Exploring The Impact Of The 2018 Data Breach Notification Act

Sarah S. Glover
Brandon N. Robinson

ALABAMA STATE BAR
142nd Annual Meeting
POINT CLEAR, ALABAMA

IT DOESN’T MATTER HOW HIGH YOU BUILD THE CASTLE WALLS …

ALABAMA'S NEW DATA BREACH NOTIFICATION ACT

- Went into effect on June 1, 2018
- 50th state to pass one (right behind South Dakota
- All 50 states and U.S. territories now have a similar statute—they **apply according to the residence of the impacted individual**
- Applies to all "covered entities"—<u>any business</u> that acquires or uses **sensitive personally identifying information** on an Alabama resident (customer and/or **employee**) as well as "third party agents"—entity that has been contracted by a covered entity to process sensitive personally identifying information

ALABAMA'S NEW DATA BREACH NOTIFICATION ACT (cont'd)

- Limited exceptions for regulated entities (e.g., financial institutions, health care)
- No private right of action (does not mean that data breach lawsuits are foreclosed in Alabama)

ALABAMA'S NEW DATA BREACH NOTIFICATION ACT (cont'd)

Implement and maintain reasonable information security measures (including records disposal)

Investigate security breaches

Notify (as applicable) impacted individuals, Alabama A.G., and consumer reporting agencies within 45 days

WHAT INFORMATION IS COVERED

- “Breach of security” or “breach” means “unauthorized acquisition of data in electronic form containing [SPII].” Multiple instances by the same source constitutes one breach
- Only covers information in electronic form
- Does not include lawfully public information or encrypted information

ALABAMA'S "REASONABLE" SECURITY MEASURES

- Designate an individual(s) to coordinate the covered entity's security program
- Identify internal and external security risks
- Adopt appropriate security safeguards and assess effectiveness of such safeguards
- Use vendor contracts that require vendors to maintain appropriate safeguards
- Evaluate and adjust security measures to account for changes in circumstances that impact security
- Keep executive management informed about the covered entity's security program

ENFORCEMENT

- Exclusively enforced by the Alabama Attorney General's office; no private right of action
- A violation of the notification provisions of the Act shall be deemed an unlawful trade practice under the Alabama Deceptive Trade Practices Act
- A knowing violation of the notification provisions shall be subject to a civil penalty of up to $500,000 per breach
- Other violations shall be subject to a civil penalty of not more than $5,000 per day for each consecutive day that the covered entity fails to take reasonable action to comply with the notice provisions of the Act

ENFORCEMENT (cont'd)

- The Attorney General can also bring an action for damages on behalf of any named individual or individuals—damages are limited to actual damages suffered plus reasonable attorney's fees and costs
- The civil penalties apply equally to covered entities as well as third party agents. Government entities are subject to notice requirements, but exempt from civil penalties

PENALTIES

- Any covered entity or third-party “knowingly” (willfully or with reckless disregard) engaging in a violation of the notification provisions will be subject to penalty provisions in the ADTPA (8-19-11), which establishes civil penalties of not more than $2,000 per violation. These penalties may not exceed $500,000 per breach
- Notwithstanding that penalty, a covered entity that “violates the notification provisions of this act” shall face penalty of no more than $5,000 “per day for each consecutive day that the covered entity <u>fails to take reasonable actions to comply with the notice provisions of this act</u>.” (46th day?)

EXEMPTIONS

- The Act does NOT <u>expressly</u> exempt entities otherwise subject to GLBA, HIPAA, etc. (like some states do)
- It does state that an entity subject to or regulated by federal laws/regs on data breach notification established or enforced by the federal government is exempt so long as they:
  - Maintain procedures pursuant to those laws, rules, etc.
  - Provide notice to affected individuals pursuant to those laws, rules, etc.
  - Timely provide a copy of the notice to the A.G. when the number of individuals exceeds 1,000
- Similar provisions exist for those subject to or regulated by state laws, rules, etc.

CONSUMER NOTICE

Written notice (mail or email) must include the following content:	
Date, estimated date, or estimated date range of breach;	Description of SPII acquired
General description of actions taken to restore security/confidentiality	General description of steps an individual can take to protect himself or herself from ID theft
Information the individual can use to contact the covered entity to inquire about the breach	

- If notice not required, entity shall document and maintain for at least five years

SUBSTITUTE NOTICE

- Website, print/broadcast media, etc., in lieu of individual notices; or alternative method approved by the A.G.
- Substitute notice allowed if either:
  - Excessive costs relative to resources of covered entity (safe harbor of $500,000)
  - Lack of sufficient contact for the individual required to be notified
  - Affected individuals exceed 100,000 persons

A.G. NOTIFICATION

- If >1,000 individuals affected, covered entity must notify A.G.
- “as expeditiously as possible and without unreasonable delay” but within 45 days of receipt of notice from third party agent or covered entity’s determination of both breach and reasonable likelihood of substantial harm

CONTENT OF A.G. NOTIFICATION

- **Covered Entity** – name, type, size (employees, gross revenue, SPOC)
- **Dates and Notices** – date when breach determination made, upload determination of no notification; if notification, then date of notification, number of residents notified, sample notification
- **Notification** – what was included in notification whether substitute notice provided and how; whether CRA notice provided

CONTENT OF A.G. NOTIFICATION (cont'd)

- **Scope of breach and investigation:**
  - Synopsis including # of affected residents, services offered, etc.
  - Assessment of covered entity—type of info collected, description of reasonable security measures
  - Facts about investigation—date investigation began, did it include assessment of nature and scope, identification of sensitive PII, measures to restore security and confidentiality, indications of outside physical possession, indications of information download or copies made

CONTENT OF A.G. NOTIFICATION (cont'd)

- **Scope of breach and investigation (cont'd):**
  - Indications information used by unauthorized persons (e.g., identity theft)
  - Whether information has been made public
- **Third-Party Agent Notification**
  - If third party notification, what date, copy of notice, when third party became aware, copy of contract with third party
- **Certification with Electronic Signature**
  - Certify accuracy and truthfulness of notification
  - Penalty of not more than $5k/day for each consecutive day the covered entity fails to take reasonable action to comply with the notice provisions of this act.

CONTENT OF A.G. NOTIFICATION (cont'd)

- **Covered entity may update or supplement at any time**
- **Information marked confidential not subject to open records or other disclosures**

CONSUMER REPORTING AGENCY NOTIFICATION

- If >1,000 individuals affected, entity shall notify “all consumer reporting agencies that compile and maintain files on consumers on a national basis, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a), of the timing, distribution, and content of the notices.
- 15 U.S.C. 1681a(f): “consumer reporting agency” means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports

THIRD PARTY NOTIFICATION TO COVERED ENTITY

- "third party agent": "an entity that has been contracted to maintain, store, process, or is otherwise permitted to access sensitive personally identifying information in connection with providing services to a covered entity."
- If a 3rd party agent experiences a breach in the system maintained by the agent, it must notify the covered entity "as expeditiously as possible and without unreasonable delay" but no later than **10 days** following determination of the breach or reason to believe a breach has occurred
- A covered entity may contract with third party to handle notifications required under this Act.

OTHER "REQUIREMENTS"

- The Act also contains other requirements apart from notification
  - Sec. 3: requires "reasonable security measures" with suggestions on what those should consider as well as what assessment of those measures should emphasize and consider
  - Sec. 4: requires "good faith and prompt investigation" that includes certain features
  - Sec. 10: requires records disposal requirements

However, <u>enforcement is limited to notification violations</u>. It remains to be seen how these provisions are used from an enforcement standpoint

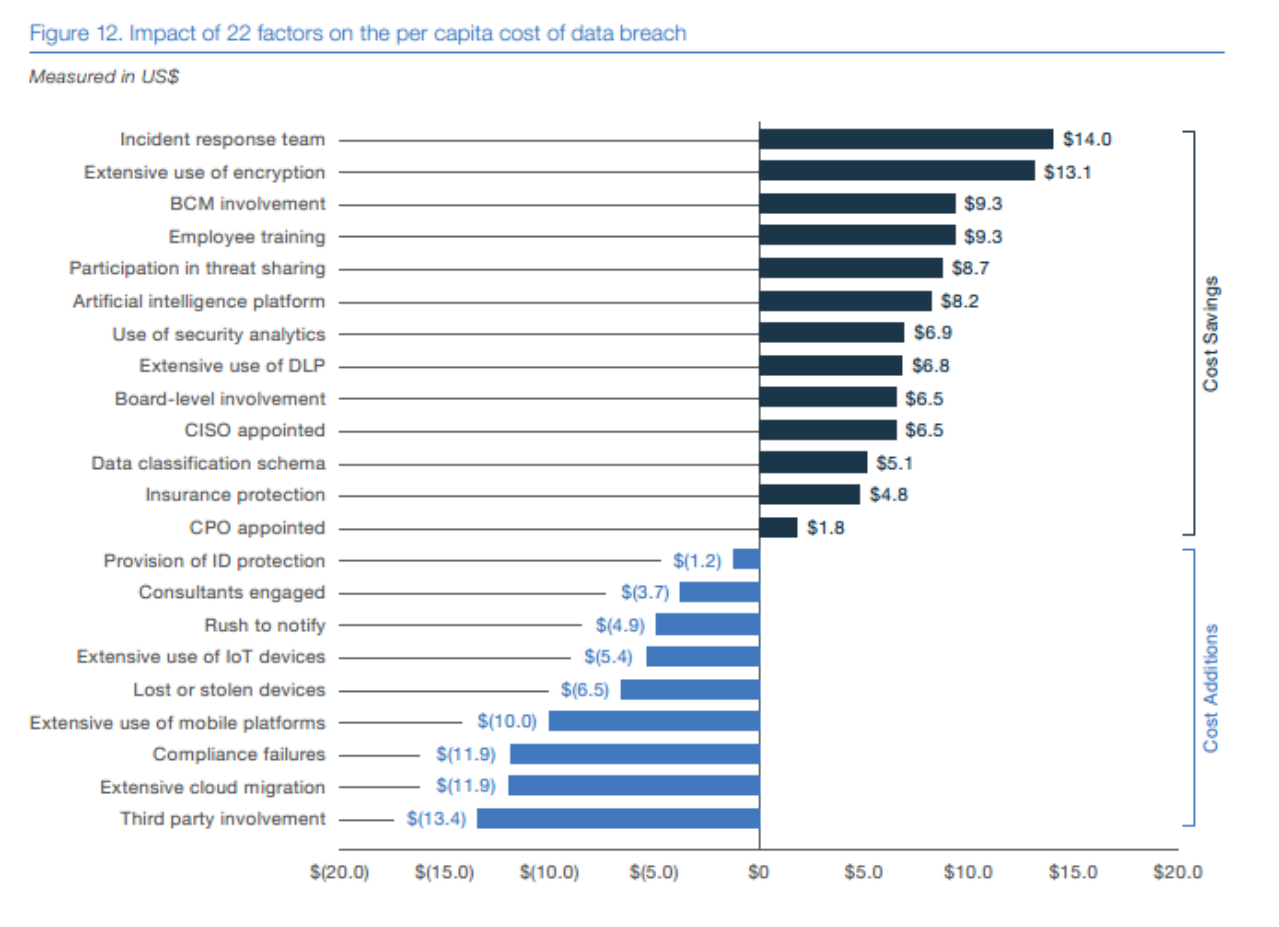
OPEN QUESTIONS

- How penalties work together – limited $2,000 vs. unlimited $5,000
  - $5,000 kick in on 46th day?
  - Is $5,000 reserved for more egregious actions?
  - Will other requirements be used as “reasonableness” factors in determining application of $5,000 penalities?
- Yet to see an enforcement action (although A.G.O. received $2M/$148M from Uber settlement)
- Exemption conditions – who decides?
- There remains room for interpretation in some areas, and thus, for advocacy as well when needed

TAKEAWAYS

- Consider “other requirements” as part of building your cyber-security posture
- Be mindful of 10/45 day clock and when it is triggered (note third party agent distinction regarding “substantial harm”)
- If non-AL residents affected, other state notification laws may apply
- Also check contracts, insurance policies for other notification requirements that may be <45 days

COST OF A DATA BREACH



Avg. cost per record = $148

Ponemon Institute 2018 Cost of a Data Breach Study

WHAT TO DO BEFORE A BREACH

- Create an Incident Response Team
- Inventory data; create a plan
- Create/review policies and procedures
- Train employees on policies and procedures as well as on good info, government practices (passwords, phishing, etc.)
- Maintain a good relationship with law enforcement
- Consider cyber insurance; review your policies
- Vendor management

VENDOR MANAGEMENT LIFE CYCLE

Phase 1: Due Diligence

- Assess risk based on access to data
- Evaluate information security practices
- Assess financial soundness

Phase 2: Contract Negotiation

- Specify safeguards
- Seek adequate allocation of responsibility and liability
- Require indemnification for data breaches

Phase 3: Ongoing Monitoring

- Conduct routine audits
- Monitor access and use of systems and data
- Evaluate whether changes in the law necessitate changes in the contract

OPPORTUNITIES: WHAT TO DO AFTER A BREACH

- *HOPEFULLY* – activate your Incident Response Team and implement your plan. If not . . . Some rules of thumb:
  - Engage legal counsel (attorney/client work product, privilege) – can be in-house or outside
  - Investigate immediately – identify source and compromised data, restore system integrity
  - Control the story – communicate internally and externally, as promptly and accurately as possible ("art of the statement"). Review for notification obligations (AL data breach law, contracts, insurance policies)

OTHER LAWS TO BE AWARE OF OR ON THE HORIZON

- **GDPR**
  - Became effective May 25, 2018, so already in effect
  - 72-hour notification requirement
  - Can apply in some circumstances even to U.S. companies without E.U. presence ("offering goods or services" or "monitoring behavior")
  - All sort of data subject rights and obligations as a "controller" or "processor"
- **California Consumer Privacy Act (CCPA)** – like GDPR, goes into effect in January 2020
- **Potential Federal Privacy Laws** – may preempt state laws, being pushed in Senate (Google, Facebook, etc.)
- **New York Privacy Act**
- **State adoptions of the NAIC Insurance Data Security Model Law**

CONCLUSION

- Handling data and potential data breaches are among the greatest risks faced by businesses
- Although many breach notification laws contain similar language, the definition of a breach and the proactive and reactive duties related to a breach response vary depending on the affected individual's state of residence
  - One-size-fits-all approach to notification will not suffice
- States are responding with increasingly frequent and divergent changes to their statutes
- Businesses must be proactive in addressing these risks and make it a priority to monitor changes to prepare for and respond to data breaches

QUESTIONS?

Sarah S. Glover, CIPP/US
Tel: (205) 254-1877
Email: sglover@maynardcooper.com

MAYNARD, COOPER & GALE
Alabama | California | New York | Washington D.C.

Cybersecurity & Privacy Practice Group

Brandon N. Robinson, CIPP/US
Tel: (205) 226-3427
Email: bnrobinson@balch.com

BALCH & BINGHAM LLP
Alabama | Florida | Georgia | Mississippi | Washington D.C.

www.dataprivacyandsecurityobserver.com

Appendix - Alabama’s Law Compared To Those In Adjacent States

COMPARISON WITH ADJACENT STATES

States	State Agency	Timing of Notice	Affected Individual Threshold	Encryption Safe Harbor / Other Exemptions
AL	Attorney General (Ala. Code § 8-19F-6)	Notice must be provided as expeditiously as possible, but no later than 45 days if the notification was received from a third party agent	1,000	• Statute not applicable if the personal information is encrypted or redacted • Exemption for good faith acquisition
FL	Department of Legal Affairs (Fla. Stat. § 501.171)	Notice must be provided no later than 30 days after determination of a breach or reason to believe a breach occurred	Attorney General Notification: 500 Credit Reporting Agencies: 1,000	• Encryption Safe Harbor • Exemption for good faith acquisition and entities in compliance with federal regulator
GA	The statute does not require notice to any governmental or regulatory agencies	Notice must be provided as expeditiously as possible and without unreasonable delay	Credit Reporting Agencies: 10,000	• Encryption Safe Harbor • Exemption for good faith acquisition and entities in compliance with its own notification procedures
MS	The statute does not require notice to any governmental or regulatory agencies	The insurance statute requires licensees to notify the MS Commissioner of Insurance no later than 3 business days after discovering the event	The statute does not require notice to any governmental or regulatory agencies or credit reporting agencies	• Encryption Safe Harbor
TN	The statute does not require notice to any governmental or regulatory agencies	Notice must be provided no later than 45 days after determination of a breach or reason to believe a breach occurred	Credit Reporting Agencies: 10,000	• Encryption Safe Harbor • Exemption for good faith acquisition and entities in compliance with its own notification procedures

COMPARISON WITH ADJACENT STATES

States	Notification Requirements	Private Right of Action	Regulatory Enforcement	Encryption Safe Harbor / Other Exemptions
AL	• Analysis of risk of harm • Substitute notice available	The statute does not provide for a private right of action	The attorney general enforces that statute under the Deceptive Trade Practices Act	No other key provisions
FL	• Analysis of risk of harm • Substitute notice available • Can be triggered by access	The statute does not provide for a private right of action	The Department of Legal Affairs may bring an action to enforce the statute as an unfair or deceptive trade practice	A public records exemption that limits the disclosure of information during the investigation
GA	• Substitute notice available	The statute does not provide for a private right of action	The statute does not provide for regulatory enforcement	No other key provisions
MS	• Analysis of risk of harm • Substitute notice available	The statute does not provide for a private right of action	The Mississippi Attorney General may enforce a breach of the statute as an unfair trade practice	No other key provisions
TN	• Analysis of risk of harm • Substitute notice available	A violation of the statute may also be a violation of the Tennessee CPA, which provides a private right of action	The Tennessee Attorney General may seek injunctions and recover attorneys' fees	No other key provisions

COMPARISON WITH ADJACENT STATES

States	Substitute Notice Requirements

AL	• Allows if the covered entity shows one of the following:
	  • The cost of providing notice would exceed $500,000 or is excessive relative to the covered entity's resources
	  • The affected class to notify exceeds 100,000 Alabama residents
	  • The notifying person lacks sufficient contact information

FL	• Allows if the covered entity shows one of the following:
	  • The cost of providing notice would exceed $250,000
	  • The affected class to notify exceeds 500,000 persons
	  • The covered entity lacks mail or email addresses for affected persons

GA	• Allows if the covered entity shows one of the following:
	  • The cost of providing notice would exceed $50,000
	  • The affected class to notify exceeds 100,000 Alabama residents
	  • The covered entity lacks sufficient contact information to provide written or electronic notice

MS	• Allows if the covered entity shows one of the following:
	  • The cost of providing notice would exceed $5,000
	  • The affected class to notify exceeds 5,000
	  • The covered entity lacks sufficient contact information

TN	• Allows if the covered entity shows one of the following:
	  • The cost of providing notice would exceed $250,000
	  • The affected class to notify exceeds 500,000 residents
	  • The covered entity lacks sufficient contact information