Cybersecurity Law Report
An Acuris company

cslawreport.com

June 9, 2021

STATE ATTORNEYS GENERAL

State AGs Share Breach Notification Tips and Latest Enforcement Concerns

By Matt Fleischer-Black, *Cybersecurity Law Report*

The offices of state attorneys general (AGs) have assumed an active role in data breach and privacy enforcement. They worked together in 2020 and 2021 on several multistate settlements and have obtained greater authority over routine cybersecurity, with at least 25 states now mandating reasonable security efforts. Privacy and security leaders from six state AGs recently discussed their views about the thousands of breach notifications they field each year and suggested how companies can best navigate the enforcement process.

Speaking at International Association of Privacy Professionals (IAPP) and Practising Law Institute (PLI) events, the regulators also described their approaches to investigations, their top enforcement concerns and recent changes in their regulatory powers and resources. This article also includes commentary from state AG practice specialists at Cozen O'Connor.

See "Steps to Protect Privilege for Data Breach Forensic Reports" (Jan. 27, 2021).

How to Approach Breach Notification Issues

Navigate the States' Portals and Forms

The 54 states and territories have many variations in their notification requirements for companies to address. Now, many states require companies to report incidents through web portals and idiosyncratic forms.

New York's mandatory portal has the benefit of automatically notifying other agencies in the state, explained Deputy AG Clark Russell during a recent PLI discussion. He advised companies to stop sending his office courtesy hard copies. For supplements or updates later in the investigation, he suggested that companies send an email message.

Connecticut's forthcoming form will have required fields, so breached companies will have to use it instead of emailing letters, said Deputy Associate AG Michele Lucan.

More forms now go beyond basic questions about the breach discovery and response, asking detailed questions about "the overall security program, specific technical controls, risk assessments, use of third parties" and even include contracting requirements, Cozen O'Connor partner Ann-Marie Luciano told the Cybersecurity Law Report. Provisions in recent AG multistate settlements address some or all of these elements, she noted.

See "Eight Data Security Best Practices Revealed by Recent AG and FTC Enforcement Actions" (Jan. 8, 2020).

Do Not Leave the AG Stuck Without an Answer

Matthew Van Hise, Chief of the Illinois AG's Privacy Unit, speaking at the IAPP panel, reminded companies that their breaches also pose a risk for front-line regulators like himself: being caught unaware when the AG calls to demand details that Van Hise does not have. To satisfy the boss, "it is important for us to have an adequate picture of where things are going – a road map for a process forward that can be quickly described," he said.

His Massachusetts counterpart, Data Privacy and Security Chief Sara Cable, agreed that early outreach is "hugely helpful" if a company is set to announce the breach or the incident might draw media coverage. "A heads up call giving me the bare bones information, even ten minutes before that press announcement is made, even when you are not sure if notification is legally required, sends a message to the AG that your client or company is trying to do the best it can and not make the situation worse for the consumer," Cable said.

Cable is open to companies' informal outreach, whether phone calls or emails. "I take a pragmatic approach. These investigations are dynamic. I understand they take a long time" and that the company may want to limit what it says until it knows more.

States' standardized forms do help lawyers move more quickly through the necessary notifications in time, Cozen partner Lori Kalani told the Cybersecurity Law Report, but "an early phone call provides the AG's office that extra context" and lets it ask questions.

Conversations about the details also help the AG when consumers call about the breach. Answering individuals occupies a significant portion of the office's time, said Florida Deputy AG Gregory Sadowski. If the AG contacts companies after a notice, "most of the time, it is just to get information so that we can tell consumers what's going on," which almost always pacifies them, Sadowski said.

See "How to Avoid Common Mistakes and Manage the First 48 Hours Post-Breach" (Jun. 22, 2016).

Streamline Notification to Avoid 50 Calls

The state AG offices now collaborate closely on cybersecurity and privacy, so reaching out early to one with fast-breaking incidents may help satisfy a larger group of regulators, noted Illinois' Van Hise. He coordinates the Privacy Working Group of the National Association of Attorneys General (NAAG), which comprises "approximately 200 Assistant Attorneys General across the country that come on collective phone calls, share collaborative ideas and efforts, discuss nationwide concerns, and share information pertaining to breach notifications that they received," he explained.

New York's Russell suggested reaching out to an active office or to Van Hise, who can send an email through NAAG to all 50 states. At this stage, AGs' main goals are to weigh how seriously the company is investigating and to gauge its cooperativeness, Russell said.

Van Hise's team receives over 2500 notifications a year, while Connecticut expects 1500 in 2021, Lucan said. Reaching out by phone almost always is fine, but definitely make the phone call when the breached company is publicly traded, has a name brand, the breach affects customers in many states,

or the exposed information is sensitive or extensive, Cozen O'Conner partner Meghan Stoppel, a former Deputy AG in Nebraska, told the Cybersecurity Law Report.

See "Learning From the Equifax Settlement" (Jul. 31, 2019).

Do Not Hedge in Consumer Notices

When a company explains satisfactorily how it notified consumers and what steps it took to protect them in the wake of a breach, the AG may not feel a need to follow up, Lucan said.

The New York AG is looking out for hedging language on companies' breach alerts to consumers, said Russell, who drafted the New York SHIELD law. When the company learns that customer data is on the dark web or was exfiltrated, its notice must state that fact and avoid vague catchall wording like "your data may have been exposed," Russell cautioned.

As consumer protection is the AGs' overarching goal, Florida's Sadowski said, in discussions with companies, the office will focus on any vulnerabilities that the company mentions in a notification.

Companies would be wise to fully own up to the technical vulnerabilities, Lucan suggested. "We are getting very watered down notices that can only guarantee follow up," she warned, noting that the AGs need to see a complete picture of the case before they will close it. Her team suspects that some companies have been skimping on information to conceal that employees failed to respond appropriately or that the company did not dedicate enough resources to responsibly tackle the breach. These kinds of omissions inspire the AG to follow up further.

Delays in sending notices to consumers or the office are a key red flag for the AGs, noted Lucan. With many breaches, companies say that law enforcement requested a delay in telling the AG or consumers, Russell reported, but New York's AG prefers that companies back that up with a note from law enforcement.

AGs are sure to follow with questions when a breach affects minors, Sadowski added.

See "How to Approach CCPA's Under-16 Opt-In Consent" (Feb. 12, 2020); and "Balancing Legalese and Simplicity in Modern Privacy Policies" (May 5, 2021).

Save Information for a Supplemental Letter

Many states now publish breach notifications on a website or after open records requests, Stoppel said, putting the company's dirty laundry into public view. One good practice is to answer tersely on the official form and share more sensitive or embarrassing details in a supplementary letter, Stoppel said. "That allows the AGs to do what they normally do, which is link to the form on their website. But they don't always publish the company's attachment," Stoppel observed.

In the race to fill out the forms, companies must also avoid naming employees or other individuals at risk, Stoppel urged. "If an employee was responsible for the breach, don't publicly expose her in that form. Put 'current employee' or 'available on request,'" she said.

See "Learning From the 'Holes' in Dunkin's Security to Mitigate Brute-Force Attacks" (Sep. 30, 2020).

Multistate Cooperation Growing

A multistate task force can be daunting for a company because it indicates serious engagement by regulators and potentially high stakes, said Hunton Andrews Kurth partner Lisa Sotto during the PLI panel. More positively, AG multistate actions provide a central place to organize the action, and usually draw state regulators familiar with the issues, she noted.

A Series of Settlements With More Than 25 States

Multistate partnerships are a crucial resource for the offices, Connecticut's Lucan said, allowing AGs to stretch small staffs and cope better with the volume of notifications.

The number of multistate AG probes on cybersecurity and privacy cases has increased. Since October 2020, multistate AG task forces reached at least five breach settlements over $1 million with companies. Each involved at least 25 states. In a December 2020 action, CafePress paid $2 million to settle an action that seven AGs brought over exposure of consumer PI and credit card and social security numbers.

A former privacy chief in the New Jersey AG office, Frankfurt Kurnit Klein Selz associate Elliot Siebers, noted that the efforts show how "the patchwork of state laws can come together and work in a streamlined manner." Regulators working together on dozens of investigations have made "the process itself highly organized, structured and effective" at moving the investigation to a fair resolution, contended Van Hise.

See "The Growing Role of State AGs in Privacy Enforcement" (Nov. 28, 2018).

Joining Arms With the FTC

The U.S. Supreme Court, in the AMG case, recently ended the FTC's ability to seek financial penalties for most matters. Collaborating with state AGs gives the FTC a way to leverage civil penalties and other state powers. On May 11, 2021, FTC Acting Chair Rebecca Slaughter said at NAAG's consumer protection meeting that the FTC intends to coordinate and collaborate more often with the AGs, recounted Luciano.

Kristin Cohen, Assistant Director of the FTC's Division of Privacy and Identity Protection, said that working alongside the AGs on the lawsuits has allowed the FTC to create remedies that best protect U.S. consumers. Cohen praised the effectiveness of the FTC's prior AG collaborations.

The FTC will seek to work with the home state AG for the company to take advantage of the state and federal jurisdiction, noted Stoppel. For collaborative actions, the FTC will also look at the strength of a state's consumer protection statute, she said. "Does it have a powerful tool and a history and the ability to wield it effectively for consumers nationwide?"

See "So, You Just Got a Letter From the FTC: A Guide for Attorneys" (Jan. 20, 2016).

Prompts for AGs Going to Court Alone

On occasional multistate cases, AGs head back home to file a case. Despite Facebook's $5-billion settlement in July 2019 with the FTC over alleged deception tied to Cambridge Analytica, the New Mexico and D.C. AGs continue to press

lawsuits against Facebook for privacy violations. "The company's conduct violated our laws and it impacted about half of the district residents," explained D.C. Privacy Section Chief Benjamin Wiseman. After defeating Facebook's motion to dismiss, his AG is now conducting discovery, he said.

Equifax settled with the FTC and 50 state and territorial AGs over its 2017 breach and for failure to maintain reasonable cybersecurity, paying $700 million. Yet, Massachusetts separately sued Equifax, to create case law for its pioneering data security statutes. "We have a responsibility to vindicate Massachusetts law," Cable said. "We wanted to get accountability as fast as possible," and a lengthy investigation was not needed as Equifax had clearly violated the state law. The state and company settled for $18 million in 2020.

See "Massachusetts Breach Notification Law 2.0: More Protections for Consumers, More Requirements for Businesses" (Jan. 23, 2019); and "Implications of Nevada's New Privacy Law" (Jul. 10, 2019).

AGs Want Expanded Notification Triggers

AGs are pursuing new powers, which then may prompt a showcase action in state court as happened in Massachusetts. Some states have updated their breach notification laws to include more triggering elements, like medical information, online credentials and biometric data, Lucan explained. On June 7, Connecticut's legislature approved an update for the governor to sign.

Biometric information is a key trigger for AGs because the technology is sure to replace usernames and passwords for authentication, Russell said.

AGs are also pushing to expand the notification trigger, from "acquisition" of data to "access." The New York Shield Law took that approach, Russell said, to ensure that companies report classic ransomware attacks.

See our two-part interview about the Ransomware Task Force: "Task Force Leader Discusses How to Beat Ransomware in a Year" (May 19, 2021); and "Task Force Leader Addresses Proposed Mandatory Reporting of Ransomware Payments" (May 26, 2021).

Reasonable Security Enforcement Growing

At least 25 states now have reasonable security or safeguards provisions in state law, noted Stoppel, with Nebraska and others adding these mandates after the Equifax breach. The AGs have a strong interest in enforcing these laws, she said. Regarding consumer data, if AG offices "get wind that there may be missteps or a laxity in the attitude there, they are definitely going to investigate."

In New York, explained Russell, the AG is no longer forced to couch a consumer data breach case on a perception of fairness or deception because the office has black letter law to use for inadequate security measures. Recent multistate settlements contain a plethora of provisions about security improvements, showing AGs' new comfort and interest in investigating security, Stoppel said.

See our two-part series on New York's new cybersecurity standards: "Expanding Definitions and Requirements" (Sep. 11, 2019); and "A Compliance Roadmap" (Sep. 18, 2019).

The Arrival of Privacy Powers

The AGs have spent notable time examining state privacy bills over the past year, reported Lucan, in a bid to strengthen their enforcement authority and tools. In Florida, said Sadowski, reviewing and commenting on the privacy legislation "was all-consuming for a couple of months."

Enforcement of privacy laws in California and Virginia will likely spill over to boost other AGs' privacy work in states without comprehensive laws, Lucan said. Breaches have dominated her AG's work for years, but privacy could claim an equal portion of her workload soon, she predicted.

When California or Virginia's AG office reviews a company's privacy notice, Stoppel said, the office "may pick up the phone and call Illinois or New York. It's a new frontier for how states potentially start investigations. Companies need to be cognizant of how responses in California could be used against them in other states."

Privacy is an attractive enforcement subject because it has become a bipartisan political concern, Florida's Sadowski observed.

See "Behind the Scenes: California AG's Non-Public CCPA Inquiries" (Apr 7, 2021).

Board Involvement and Ransoms Now AG Concerns

AG offices are increasingly scrutinizing ransomware notifications to ensure companies have adequately investigated the incident. "In Connecticut, we are taking a close look to make sure companies are doing the legwork to try to find out the true scope of the attack. In some cases, we will ask how far back logs were reviewed, maybe even ask for copies of those logs," Lucan said.

Many companies previously declined to report ransomware attacks to states, citing minimal risk of consumer harm and, thus, no obligation to notify. "Even for a traditional breach, a risk of harm analysis is very difficult because it is speculative in nature," Stoppel said. In Connecticut, more companies now are reporting them, even if they have not confirmed that data was exfiltrated, Lucan noted.

Corporate governance is now important in the AG's reviews, said Sadowski. The Florida AG wants boards to have skin in the game and to ensure leadership provides resources for security.

"That is a new trend in the multistate investigations," said Luciano. AGs are now evaluating the company's governance mechanisms to ensure security issues go up the ranks, checking what the board learns about, and what resources exist to ensure that issues are identified and addressed, she reported.

See "Twelve Steps for Engaging the Board of Directors and Implementing a Long-Term Cybersecurity Plan" (Sep. 16, 2020); and "Establishing a Foundation for Breach-Notification Compliance in a Sea of Privacy Laws" (Jan. 29, 2020).