Karen White
CWAG-AG Alliance Executive Director

1300 I Street
Sacramento, CA 95814

916.833.2603
Karen.White@AGAlliance.org

Introduction

All fifty states and the District of Columbia have laws specifically designed to deal with cybersecurity breaches. However, the laws in each state vary widely. The concept of privacy across the globe is fluid. With the official implementation of the European General Data Protection Regulation ("GDPR"), companies that operate internationally have been forced to develop complex security systems to accommodate the GDPR's pro-privacy, pro-user approach. Domestically, security systems that house our data remain complex and widely misunderstood.

State Attorneys General ("AGs") are this country's chief consumer protection advocates. In this role, AGs continuously track privacy policies, monitor companies' compliance with such policies, and sometimes enforce them against companies that abuse the trust consumers place in them. While AGs have traditionally taken a reactive role in data privacy enforcement, opportunities exist for proactive engagement and the development of proper incentives for businesses to voluntarily implement, apply, and maintain robust cybersecurity programs.

Background

The Conference of Western Attorneys General ("CWAG") is a bipartisan 501(c)(3) organization dedicated to providing educational opportunities to AGs. CWAG provides consumers and business entities the opportunity to exchange information and expertise with the law enforcement community in areas where communities are experiencing change. CWAG also serves as a venue where public-private partnerships are forged in order to assist in the creation of good public policy.

In the cyber security and data privacy context, civil violations and criminal threats continue to escalate and become more sophisticated and complex. In response to this dynamic, CWAG created the Cybersecurity Working Group ("Working Group") two years ago in the wake of a series of inquiries from companies wanting to know how AGs will handle their prominent role in cybersecurity, and how companies can handle requests for more information regarding cybersecurity events from AGs and senior staff. The Working Group has had numerous substantive policy discussions among relevant stakeholders—AGs, federal and state regulators, private businesses, and privacy groups—regarding what a balanced enforcement framework could look like that allows for increased certainty for businesses concomitant with stringent consumer data protection. The Working Group has met four times with as many of fifty participants at a time.

The purpose of the Working Group was originally information sharing. When the Working Group first met, several states did not even have cyber breach laws on the books. Through discussions, it became clear that there was indeed confusion on both sides of the table regarding cyber events. The Working Group identified the need to encourage businesses to act prophylactically to better protect consumer data. The AGs acknowledged that they use their enforcement authorities at least in part with a hope to encourage other business to have mechanisms in place reasonably designed to protect private consumer data. All agreed that enforcement actions alone were unlikely to bring about real change. Nobody can secure their data and systems from 100% of attacks, but all can take actions that reasonably comport with the accepted industry security standards and thereby substantially lessen the likelihood and

effect of a successful attack. And those are the entities that should benefit from a safe harbor.

The Working Group focused on "safe harbor" provisions as a public policy option worth exploring in detail. This paper develops this concept further and attempts to bring structure to the discussion by summarizing the Group's key findings with respect to "safe harbor" and other pressing policy issues germane to the cybersecurity conversation.

I. The Policy Considerations Behind the "Safe Harbor" Concept

As AGs representing the interests of our states, we are committed to ensuring the protection of constituents' personal information and data, as well as safeguarding consumers when their personal information or data is compromised. Similarly, we are increasingly aware that the private sector—including businesses both large and small—recognizes the ever-present threat to the security of their online operations, including customer data and business information. This recognition has led to enhanced understanding of the dynamic cybersecurity environment and the need for businesses and government entities to continually reassess and invest in both the safety and security of their networks and in the security and protection of consumer data.

Well-intentioned government entities and businesses have taken appropriate steps to protect consumers but still fall victim to data breaches, cyberattacks, and other security events that implicate the public welfare. When a company is a victim—and even when the company took reasonable steps to prevent such an event—the consequences can be severe.

It is the recommendation of the CWAG Cyber Security Working Group that a public dialogue take place around the suggestion that state laws should evolve to reflect this reality. As such, this Working Group has focused on the suggestion that states consider creating a civil defense, or "safe harbor," and make it available to private businesses who take reasonable steps to secure consumer data.

Unanimity on this issue is not possible. There are simply too many variables and legitimate, deeply held policy positions. Nevertheless, tackling tough, contentious issues are a hallmark for AGs. As leaders in this space, AGs must remain vigilant in our commitment to protect consumers' private information and we must provide consistent guidance for businesses, particularly small- to medium-sized businesses, to act prudently. Without a consistent and fair regulatory field on which to play, businesses will not make the investment to bring safe services and products to market.

The participating AGs believe that good cybersecurity is good business. A business that collects, maintains, and uses private information must protect it; market forces also create a powerful incentive to protect private information. That is, consumers will frequent businesses that provide reliable data security; those that fail to provide privacy protections will fail. Such logic, however, ignores the cost (to consumers and businesses) of data losses that will occur while the market sorts good from bad. It also ignores that even the best cybersecurity defenses may still be breached: "it is not a question of whether an organization will be breached, but when." Not even government is immune from breaches. It would be fundamentally unfair for government to claim immunity when it is breached, yet hold private entities to a standard it knows is impossible to maintain.

Through its discussions with stakeholders, the Working Group has observed that almost all businesses desire to "do the right thing" when it comes to cybersecurity. Breaches and other data security challenges directly cause financial and reputational harm to companies, and this damage can in turn create additional

economic complications if litigation ensues or if the reputational harm is so great as to thwart the interest of future customers in engaging with the company. Companies aim to protect themselves and their customers but often wonder, "Am I doing enough?" or "Am I doing this right?"

A legal "safe harbor" cuts to the core of these challenges by aligning the interests of businesses and their customers: businesses want comfort that investments in cybersecurity will help mitigate legal exposure if a security event occurs, and consumers want to patronize companies that are making appropriate investments in cybersecurity so that their own economic interests are protected. This cybersecurity symbiosis should be encouraged and fostered for the benefit of the entire online ecosystem. The opposite view—that investing resources in cybersecurity offers no net benefit to businesses as they will be punished either way in response to a breach event—creates misaligned incentives that push companies to opt against cybersecurity improvements to the detriment of their own business and the safety of their customers' data.

The potential legal defense that a "safe harbor" provides will encourage businesses to invest resources in cybersecurity enhancements that follow best practices and industry-specific frameworks. It will also allow businesses to view and treat cybersecurity upgrades as investments, not costs. These investments will directly improve security for businesses and consumers alike.

Perhaps most critically, the Working Group believes that a "safe harbor" would incentivize companies to voluntarily report breach events as early as possible because the companies—at least those that have taken appropriate steps to align themselves with the provisions of the "safe harbor"—would not subject themselves to legal liability by merely disclosing the breach event. The "safe harbor" would provide a reporting entity with legal protections that would mitigate undue litigation exposure. Consumers benefit from early disclosure as they are able to take appropriate steps to protect their data and personal information, such as by changing passwords or requesting credit freezes, when appropriate.

Lastly, in instances when a private entity is sued as a result of a data breach or other security incident, a "safe harbor" would provide guidance to the courts in assessing liability, which again has the effect of aligning the interests of private businesses and consumers' right to have their data protected: companies that take steps to meet the criteria of a "safe harbor" will be viewed favorably by courts and shielded from liability.

II. Implementation of a "Safe Harbor" Policy

Within the Working Group's discussion of the "safe harbor" concept, there was considerable attention paid to the question of how to implement an effective "safe harbor" provision. While a majority of Working Group participants support the macro-level concept of a "safe harbor," the Group could not agree on much else. But the Working Group does almost uniformly believe that if a business voluntarily makes reasonable and timely investments in its cybersecurity, and that same business is

victimized by a third party breach,[1] it should have the opportunity to use its investment affirmatively to mitigate liability.

Terminology – Even the term "safe harbor" was debated, with some suggesting a "presumption of innocence" was a superior concept to an affirmative defense. Others believed such a risk mitigation program would require a government regulator who would approve a security regime in advance for any company interested in having the benefit of liability protections. Still others believed a subjective policy, akin to prosecutorial discretion, to be applied by a regulator[2] (or judge) after a breach would be best. The Working Group also debated whether legislation would be required to effect a "safe harbor," or in a position paper or statement of principles could achieve the same objective. But the Working Group agreed that it is important is to make clear to both consumers and businesses alike that adequate investment in data protection will bring a concomitant benefit.

Standard – The Working Group frequently discussed the appropriate standard to apply. By default, the Group adopted a reasonableness approach. Other concepts regularly advanced were negligence, gross negligence, strict liability, qualified (pre-approved by the regulator), and a tiered concept where the available benefits were in proportion to the level of security. Most agreed that the standard should include a "totality of the circumstances" analysis.

Framework – How best to secure data was as elusive to the Working Group as it is to the entire global security community. True security is expensive, complex, and fluid. Worse still, most agree nothing is ever absolutely secure. Meanwhile, there is almost universal agreement that most companies can do much more. Solutions range from the simple low-tech solutions that everyone can (and should) implement, such as not writing your password on a sticky note attached to your computer screen, to holistic approaches involving expensive systems technology requiring 24-hour human teams to manage. One size does not fit all.

One state has already adopted the "safe harbor" concept. Ohio Senate Bill 220, was signed into law on August 3, 2018. The bill allows three classes of business:

1. Non-regulated entities (typically corporations that collect and process PII);
2. Regulated entities (those that maintain sensitive data such as HIPPA); and
3. Businesses that only process consumer purchasing information (i.e. credit card transactions)

---

[1] This paper does not address data compromises that result from internal or physical means, *i.e.* an employee who stole data or the loss of a laptop containing consumer data.

[2] This approach would allow regulators to promulgate appropriate rules for regulated businesses with review and comment period. For example, the applicability of HIPAA and Gramm-Leach-Bliley would be considered.

to benefit from an affirmative defense if they reasonably had in place an appropriate cybersecurity framework prior to the breach. No single framework is favored per se, rather a "reasonable" adherence to at least one of several enumerated framework approaches appropriate for the class of business is what the defendant must demonstrate to earn the liability protections. The new statute purports to respect the "scale and scope" of a business's cybersecurity program because it has factors, such as the amount of resources available to a business, that go to whether or not their program was "reasonable." Ohio's approach is laudable and this group will monitor both the business response — that is, whether such a policy actually incentives proactive private investment in cybersecurity — as well as how the new law is tolerated and applied by the courts.

Consensus exists within the Working Group that "safe harbor" is a meaningful and important concept to pursue. There remains a divide on how to do it. There is no agreement on which framework (or even set of frameworks) to embrace and there is a lack of agreement on whether a framework is even appropriate. One participant candidly acknowledged that developing an appropriate framework "will likely take months of public, private, and academic deliberation to yield fruit." Our group has been working on this issue for nearly two years already. While we are open to continued dialogue and are confident our efforts will improve with time, we acknowledge no singular approach will work. Like Ohio, a malleable approach seems necessary but lacks the regulatory certainty we had originally sought to identify.

Almost everyone agrees the NIST Framework is the most widely known, well understood, and broadly applicable cybersecurity framework available. Moreover, many security protocols already in place are modeled on the NIST Framework. The primary concern, however, with NIST being the only framework relied upon in a safe harbor policy is that it lacks the flexibility necessary to truly and properly incentivize all the different actors that collect, manage, and use consumer data. And, there are newer security frameworks that are now widely available and have proven successful. To adopt just one, felt to the group as leaving too much benefit and too many companies (and their customers) on the open seas rather than inviting them into calmer waters of a harbor. Indeed, NIST standards do not work for all businesses when considering factors such as:

size of the company, nature of the company's business, sensitivity of the data maintained by the company, available technological safeguards, the costs of such safeguards, and industry standards. Despite that, it is difficult to foresee any legislation or regulation adopted in the near future that establishes a safe harbor and fails to rely, at least in part, on the NIST Framework.

It may be that the sweet spot for any policy is "NIST+." NIST, as the standard bearer, even if perhaps dated and clunky, coupled with at least one other approach or multiple approaches seemed to garner the greatest support (or lack of opposition). In particular, the idea of industry specific standards was advanced as a laudable approach and many advocated for compliance with existing duties, such as Graham Leach Bliley (GLB), as adequate. For example, an industry group that by the nature of its business processes possesses particularly sensitive data – hospitals for example – might need a different or higher or more sophisticated framework to be applied if the entity seeks to qualify for a liability protections. Small businesses, especially those that do not maintain PII – a convenience store or gas station – might qualify, if hacked, for safe harbor with relatively minimal safeguards in place. Small businesses within an identified industry group – perhaps a solo tax preparer – would be forced to make the choice of investing in a NIST cybersecurity system or customizing with an industry group framework. So long as the industry group is clearly defined so business and customers can understand in which group they belong, and that each group is clearly correlated to an appropriate framework, this approach would be successful. A scalable approach could create limited flexibility and avoid ambiguity for the regulator and the regulated community alike.

Scope of Defense – The liability a company may face post-breach event can come from many potential directions, but the two primary areas of concern are potential public enforcement actions by an AG (or AGs) as well as other regulators, and private or class-action lawsuits. At a minimum, the Working Group believes that some protection from private class action lawsuits is appropriate when a company has taken steps to maintain its cybersecurity. Additionally, specific defenses from certain types of relief, *i.e.*, penalties or injunctive relief, could also be tailored for any state policy. The issue of "repeat offenders" arose as did waiver for egregious behavior (such as failing to install a simple patch or failing to react once knowledge of a breach occurred). AGs should consider the level of scrutiny they use to address the merits behind a business' claim to have aligned with a standard. Even if a company legitimately, in good faith, aligns its program with an industry standard, there will likely be an adversary to argue the contrary.

Data Type – There was some discussion, though limited, that "safe harbor" should only be available for certain types of data. For example, if a company collects particularly sensitive types of data then it should not qualify for any liability protections. Yet this might be the type of business that should have strong incentive to keep its data safe.

Business Size – There was general agreement that business size does not matter.

Cybersecurity in the modern era is just another cost of doing business and it was the group's position that small or mid-sized business should not be treated differently. There is simply no difference in the harm potential for private data stolen because of where it was stolen. It was also noted that one breach, even if small, is woven into a mosaic of hacked information making more sophisticated attacks possible.

All of these concerns and arguments—and several others not listed—must be considered before implementing a state standard for cybersecurity protection. While NIST might not be the best option, it will be important as a starting point and guide for developing criteria for a more diverse and applicable cybersecurity program for businesses.

III. Government Enforcement Actions

Much of the Working Group dialogue focused on the risk—financial and reputational—that a private class action lawsuit posed to a company that suffers a data breach. Both businesses and AGs, however, often struggled with the latter's role as a regulator. The AG members of the Working Group routinely touched upon certain factors their offices might consider in making a determination to bring an enforcement action against a company that suffered a breach event. Similarly, the private sector participants voiced an interest in learning how an AG might assess a case during the investigative stage and whether the AGs could ever endorse the availability of a "safe harbor" for private companies defending an enforcement action brought by the government.

A. Factors Considered During Investigation

Severity – All acknowledge that the scope of impact to consumers will be a core consideration during any investigation and subsequent decision to litigate. The compromise of a handful of consumers' data is unlikely to cause the wide scale consumer harm that a breach of hundreds of millions of consumers' data across every jurisdiction in the United States.

Frequency – The frequency of breach events at a company is an important consideration. If a company experiences data breaches more than once, one could reasonably conclude that it did not take appropriate steps to mitigate risk.

Self-Reporting – The Working Group wanted regulators to credit self-reports and proactive steps to mitigate to a greater degree. Even though reporting to AGs of a breach is required in many states, targets of a successful breach often go beyond the minimum required and this conduct should be factored into regulatory reaction.

Numerosity – There are millions of cyber attacks and attempted breaches each day but some businesses are targeted more often. The number of threats a business or industry must deal with should be relevant to determining culpability.

Adequate Notice – The timing and nature of notice to consumers will be a factor in assessing potential liability. Quick, targeted multi-media notice will be superior to delayed generalized notice.

Length of Breach – The amount of time, or number of days, a third party has unauthorized access to data might be a factor. Generally speaking, the longer a breach

is ongoing, the more expensive the breach will be to mitigate.

Identification of Breach – Whether the company self-identifies a breach and acts immediately should be considered by a regulator. If a third party identifies the breach first, before the entity that is actually in control of (and thus responsible for) the data, it may be an indicator that the security protocols are not robust enough.

Breach Uniqueness – Regulators should consider whether a breach is the result of new or first-time techniques. Conversely, if an entity were to be breached as a result of a known hacking tactic or a previously identified vulnerability, that entity would not be viewed as appropriately diligent.

B. Presumption of Blamelessness

The affirmative defense that a "safe harbor" offers is typically available in private litigation only and not available to entities responding to regulatory or public enforcement actions. What is more common, however, in public enforcement actions—specifically criminal prosecutions—is the concept of a rebuttable presumption in favor of one party where, in appropriate circumstances, the burden of proof shifts from one party to another. States could consider establishing a "presumption of blamelessness" as a way to bring clarity to the procedural benefits a company could be entitled to during an enforcement proceeding brought by a government regulator if that company makes appropriate investments in its own cybersecurity.

For example, a company with a robust cybersecurity program that experiences a breach could enjoy a "presumption of blamelessness" if, after a regulator seeks to enforce against that company for violations derivative of the breach event, the company convinces a court that the presumption is appropriate based on its investment in its cybersecurity program. If such a motion is successful, the court could require the regulator to meet a new, higher burden of proof to hold the company responsible. There are a variety of ways such a burden-shifting regime could work but in many instances they would need to be statutorily created and applied during formal legal proceedings where an independent decision maker can assess the facts.

IV. Additional Policy Issues Relevant to "Safe Harbor" and Security Event Reporting

Throughout the course of the Working Group's discussions, several ancillary policy concepts were raised by stakeholders and, due to their direct bearing on the fairness and viability of a "safe harbor" concept, we include them in this report.

A. Tax Incentives for Investment in Cybersecurity

To encourage businesses to invest in cybersecurity, state tax incentives could be offered. Tax deductions that allow for investments in cybersecurity to be subtracted from a business' taxable income, or tax credits that allow for those investments to be subtracted from the amount of taxes owed by a business are possibilities. States should weigh the loss of revenue from tax incentives against how that money could be used to increase cybersecurity.

B. Extending "Safe Harbor" to Contractors and Vendors

Often businesses rely on third parties—contractors and vendors—to store or process data that the business aggregates in the course of its operations. Such businesses are mindful that their own legal risk in the data breach context is directly linked to the compliance of the third party entity. The "safe harbor" concept advocated by this Working Group must take into consideration the practical reality that much of the data collected by companies today is shared with third parties. Accordingly, the "safe harbor" should encourage businesses to take appropriate steps and conduct due diligence to ensure that vendors are committed to protecting consumer data and, in turn, provide reasonably proportional protections in response to such efforts by companies. In other words, if a company provides information to a vendor and contractually requires that vendor to implement reasonable security measures, that would also trigger the safe harbor for the company.

Furthermore, it is important to consider that in many breach reporting frameworks, state laws may require that contractors and vendors provide notifications to consumers in instances of breach. In many instances of breach, however, third-party contractors and vendors have no privity with consumers and thus would be unable to report such a breach to affected consumers. We recommend that language recognizing and addressing this distinction be incorporated into state data breach laws.

C. Account Takeovers

Over time we have learned that cybersecurity events are not all the same, and yet today the reporting of various security events to AGs and other regulators is done in a homogenized manner. The reality of the evolving cybersecurity environment is producing reporting that can often be both voluminous and valueless to law enforcement, creating confusion and sub-optimizing its practical utility. An acute example of this evolution is the Account Takeover ("ATO"), a growing phenomenon in the cybersecurity space. Yet ATOs are distinctly different events from data breaches and should be evaluated and reported using different reporting rubrics and analytical methodologies.

As a consequence of the many of large-scale data breaches that have been perpetrated against major companies and government entities in the past several years, online financial services, and similar financial account companies have seen an increase in a specific type of security attack, the ATO. ATOs involve the use of personally identifiable information that was previously stolen from one or more sources in data breach events; that personal data is then "weaponized" and used to attempt to gain electronic access to preexisting individual accounts through criminal cyberattacks against public and/or private sector online platforms, frequently involving financial accounts of various types. Thus, data breaches and ATOs are two distinctly different and identifiable criminal acts being perpetrated .

Unlike large-scale data breach events, ATOs are the result of attempts by criminals who apply existing lists of previously stolen customers' user ID/password combinations — for example, millions of stolen ID/password combinations are sold for pennies among criminals in transactions on the Dark Web —which are then used to launch online cyberattacks on public and private sector websites. These events, often

with millions of rapid-fire, sophisticated computerized attack attempts, are called "list validation attacks." Depending upon the circumstances, ATO criminals use stolen identity data to access consumer accounts if the user ID and password are successfully matched against an existing account, for which the consumer had set up the same ID and password. The attacks are most often directed against accounts with financial value of one type or another.

Organized criminal enterprises, and even international nation state-sponsored activities, are increasingly performing ATOs using refined, highly sophisticated computerized attack techniques, such as botnets, to optimize the greatest illicit results. Criminals can also gain access to citizens' existing login credentials for online accounts through email "phishing" attacks, where the consumer unwittingly provides improper access to their personal information by clicking on an email from a cyber-attacker that was masquerading as a legitimate communication.

In order for US and state government data breach notification laws to be effective vehicles for remediating injury from actual data breaches, and for government to be able to most effectively combat ATOs, the differentiation of these crimes must be recognized for what they are and what they are not. ATOs are separate crimes from data breaches, and are the byproduct of the widespread availability of stolen personal information, the availability of which resulted from previously committed data breaches at institutions who have and will continue to be required to report these Data Breach occurrences as required by law.

Reporting an ATO event provides different information about a different crime than a data breach, and is usually unrevealing about the underlying original data breach crime and cause of the injury (*i.e.*, personally identifiable data stolen from another source or from the consumer themselves). Information about an ATO is actually information about the distinct, second crime being committed *utilizing* data from a data breach. Treating the two crimes as the same unnecessarily saturates the data breach notifications that a state government agency or AG staff must review, where such information reporting must be analyzed and understood in order to protect the public. ATO crimes are very often being perpetrated by a different criminal party unrelated to the original bad actor that conducted the original data breach. The criminal who facilitates an ATO likely obtained the credentials utilized for the attack anonymously on the Dark Web from other criminals selling the proceeds of their separate data breach crimes.

In response to the rise in ATOs, and the realities of the uniqueness of this type of cybercrime, state data breach notification laws should support a separate treatment of ATOs by separately providing for a "Suspicious Activity Reporting" model, similar to that already utilized by financial services entities through federal and state agencies with regulatory authority over those industries. As AGs continue to use their enforcement authority to ensure that consumer information as well as public and private sector financial assets are all protected, and as policy conversations with respect to updating state data breach laws and reporting requirements continue to evolve, the distinction

between an ATO and a data breach should be explicitly recognized in data breach statutes, with differentiated provisions and reporting methodologies.