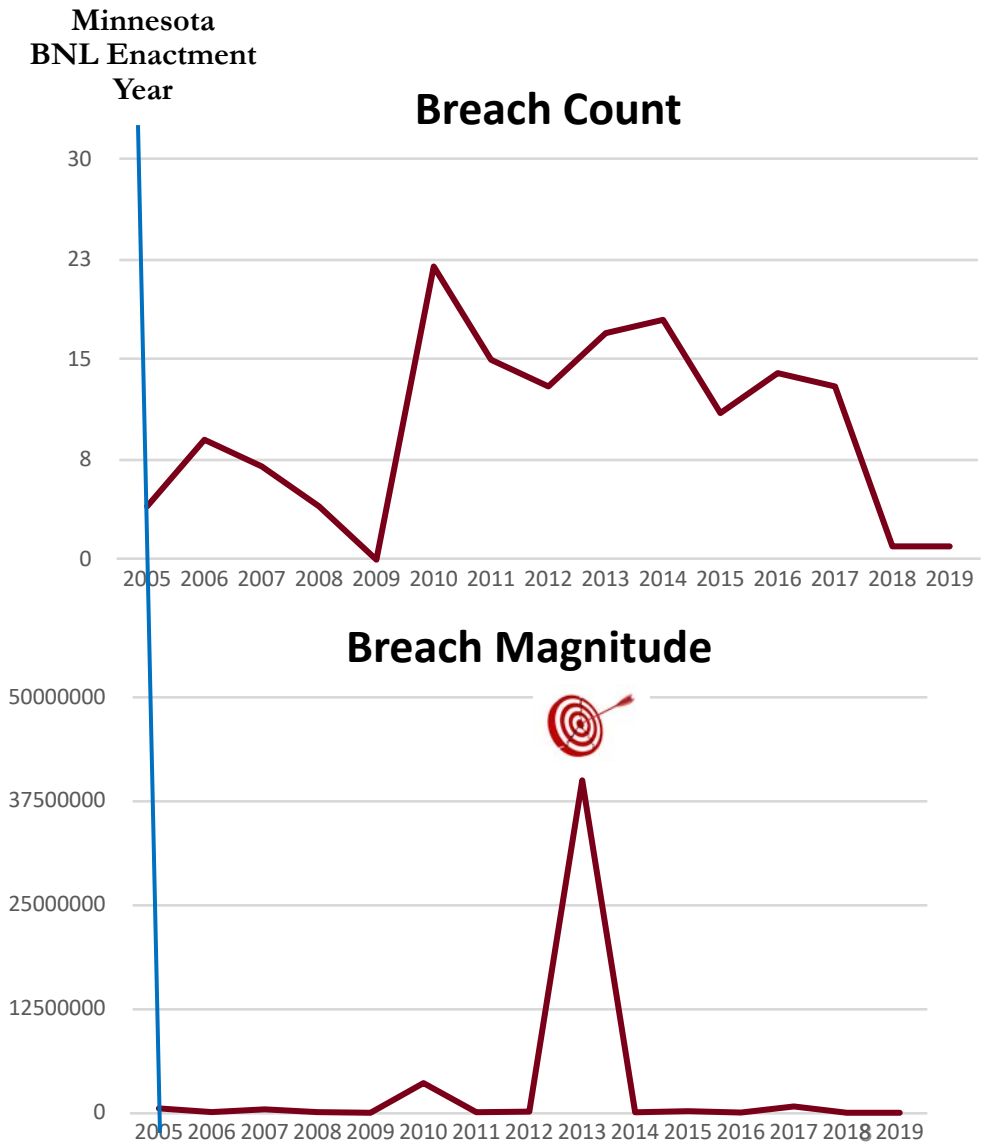


- Estimation Strategy: 2-way difference-in-difference fixed effects (DiD) approach. OLS (magnitudes) and QML Poisson (counts) estimation. Phased implementation based on when states enact BNLs from 2005-2018.

Some Descriptive Statistics and Minnesota's Example

- <u>Descriptive Data Breach Statistics (PRC)</u>:

1. Mean Count/Magnitude: 32/13.2M
2. Median Count/Magnitude: 5/36,972
3. Standard Deviation: 19/172M
4. Minimum Count/Magnitude: 0/0
5. Maximum Count: 189 (Maryland, 2014)
6. Maximum Magnitude: 4.5B (California, 2016)



Core Regressions: No Effects

	(1)	(2)	(3)	(4)
Dependent Variable	ln(Records)	ln(Records)	numEvents	numEvents
Estimator	Log-OLS	Log-OLS	Poisson	Poisson
Treatment	Any BNL	BNL w/ Private Right of Action (PROA)	Any BNL	BNL w/ PROA
Any BNL Enacted	0.258		-0.0349	
	(0.700)		(0.117)	
BNL w/ PROA Enacted		1.035		0.136
		(0.963)		(0.349)
State Fixed Effects	Yes	Yes	Yes	Yes
Year Fixed Effects	Yes	Yes	Yes	Yes
Observations	765	765	765	765
	0.543			
	51		51	
	Robust standa		entheses	
	*			

Coefficients are universally waaay insignificant

36% of a St Dev is 1.74 and 6.75

We are at less than 15% for MDEs except in Column 3

Pre-, Post-Treatment Trends: No Effects

	(1)	(2)	(3)	(4)
Dependent Variable	ln(Records)	numEvents	ln(Records)	numEvents
Estimator	Log-OLS	Poisson	Log-OLS	Poi
Treatment	Privacy Law	Privacy Law	PROA	P
Rel Time t-4+	-0.746	-0.168		
	(0.917)	(0.225)		
Rel Time t-4	-1.376	-0.0908	-5.878***	
	(1.320)	(0.188)	(1.654)	
Rel Time t-3	-0.184	-0.231	-1.219	-
	(1.234)	(0.162)	(2.881)	(
Rel Time t-2	-0.899	0.00651	-0.711	-
	(0.735)	(0.102)	(1.327)	(0.
	Omitted Periods To Avoid Dummy Variable Trap			
Rel Time t+1	0.189	0.128	-0.496	-0.106
	(0.619)	(0.136)	(1.173)	(0.2
Rel Time t+2	0.115	0.0115	0.764	-0
	(0.745)	(0.138)	(0.953)	(0.
Rel Time t+3	-0.384	-0.103	-0.510	-0
	(0.731)	(0.143)	(0.794)	(0.
Rel Time t+4	0.115	-0.0226	-0.924	-0.
	(0.873)	(0.168)	(1.311)	(0.
Rel Time t+5	-0.919	-0.0340	-0.677	-0
	(0.821)	(0.218)	(0.871)	(0.
Rel Time t+6	-0.0283	0.190	-0.763	0.
	(1.000)	(0.356)	(1.151)	(0.
Rel Time t+7	-0.185	0.0242	0.264	0.00136
	(1.105)	(0.224)	(1.235)	(0.216)
Rel Time t+8	-0.426	-0.0644	-1.264	-0.0
	(1.244)	(0.255)	(1.215)	(0.
Rel Time t+9	1.467	-0.0947	0.815	-0.
	(1.283)	(0.278)	(1.334)	(0.
Rel Time t+10	0.387	0.117	0.195	0.
	(1.373)	(0.292)	(1.466)	(0.
Rel Time t+10 +	-0.258	0.201	-1.318	0.
	(1.539)	(0.322)	(1.001)	(0.
State Fixed Effects	Yes	Yes	Yes	Y
Year Fixed Effects	Yes	Yes	Yes	Yes
Observations	765	765	765	763
R-squared	0.553		0.552	
Robust standard errors clustered on states in parentheses				
*** p<0.01, ** p<0.05, * p<0.1				

No persistent pre-treatment trends

Not a single point estimate breaks out 36% threshold

There are fewer significant items than chance would predict!!

Internal v. External Causes: No Effects

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Dependent Variable	ln(Records)	ln(Records)	numEvents	numEvents	ln(Records)	ln(Records)	numEvents	numEvents
Sample	Externally-Caused Data Breaches (e.g., Hack)				Internally-Caused Data Breaches (e.g., Employee Error)			
Estimator	Log-OLS	Log-OLS	Poisson	Poisson	Log-OLS	Log-OLS	Poisson	Poisson
Treatment	Any BNL	BNL w/ PROA	Any BNL	BNL w/ PROA	Any BNL	BNL w/ PROA	Any BNL	BNL w/ PROA
Any BNL Enacted	0.135		-0.0188		1.000		0.0957	
	(0.790)		(0.153)		(0.573)		(0.151)	
BNL w/ PROA Enacted		0.709		0.292		1.596		0.229
		(1.134)		(0.516)		(1.057)		(0.608)
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year Fixed		Yes	Y			Yes		
		765	7			765		
		0.458				0.492		
		51				51		
Robust standard						**entheses**		
***** p<0.01, ** p<0.05, * p<0.1**								

Coefficients are (again) universally waaay insignificant

No pre- or post-treatment trends

Other indicators of precisely-estimated null effects hold

BNL Effects on Downstream Data Misuse: Effects!!

	(1)
Dependent Variable	ln(ID Theft)
Estimator	Log-OLS
Sample	2005 - 2010
Treatment	Any BNL
Any BNL Enacted	-0.0514*
	(0.0211)
State Fixed Effects	Yes
Year Fixed Effects	Yes
Observations	306
R-squared	0.997
Number of Groups	51
Robust standard errors clustered on states in parentheses *** p<0.01, ** p<0.05, * p<0.1	

Maybe BNLs were instead meant to deter "downstream" data misuse by malicious actors…

Romanosky *et al.* (2011) found evidence of that in early BNL enactments (2000s)

Okay, so we can replicate their results using FTC Sentinel data on ID Theft magnitudes

BNL Effects on Data Misuse: No Effects in the Longer Run

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	
Dependent Variable	ln(ID Theft)	ln(Fraud)	numTheft	numFraud	ln(ID Theft)	ln(Fraud)	numTheft	numFraud
Estimator	Log-OLS	Log-OLS	Poisson	Poisson	Log-OLS	Log-OLS	Poisson	Poisson
Treatment	Any BNL	Any BNL	Any BNL	Any BNL	BNL w/ PROA	BNL w/ PROA	BNL w/ PROA	BNL w/ PROA
Any BNL Enacted	-0.0289	-0.0111	-0.0539	0.174*				
	(0.0274)	(0.0572)	(0.0654)	(0.0745)				
BNL w/ PROA Enacted					-0.0316	-0.124	0.0206	-0.129
					(0.0514)	(0.121)	(0.0730)	(0.0834)
State Fixed Effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year Fixed		Yes		Yes	Yes			Yes
		765		765	765			765
		0.975			0.98			
		51		51	51			51

Then, we can show that negative BNL effects on ID theft (and fraud) do not persist over longer term: 2005-2019

BNL enactment may prompt more (not less) fraud (Column 4).

Other indicators of precisely-estimated null effects hold

Consistent Non-Effects on Breach Counts & Magnitudes

1. In early years (2005-2010, 2005-2015).
2. Smaller, less-insured, locally-operating firms
3. After state data security and disposal laws were enacted.
4. When considering other BNL characteristics: Access Trigger, Acquisition Trigger, Individual Notification, Owner Notification, AG Notification.

However we try to partition the data, we keep coming up with no BNL enactment effects.

The same indicators of precisely-estimated null effects hold.

If BNLs are all for naught, then we should ask two questions: Why? and What do we do?

Remember How BNLs Should Work

- BNL enactment itself should decrease data breaches…and right away:

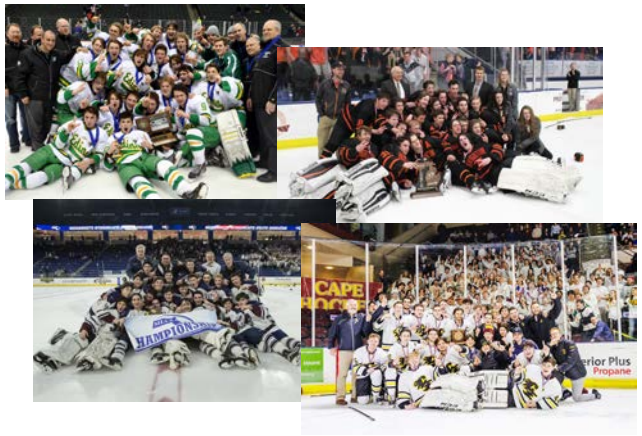
1. Impose breach search, notification, and mitigation costs on firms.
2. Impose fines as well as public and private liability for untimely notification.
3. Put public officials (*e.g.,* State AG) and residents on notice.

- BNL enactment should prompt broader market developments that decrease data breaches…in the long run (Becker, 1968):

1. See development of data security, breach surveillance, and breach mitigation standards in firms.
2. Let firms position themselves in a "market for data privacy."
3. See development of consumer-accessible information on how firms are doing in their market position.
4. Let consumers choose firms based on their own preference for data security versus cost.

State BNL Standards Are Inconsistent

- Tom (2010: 1570) describes BNL variation as "so numerous that it is virtually impossible to convert these state laws into the more manageable format."



State	BNL Year	Notification Trigger	No Harm Exception	Individual Notification	Owner Notification	AG Notification	PROA
Minnesota	2005	Acquisition	No	Yes	Yes	No	Yes
Michigan	2007	Access	Yes	Yes	No	No	No
Massachusetts	2007	Acquisition	No	Yes	Yes	Yes	No
Maine	2006	Misuse or Risk of Misuse	Yes	Yes	Yes	Yes	No

Consistently great high school hockey. Inconsistent BNL standards

BNL Information Is Insufficient

March 2021 leak and then hack of PII for 3 million VWA owners and potential owners. Records for up to 90,000 of them were being sold on dark web (*e.g.*, "Tor" network).

51 "states"

19 States With Web Searchable Archives

Hawaii, Maryland, Montana, Oklahoma, Oregon, Texas, Washington.

No mention of VWA leak and hack

Single line item listing the date notification was sent (June 11, 2021), number of state residents affected (875), and "total" number individuals affected (90,184).

Maybe the "best" BNL website with incident description, dates, letters sent by VWA.

California, Delaware, Iowa, Indiana, Maine, Maryland, Massachusetts, New Hampshire, North Dakota, New Jersey, Vermont.

Notes the incident but varying detail…

Paragraph describing the incident and then a hyperlink to the ***State of Maine's*** BNL website for details.

BNL Information Is Untimely and Insufficient

March 2019 hack of PII for more than 100 million Capital One customers: accounts and credit card applications.

Minn. Stat. § 325E.61 and 325E.64: [D]isclosure must be made in the most expedient time possible and without unreasonable delay…

Capital One hires Debevoise & Plimpton law firm to manage breach response…

Debevoise & Plimpton

Debevoise & Plimpton law firm hires breach response firms

- Computer Engineering Firm
- Cyber-Security Firm
- Public Relations Firm

Interim and final reports go through Debevoise & Plimpton law firm where they may be edited prior to sharing with key Personnel at Capital One: top management team, corporate board, select IT personnel.

ATTORNEY-CLIENT PRIVILEGED

Reports and related materials are covered by attorney-client privilege and/or attorney work product defendable from disclosure to state insurer and regulator.

How to Make BNLs Work: Replace State w/ Federal Regime

- A national BNL regulatory regime for a national (international) policy challenge:

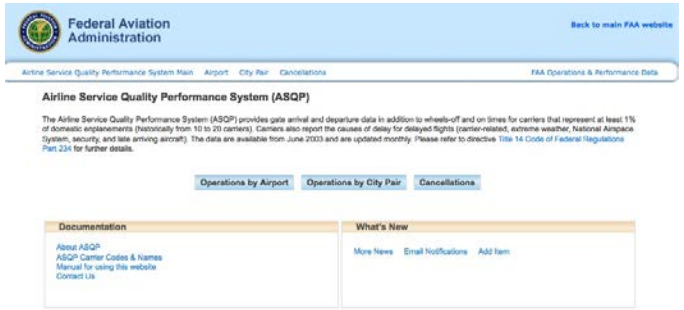
1. Vested in an agency with standards-setting, information disclosure, and law enforcement experience and expertise: SEC, FTC.

2. General expert body and industry-specific expert bodies to advise on standards setting and revision: SEC (and maybe) FTC.

3. Consumer- and analyst-accessible information on firm data security, breach history, mitigation efforts like the FAA has: (who knows with SEC or FTC).

4. Cyber incident response privilege, evidentiary admissibility limits on previous measures to limit/respond to breaches.

Presented by Advisory Board Subject Matter Experts



How to Make BNLs Work: Reform State Regimes

- A state BNL regulatory regime for a national (international) policy challenge:

1. Vested in an agency with standards-setting, information disclosure, and law enforcement experience and expertise: State Attorney General.

2. General expert body and industry-specific expert bodies to advise on standards setting and revision: SEC (and maybe) FTC.

3. Consumer- and analyst-accessible information on firm data security, breach history, mitigation efforts: State AG's Consumer Protection Division.

4. Cyber incident response privilege, evidentiary admissibility limits on previous measures to limit/respond to breaches.

5. Experimentation in 50 (51) state "laboratories" for best practices.

Presented by Advisory Board Subject Matter Experts

Maybe the "best" state BNL website with incident description, dates, letters sent by breached firms.

Take Aways From the Talk

- **Key Research Findings**: 1) State BNLs reduce neither breach counts nor breach magnitudes; 2) BNLs reduce neither downstream ID theft/fraud counts nor downstream ID theft/fraud magnitudes. BNLs don't work.

- **How to Make BNLs Work**: 1) Give consumers (and analysts) consistent BNL standards and sufficient, timely information to create markets for data security where firms can position themselves; 2) a single federal BNL replacing state BNLs can do so, but Congressional action is unlikely; 3) reforming existing state BNLs to include searchable archives, revised privilege and evidentiary rules governing breach response and disclosure, vested in a competent state agency can also do so…in time.

- **Some Federal Agencies and State Governments Seem Open to These BNL Reforms**: 1) The SEC at the federal level and states with strong consumer protection traditions and unified government (*e.g.*, Minnesota); 2) There is a consensus across public, private, and civil society sectors that the time for action is now.

- **That's Why I'm Here Today**: You and your organizations are key to making this happen…perhaps with a little evidence from the Academy!

CARLSON SCHOOL OF MANAGEMENT
UNIVERSITY OF MINNESOTA

Law School

UNIVERSITY OF MINNESOTA
Driven to Discover℠

State Breach Notification Laws Aren't Working… But They Could

Paul M. Vaaler
Law School & Carlson School of Management
University of Minnesota

Thanks

And Go Gophers. Beat the Spartans!

Paul M. Vaaler (vaal0001@umn.edu
13th Annual Cybersecurity Summit
Double Tree Hotel, Bloomington, MN
October 24-26, 2023
3:00-3:30pm
Ballroom