STATE OF NEW MEXICO
OFFICE OF THE ATTORNEY GENERAL

HECTOR H. BALDERAS
ATTORNEY GENERAL

New Mexico's Data Breach Notification Act at One Year Old

Presented By:

Brian E. McMath
Assistant Attorney General
Consumer & Environmental Protection Division
(505) 717-3531
bmcmath@nmag.gov

On January 12, 2018, Senator Elizabeth "Liz" Stefanics introduced Senate Memorial 12 ("SM 12"), entitled "Data Breach Notification Act Compliance." SM 12 was passed unanimously on February 14, 2018 and signed. In SM 12, the Senate requested that the New Mexico Office of the Attorney General ("NMOAG") review and evaluate the following:

> A. The compliance in New Mexico of the owners and licensees of personal identifying information and the service providers that retain that information under contract with the Data Breach Notification Act;
>
> B. The effectiveness of the current requirements of the Data Breach Notification Act in protecting personal identifying information and in assisting consumers to protect their credit after a data breach incident; and
>
> C. The methods that various states have used to ensure that consumers may lock their credit reports for free and the costs and benefits of those methods.

Further, the Senate requested the NMOAG create a report with the conclusions of its review and evaluation, along with proposals to strengthen consumer data security and breach notification. Finally, the NMOAG was asked to present that report to the appropriate legislative interim committee prior to that committee's final 2018 meeting. What follows is the NMOAG's report, as requested by the Senate in SM 12.

Executive Summary

The ease and convenience of chip-enabled credit cards, one-click online purchases, and GPS navigation in everyone's pocket often comes at a price. Theft of personally identifiable information ("PII") is a thriving business that costs consumers and governments untold sums of money, and the problem is getting worse. Data breaches continue to grow in size and number each year across the United States. While breaches are often painful for the companies whose systems are hacked, these breaches can cause years or decades of strife for consumers who suffer identify theft or other information-based harms. It is this consumer-centered harm that statutes like New Mexico's Data Breach Notification Act ("DBNA") attempt to address.

As of 2018, all fifty states have enacted data breach notification laws, and for good reason. If a company is hacked and a consumer's data is stolen, the consumer has no way to know. The purpose of statutes like the DBNA is to ensure that consumers are able to protect themselves in the event of a breach, as well as to incentivize companies who collect this data to tenaciously protect it. Though state statutes vary widely in their definition of PII and in their reporting requirements, the number of data breach notices New Mexico receives pursuant to the DBNA appears to comport with the number of notices other states with similar statutes receive, when adjusted for population. Thus, the NMOAG infers that the DBNA is being complied with at rates similar to those rates reported by similarly situated states. Some states (such as those that require all data breaches be reported regardless of the number of affected citizens) receive many more notices than New Mexico receives, and others (such as those states with no reporting requirement for private businesses as all) receive fewer. While mega-breaches are getting more common every year, it appears that the majority of data breaches reported to states (as high as 98% of those reported) typically affect fewer than 500 residents.

The events of the past year have demonstrated the need for statutes like the DBNA. In September 2017, just two months after the DBNA was enacted, consumer credit reporting agency Equifax announced a data breach affecting 143 million Americans, or nearly half the adult population of the United States. While the Equifax breach was written about extensively due to its size and the types of data compromised, Equifax appears to have notified affected consumers within legally mandated timeframes. While the Equifax breach was large and intrusive, affected consumers were notified and were able to take steps to protect themselves. In contrast, ride hailing service Uber Technologies suffered a data breach that compromised the PII of 57 million users worldwide in November 2016. Rather than disclosing the breach, Uber paid the hackers to delete the stolen data and then covered up the payment by falsifying internal documents. The affected users were not alerted to the compromise of their data until a year after it happened, resulting in multiple lawsuits, a state attorney general investigation, and a nationwide settlement.

The existence of these mega-breaches and others like them indicates that statutes like the DBNA are necessary to help consumers protect themselves. However, the events of the past year and the questions posed in the Senate Memorial have also highlighted several weaknesses in the DBNA. The most significant of these weaknesses as they pertain to the Senate Memorial is the DBNA's lack of an explicit investigatory function similar to those found in other consumer protection statutes. This limits the State's ability to independently confirm the answers to the first two questions posed in the Memorial, *i.e.* determining levels of compliance with, and the overall effectiveness of, the DBNA. This lack of a DBNA-specific investigatory provision means the NMOAG must typically rely on companies to self-report, and clearly some (like Uber) do not. Other issues identified include overly restrictive definitions of PII, overly permissive language pertaining to a company's duties under the statute, a 1,000-resident reporting threshold that results in most data breaches going unreported, a statutory cap on civil penalties that may be too low when compared to the size of the companies regulated, and no requirement that breached entities assist consumers in protecting their identities in the wake of a breach. These issues are explained in detail, and proposed solutions have been provided.

The DBNA is a critically important consumer protection statute, and it will only become more important as New Mexicans live more of their lives online. With a strong investigatory function, powerful monetary penalties to incentivize compliance, and other modifications, the DBNA can protect New Mexicans even better in the future.

I. INTRODUCTION & BACKGROUND

A data breach occurs when an unauthorized person gains access to, uses, or removes information.[1] Members of the general public tend to be most concerned with data breaches involving "personally identifiable information" ("PII," also called "sensitive personal information" or, in New Mexico's data breach law, "personal identifying information" and "biometric data").[2] Examples of PII include:

- Full name, maiden name, or alias;
- Social security number, passport number, driver's license number, taxpayer identification number, bank account number, or credit card number;
- Street address or email address;
- Personal characteristics, including photographs, fingerprints, handwriting, or biometric data like voice signatures and facial geometry; and
- Information about an individual linked or linkable to one of the above (e.g. date of birth, place of birth, race, religion, weight, activities, employment information, medical information, educational information, or financial information).[3]

Other examples of sensitive data often targeted in a breach include corporate trade secrets and intellectual property. However, unlike PII breaches, these breaches are typically the work of someone known to or employed by the target and are typically undertaken as part of a corporate espionage effort. This report will focus on PII breaches affecting consumers, like the 2017 Equifax breach.

[1] https://www.experian.com/blogs/ask-experian/what-is-a-data-breach/.

[2] *See* NMSA 1978, § 57-12C-2.

[3] National Institute of Standards and Technology, Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* at 7, (2010) (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf).

While it is difficult to count data breaches nationwide due to duplication, differences in definitions, and lack of reporting, it is generally agreed that data breaches are increasing in both number and size. According to the non-profit Identity Theft Resource Center, the number of U.S. data breaches tracked in 2017 reached an all-time high of 1,579 breaches, an increase of nearly 45% over 2016.[4] Nearly two-thirds of those breaches were the result of computer hacking, and the top three industry sectors targeted were Business (55%), Medical/Healthcare (23.7%), and Banking/Credit/Financial (8.5%).[5] Credit card numbers and Social Security numbers were both popular targets.[6]

When a breach occurs, consumers often have no way of knowing their PII may be compromised. Without knowledge that a breach affecting them has occurred, consumers are largely defenseless against identity theft, illicit purchases made with their payment cards or from funds in their financial accounts, and other fraudulent activities. Consumers can take steps to protect themselves in the wake of a breach through credit freezes and monitoring, but only if consumers are alerted to the breach.

Entities that suffer a breach, especially those that are publicly held, may be reluctant to inform regulators or the public of their security failures in an attempt to avoid damage to their reputation and a resulting injury to their bottom line. However, this corporate silence deprives consumers of the knowledge that their information has been compromised, hampering consumers' ability to protect themselves from harmful consequences like identity theft.

To address this tension, many states have passed data breach notification laws, starting with California in 2002. These statutes typically impose a notice requirement and penalize

[4] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, at 3 (Feb. 8, 2017) (https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf).
[5] *Id.*
[6] *Id.* at 4-5.

entities that remain silent about breaches affecting consumer PII. During the 2017 legislative session, New Mexico passed its own Data Breach Notification Act (NMSA 1978, §§ 57-12C-1 to -12) ("DBNA") which went into effect July 1, 2017. The DBNA requires breached entities to notify all affected New Mexico residents of a breach within forty-five calendar days with some exceptions.[7] If the breach affects more than 1,000 New Mexico residents, the breached entity is also required to notify the NMOAG and all major consumer reporting agencies within the same forty-five day period (though consumers must be notified irrespective of the size of the breach).[8] If the breached entity fails to provide the requisite notice to affected consumers, the State may file an action against that entity on behalf of those consumers seeking injunctive relief, actual damages, consequential financial losses, and civil penalties.[9]

Just two months after the DBNA went into effect, consumer credit reporting agency Equifax reported that it was the target of a breach that compromised the PII of 143 million consumers, including more than 860,000 New Mexicans. According to Equifax, the breach took place from mid-May through mid-July 2017, and compromised a number of different categories of PII. The Equifax breach is still being actively investigated, and Equifax announced as recently as March of this year that even more consumers were affected than originally thought.[10] Equifax's former CEO admitted before the United States Congress that Equifax failed to safeguard consumer data. New Mexico is currently helping lead a multi-state investigation into the company.

[7] *See* § 57-12C-6; *see also* § 57-12C-8, -9 (detailing other exceptions).
[8] *See* § 57-12C-10.
[9] *See* § 57-12C-11.
[10] *Equifax's massive 2017 data breach keeps getting worse*, Washington Post (Mar. 1, 2018) (https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?noredirect=on&utm_term=.664cebe0ffb7).

II. SENATE MEMORIAL 12 – REPORT BY THE NMOAG

A. COMPLIANCE WITH THE DBNA

In SM 12, the Senate asked the NMOAG to "review and evaluate ... the compliance in New Mexico of the owners and licensees of [PII] and the service providers that retain that information under contract with the [DBNA]." At the outset, providing a response to this request is difficult for a number of reasons. First, the DBNA places the responsibility of reporting data breaches on the breached entity while simultaneously affording the NMOAG no DBNA-specific investigatory power to confirm that breaches have or have not occurred. Under the DBNA, the NMOAG has a limited ability to monitor compliance other than through voluntary reporting. Thus, if an entity suffers a breach and fails to provide notice of that breach, the NMOAG has no way of knowing about the breach unless and until some other adverse consequence arises that can be traced back to that breach (for example, a consumer complaint about identity theft using information that could have come only from the breached entity). Second, the DBNA and its reporting requirement are only a year old, meaning the NMOAG has no year-over-year reporting statistics for comparison. A year-over-year increase in reports received (assuming the number of actual breaches remained reasonably constant) would indicate an increase in compliance; however the NMOAG has no such data.

Nevertheless, the NMOAG will provide what information the NMOAG does have. From July 1, 2017 through July 1, 2018, the NMOAG received 37 DBNA notices from businesses and public entities in the following general categories:

- Public universities
- Hotels and lodging
- Real estate

- Retail establishments
- Credit reporting agencies
- Online retailers
- Restaurants
- Insurance
- Healthcare
- Airlines
- Financial services

Several breached entities claimed they were unable to determine the exact number of New Mexico residents affected. For those that were able to determine the exact number, the number of affected New Mexicans ranged from zero (notices were sent nationwide to all states whether residents were affected or not) to 863,486 (from the Equifax breach). These entities reported a total of 903,541 potentially affected New Mexico residents, though more than 95% of that number was from Equifax alone.

AVG. RESIDENTS AFFECTED PER BREACH JULY 2017-JULY 2018:	30,118[11]
AVG. RESIDENTS AFFECTED (w/o Equifax):	1,381[12]

The causes of these breaches ranged from malware downloaded into a retailer's point-of-sale system to the physical theft of a laptop containing sensitive information. Credit card numbers and Social Security numbers were the categories of PII most often targeted, and free credit reporting and identify theft protection were the solutions most often proposed by the breached entities to affected consumers.

[11] This figure does not include the seven notices received indicating that the breached entity could not determine the exact number of affected residents.

[12] Same.

In at least one instance, a breached entity provided notice well outside the 45-day notice window. Uber Technologies, Inc., a popular ride-sharing service estimated to be worth $70 billion, was attacked by hackers and suffered a breach in November 2016, which compromised the PII of 57 million users. Uber then attempted to cover up evidence of the breach by paying off the hackers to delete the stolen data and then disguising the reasons for the payment. Uber eventually provided notice of the breach a year after the fact, in November 2017.[13] While New Mexico has little recourse against Uber under the DBNA since Uber had no duty to report the original breach before the bill's enactment, the Uber example highlights a central weakness of the statute: if Uber had not self-reported the breach, it is unclear if a state like New Mexico would have the investigatory ability to ever uncover the breach independently. Further, even after Uber decided to report, the NMOAG had no DBNA-specific investigatory mechanism to verify Uber's public statements about what happened and when. Uber eventually settled with attorneys general of all fifty states and the District of Columbia for $148 million in late September 2018.[14]

In order to assess compliance in New Mexico, it may be useful to compare the number of notices the NMOAG has received to those received by states with similar statutes and requirements. The following is a sample of data notices received by other state attorneys general or state consumer agencies over the last three to eighteen months[15]:

[13] *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, New York Times (Nov. 21, 2017) (https://www.nytimes.com/2017/11/21/technology/uber-hack.html).
[14] *Uber agrees to $148 million settlement over data breach*, KOB-TV Channel 4 (https://www.kob.com/business-news/uber-agrees-to-148-million-settlement-over-data-breach/5085544/).
[15] Due to some states' reporting systems and/or the date their data breach notification laws were enacted, these numbers may reflect (i) the twelve months preceding this report, (ii) the most recent fiscal year, (iii) the most recent calendar year, or (iv) the months since the state's reporting requirement was enacted.

STATE	AVG. NOTICES/ MONTH	REPORTING THRESHOLD	NOTES
AZ	N/A	> 1,000 residents	AZ began requiring AG notice in April 2018 and had no data to report yet.
CO	N/A	N/A	CO's new data breach notification law went into effect September 2018.
CT	56.3	None	CT's PII definition is narrower than other states with no reporting threshold.
DE	4	> 500 residents	Average since DE began requiring AG notice in April 2018; very broad PII definition.
HI	2.6	> 1,000 residents	HI's definition of PII is comparatively narrow and does not include biometric data.
IN	67.5	None	IN's definition of PII is comparatively narrow with no reporting threshold.
ID	2.1	N/A	ID requires only state agencies to report breaches, no requirement for private entities.
IA	3.7	> 500 residents	IA allows substitute notice to be sent either to the state AG or to local law enforcement.
LA	59.6	None	LA requires AG notice in its administrative code rather than by statute.
MA	139.3	None	MA received 1,671 notices in 2017, 98% affecting fewer than 500 residents.
MT	25	None	MT requires government and private entities to report, and MT's definition of PII is broad.
NE	37.8	None	NE is the sample state closest in estimated population to NM.
NH	38.7	None	NH requires notice to an entity's primary regulator or, if not applicable, only then to the AG.
NM	3.1	> 1,000 residents	Average from July 2017 to July 2018, the first year of enactment.
NY	131.9	None	NY received 1,583 notices in 2017, 88.3% affecting fewer than 500 residents.
NC	73.2	None	If breach affects >1,000 residents, consumer reporting agencies must be notified.
OH	N/A	N/A	OH requires only government agencies to report breaches, no requirement for private entities.
OR	8.2	> 250 residents	OR's definition of PII is broad and includes health-related information
SC	4.3	> 1,000 residents	Notices are sent to the Department of Consumer Affairs and also occasionally to the AG.
TX	N/A	N/A	No requirement to report breaches to the AG.
UT	1	N/A	UT requires only government agencies to report breaches, no requirement for private entities.

STATE	AVG. NOTICES/ MONTH	REPORTING THRESHOLD	NOTES
WA	5.5	> 500 residents	WA's definition of PII does not include biometric data; AG posts all notices online

While there are significant differences between the states in how each addresses this issue, several broad inferences can be made from this sampling of data.

First, states with reporting thresholds predictably receive far fewer data breach notifications on average than those without such thresholds. According to annual reports from Massachusetts and New York, the overwhelming majority of breaches reported to those state attorneys general affected fewer than 500 residents. While this is data from only two states, when combined with the sample of data above, it strongly suggests that the overwhelming majority of data breaches affecting New Mexicans likely go unreported to the NMOAG due to the 1,000-resident reporting threshold. It should be mentioned that 16 of the 37 notices New Mexico received between July 2017 and July 2018 concerned fewer than 1,000 residents. Therefore, either these entities did not possess contact information for the affected residents and issued substitute notices under Section 57-12C-6(D)(3), or these entities issued essentially "good neighbor" notices to the NMOAG even though notice was not legally required. The NMOAG does not have enough information to discern which of these two categories the sub-1,000-resident notices each fall into. However, in at least three instances, the NMOAG received a data breach notice even though zero New Mexico residents were affected, meaning these were almost certainly "good neighbor" notices rather than substitute notices under Section 57-12C-6(D)(3). It therefore appears likely that a significant portion of the notices the NMOAG received over the past year may not have been legally required. If all private entities actually adhered to the 1,000-resident threshold (assuming no Section 57-12C-6(D)(3) substitutes), New Mexico might have received as few as 21 notices over the past year, or less than two per month. There are likely entire business sectors whose data breach activity is invisible to the NMOAG and to the Legislature because their breaches never trip the 1,000-resident threshold.

Second, statutory language, rather than population, appears to significantly affect how many data breach notifications a state is likely to receive. Delaware, Montana, Nebraska, and New Hampshire all had estimated 2017 populations[16] lower than New Mexico's, but each received more data breach notifications than New Mexico. As a largely rural western state, Montana provides a useful comparison that highlights how statutory language can greatly impact how and when breached entities provide notice. In Montana, the state attorney general received approximately *eight times* as many data breach notifications as the NMOAG despite having a population approximately half the size of New Mexico's. Based on the data above, the NMOAG attributes this difference, in large part, to Montana's lack of a reporting threshold.

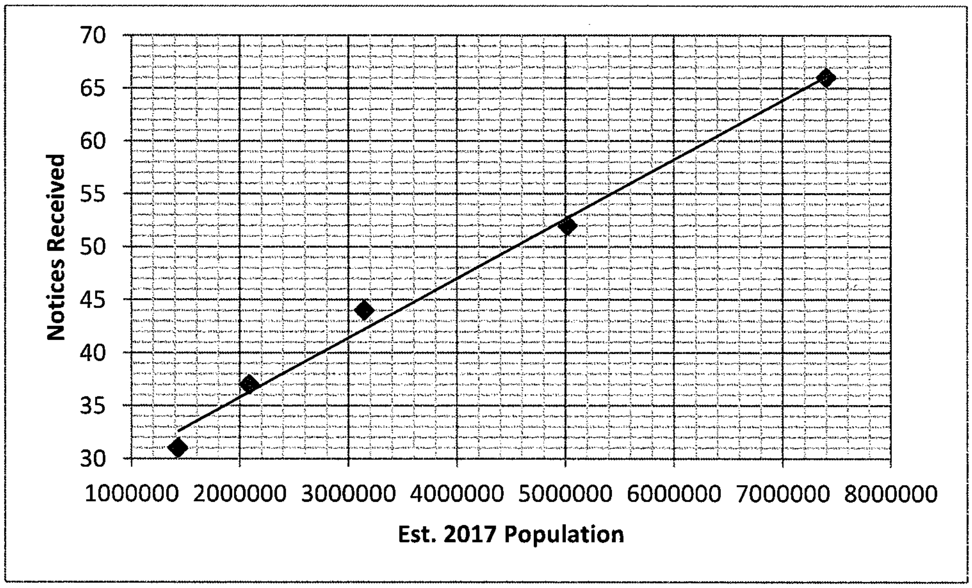
Third, population is likely a good predictor of data breaches assuming similar statutory language, reporting thresholds, and other requirements. The states in this sample that represent the closest comparisons to New Mexico on a statute-to-statute basis are Hawaii, South Carolina, Iowa, and Washington. All five states have 500+ resident reporting thresholds, similar definitions for "security breach," and similar definitions of PII.[17]

[16] U.S. Census Bureau, Annual Estimates of the Resident Populations for the United States, Regions, States, and Puerto Rico: April 1, 2010 to July 1, 2017 (https://www.census.gov/data/tables/2017/demo/popest/state-total.html).

[17] Delaware also has a 500-resident reporting threshold, however Delaware's definition of PII is far broader than the other states and includes e-mail addresses, medical records, and health insurance information. This broad definition of PII likely contributed to Delaware's relatively high number of data breach notices as compared to its population.

State	Est. 2017 Population	Appx. notices received per year
HI	1,427,538	31
NM	2,088,070	37
IA	3,145,711	44
SC	5,024,369	52
WA	7,405,743	66

When placed on a graph, the data suggest a relatively linear relationship:



From this (albeit small) sample of data, it would appear that the number of notices New Mexico receives is in line with the number of notices received by other states with similar reporting requirements as a function of population. Thus, the NMOAG infers that DBNA compliance is likely at rates very similar to compliance rates reported by other states with similar statutes.

In sum, it is very difficult to assess compliance with the DBNA without an independent investigatory mechanism. It is also clear that reporting thresholds in data breach notification statutes likely (but legally) prevent states from being notified about the majority of data breaches affecting their citizens. Finally, while compliance is difficult to assess, New Mexico does not appear to be an outlier when compared to states with similar statutes and reporting thresholds.

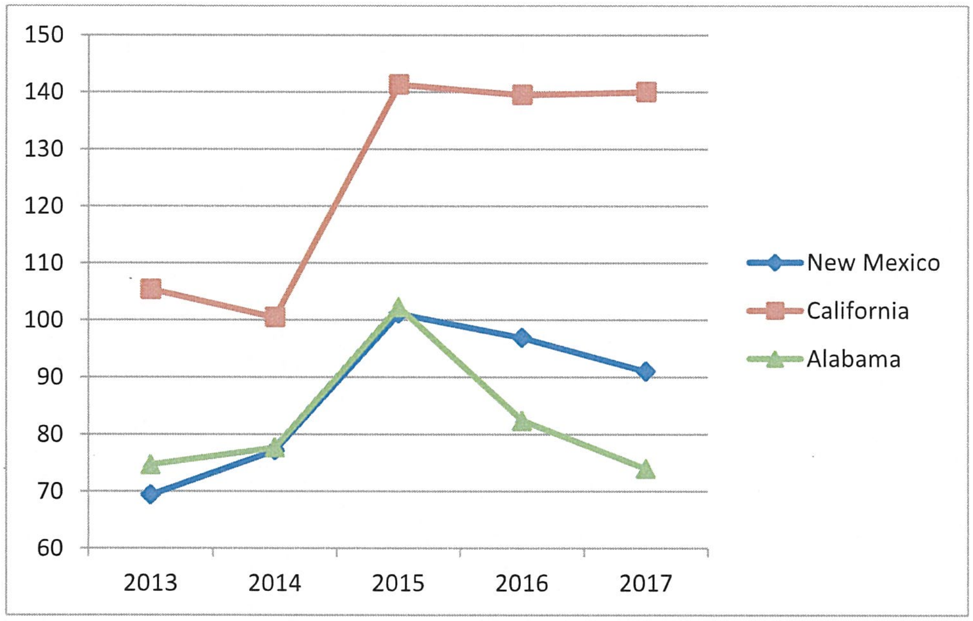
B. EFFECTIVENESS OF CURRENT DBNA REQUIREMENTS

In SM 12, the Senate asked the NMOAG to "review and evaluate ... the effectiveness of the current requirements of the [DBNA] in protecting [PII] and in assisting consumers to protect their credit after a data breach incident." As discussed above, this evaluation is difficult because (i) the NMOAG has no statutory authority to investigate breaches independently to determine if breaches are going unreported or underreported, (ii) the DBNA is a very new statute with limited associated data, and (iii) due to the language of the DBNA itself, many entities are not required to report breaches to the NMOAG.

1. The DBNA and Identity Theft

One metric that may be useful to examine in this context is the number of reports of identity theft in New Mexico. Since identity theft is often the goal of hackers seeking unauthorized access to PII, variations in reports of identity theft might offer a clue as to whether the DBNA is effective at protecting PII. According to the Federal Trade Commission ("FTC"), New Mexicans reported 1,909 instances of identity theft in 2017, or 91 reports per 100,000 residents.[18] While those numbers reflect a downward trend as compared to previous years, that trend appears to have started in 2016 before the passage of the DBNA. Additionally, California (the first state to pass a data breach notification law in 2002) consistently reports rates of identity theft much higher than New Mexico's. By contrast, Alabama's data breach notification law just recently went into effect in June 2018, but Alabama consistently reports rates close to or lower than New Mexico's.

[18] *Consumer Sentinel Network Data Book 2017: State Rankings: Identity Theft Reports* (https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/consumer-sentinel-network-data-book-2017/state-rankings-id-theft-reports).



Reports to FTC of identity theft per 100,000 residents by year
Source: FTC Consumer Sentinel Network Data Books 2013-2017.

So while the DBNA may be reducing rates of identity theft in New Mexico, the extent of that effect is still unclear and more data is needed.

2. The Language of the DBNA

Turning to the protections provided by the language of the DBNA itself, the NMOAG proceeds from the basic assumptions that the best ways for a statute like the DBNA to help consumers protect their credit are by: (i) preventing the data breach from occurring in the first instance, (ii) requiring that the consumer be notified that their data was compromised if a breach does occur, and (iii) providing the consumer with information about his or her options in the wake of a breach. Consumers have little control over how entities collect and store their information, and consumers cannot protect themselves in the wake of data breaches they do not know about. While statutes should not seek to compel consumers to protect themselves in the wake of a breach, statutes like the DBNA can and should compel entities to tenaciously protect consumers' PII and, if those protections fail, to notify victims quickly and effectively so the victims can then decide how best to proceed. To that end, the NMOAG's analysis of the DBNA's effectiveness at helping consumers protect their credit will focus largely upon: (i) the DBNA's effectiveness at compelling entities to protect PII, and (ii) the DBNA's effectiveness at compelling breached entities to notify consumers that their credit may be at risk.

Beginning with the definitions in Section 57-12C-2, the DBNA's definition of PII is narrower than the definition promulgated by the National Institute of Standards and Technology mentioned above and narrower than definitions used in other states. Under the DBNA, information only qualifies as PII if it constitutes a combination of information that is "usable," i.e., a person's name "in combination with" various data elements, and then only if such data elements are unencrypted or an encryption key was also accessed. And, the exposure of a consumer's full name, home address, email address, date of birth, and place of birth might not be considered a reportable data breach. The exposure of a consumer's full name, date of birth, and credit card number without the credit card's security code also might not be considered a reportable data breach. Even more worrisome, the exposure of a consumer's medical records and personal medical history, as long as those records do not include the enumerated data elements under Section 57-12C-2(C)(1)(a)-(e), might not be considered a reportable breach.[19] These definitions are important because the DBNA's duty to notify under Section 57-12C-6 arises only when the compromised data falls into one of the DBNA's narrow definitions of PII.

In addition, the DBNA defines a "security breach" as "the unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data and the confidential process or key used to decrypt" that data. This is narrower than the industry-standard definition of a "data breach," which is the unauthorized access or acquisition of data, computerized or

[19] Such a disclosure may run afoul of other state statutes, however, like Section 24-14B-6 of the Electronic Medical Records Act.

otherwise, encrypted or not. Under the DBNA definition, an entity might not be required to report a data breach if PII were acquired in a non-digital format, or if encrypted PII were acquired without the encryption key (which could then be acquired during a subsequent breach at another time).

Moving to Section 57-12C-3, this section's requirement that regulated entities "arrange for proper disposal" of PII is vitally important because the longer an entity keeps PII, the greater the risk that PII will be improperly accessed. However, the section requires disposal only when PII is "no longer reasonably needed for business purposes." The term "reasonably needed for business purposes" is not defined in the statute and may allow for ambiguity in how regulated entities meet this particular requirement. Further, entities are not required to maintain records of their disposals, meaning neither consumers nor the State can easily verify that disposal has in fact occurred or how that disposal was performed.

Similarly, Section 57-12C-4 requires regulated entities to implement security procedures and practices to protect PII, but those security procedures and practices need only be "reasonable … [and] appropriate to the nature of the information[.]" No additional definitions are provided. While it is difficult to codify a requirement that must constantly evolve to keep up with technological innovation, it is also difficult for the State to prosecute an entity under this section because the language is too vague and open to interpretation.

The DBNA's notification requirement, which in many respects is the very heart of the statute, does not apply if the regulated entity determines "after appropriate investigation … that the security breach does not give rise to a significant risk of identity theft or fraud." Section 57-12C-6(B). Again, the statute offers little guidance on what an "appropriate investigation" might entail or what "significant risk" might look like. This section creates what the NMOAG believes to be a substantial loophole that can insulate entities from liability under the DBNA simply by engaging in what the entity (not the NMOAG or any other state or federal regulator) believes to be an appropriate investigation to determine no significant risk. Besides giving the regulated entity discretion to determine what constitutes an appropriate investigation, this section goes a step further and gives the entity discretion to determine if there is a "significant risk of identity theft or fraud". This broad discretion is worrisome because there is a strong self-interest for the entity to determine that there is no risk to consumers. Additionally, such discretion may not be appropriate to give to entities with no specialized training or knowledge as to what constitutes a risk to New Mexico consumers.

Section 57-12C-7 provides regulated entities with an outline of information they are required to include in each breach notice. This section's reference to the federal Fair Credit Reporting Act ("FCRA") is important because, as discussed below, recent changes to FCRA enable consumers to lock their credit free of charge without proving they have been the victim of identity theft. Conspicuously, the state Credit Report Security Act ("CRSA"), which also contains requirements pertaining to credit reporting and locking, is not mentioned in this portion of the statute. However, as discussed below, recent changes to FCRA may preempt the relevant portions of the CRSA, obviating the need to reference both.

Section 57-12C-10 requires breached entities to report breaches affecting more than 1,000 New Mexico residents to both the NMOAG and to major consumer reporting agencies as defined by the federal Fair Credit Reporting Act ("FCRA"). As demonstrated by the sampling of data above, some entities choose to issue "good neighbor" notices while other entities clearly do not. Again, based on data provided by Massachusetts and New York, 88% to 98% of data breaches reported to those attorneys general concerned fewer than 500 residents. If all private entities that retain or license New Mexicans' PII had chosen to adhere to the 1,000-resident threshold over the past twelve months (as would have been their legal right to do) and were not eligible to provide substitute notice, New Mexico might have received roughly as many data breach notices as those states with *no reporting requirement for private entities whatsoever*. In other words, the 1,000-resident threshold is so high that it effectively renders the DBNA's requirement to notify the NMOAG and major credit reporting agencies almost meaningless. This reality, coupled with the fact that the NMOAG has no independent investigatory authority over these matters, means the NMOAG has significant difficulty in effectively enforcing the DBNA.

While the NMOAG is authorized by Section 57-12C-11(C) to file an action against a regulated entity seeking civil penalties, those penalties are limited to $25,000 for violations of the DBNA, except for violations related to a failure to notify. As to violations other than failure-to-notify, the section is unclear on precisely what constitutes a violation. For example, the statute could be read to mean that if a breached entity fails to implement reasonable security measures to protect the PII of a single individual, that failure is a violation of the DBNA. By that reading, the breached entity's failure to protect the PII of two individuals would be two violations, and so on. Conversely, the statute could be read to limit a breached entity's civil penalties for violations other than failure-to-notify to $25,000 per breach event. By that reading, the flat $25,000 penalty amount would be imposed irrespective of (i) the duration of the breach before detection, (ii) the quantity or character of the PII that was compromised, (iii) the culpability of the breached entity in causing the breach or covering it up, (iv) the size of the breached entity, or (v) the number of consumers ultimately placed at risk.

Turning to the failure-to-notify penalties, these penalties are limited to $10 per non-notified consumer up to $150,000. Therefore, the civil penalty for failing to notify 15,000 consumers is the same as failing to notify 15,001 consumers or 300,000 consumers or any other number of consumers greater than 15,000. While the majority of breaches reported to the State over the past year involved fewer than 15,000 consumers, the Equifax breach involved 863,486 consumers. Hypothetically, if Equifax were found to have failed to notify those consumers in violation of the DBNA, Equifax's civil penalties would have been capped at $150,000, versus $8.63 million if the $10-per-consumer penalty were applied without a cap. This is important because as more Americans conduct more of their shopping, banking, healthcare, and other personally sensitive activities online, the State can likely expect to see more breaches on the scale of Equifax in the future rather than fewer. According to one source, approximately *7 billion records* were exposed nationwide during the first three quarters of 2017 alone, representing a four-fold increase from the same period in 2016.[20] In addition, it bears mentioning that a penalty of $150,000 likely would not provide the desired deterrent effect on an entity like Equifax, which reported $3.1 billion in revenue in 2017 alone. If one of the goals of the DBNA is to compel compliance with its requirements, part of that should be imposing penalties that truly deter bad actions.

As to the language of the penalties section generally, the section imposes a "knowingly or recklessly" standard in order to secure civil penalties. The result: negligent exposure of records appears to carry no civil penalty of any kind, and the State faces additional evidentiary burdens in proving the breached entity's culpability before civil penalties may be assessed. While New Mexico does not yet have data on this point, according to the New York Attorney General, one in four data breaches that occurred in New York in 2017 were attributable to negligence.[21]

[20] *See* Risk Based Security, *Q3 2017 Data Breach QuickView Report* (Nov. 8, 2017) (summary available at https://www.riskbasedsecurity.com/2017/11/2017-yet-another-worst-year-ever-for-data-breaches/).

[21] *Information Exposed: 2017 Data Breaches in New York State* (https://ag.ny.gov/sites/default/files/data_breach_report_2017.pdf).

Finally, the DBNA does not impose any remedial requirements on breached entities beyond reporting following a breach. Many larger entities offer free temporary credit monitoring to affected consumers in an attempt to earn back customer trust and not lose market share, but the DBNA does not require such remedial measures. As discussed more fully below, other state statutes could provide a model for remedial requirements in the wake of a breach that could help protect consumers' credit.

C. STATE/FEDERAL LAWS REGARDING CREDIT FREEZES

While the DBNA does not contemplate credit locking and unlocking, New Mexico's Credit Report Security Act ("CRSA") does require consumer reporting agencies to place and remove security freezes on consumers' credit reports upon request. *See* NMSA 1978, § 56-3A-3. Under current state law, consumer reporting agencies are permitted to charge a fee for these services in accordance with Section 56-3A-3(I).

However, this provision of the CRSA and those like it in other states are likely now moot given the recent passage of the federal Economic Growth, Regulatory Relief, and Consumer Protection Act, Public Law 115-174 (May 24, 2018) ("the Act"), which took effect September 21, 2018. Section 301 of the Act amends the federal FCRA Section 1681c-1 to require consumer reporting agencies to place and remove security freezes and fraud alerts on consumers' credit reports for free. Unlike the CRSA, a consumer need not prove they have been the victim of identity theft in order to obtain a free security freeze or fraud alert under the Act. FCRA expressly preempts state laws to the extent those laws are inconsistent with the federal statute, meaning New Mexico's CRSA and similar state laws allowing fees will likely be at least partially preempted. *See* 15 U.S.C. § 1681t(a).

III. CONCLUSIONS OF REVIEW

The DBNA is a critically important piece of legislation designed to protect New Mexico consumers from new and evolving threats in the digital age. However, because of a lack of independent investigatory authority, a high reporting threshold, overly restrictive definitions, and generous grants of autonomy to regulated entities in deciding what to report and when, the DBNA may not be fully accomplishing its goals of protecting consumers (i) from having their data compromised at all, and (ii) from adverse consequences following an unauthorized breach. Further, because the NMOAG lacks the ability to investigate, the NMOAG cannot accurately determine whether the DBNA is accomplishing its stated goals for the reasons discussed herein. The NMOAG encourages the Senate to consider the proposals below to strengthen the DBNA's protections of New Mexico consumers.

IV. PROPOSALS TO STRENGTHEN THE DBNA

A. Definitions and Standards

1. Expand the definition of PII

By way of example, Alabama's 2018 data breach act defines PII to include, among other things:

- "[I]nformation regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;"
- "An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual;" and

- "A user name or email address, in combination with a password or security question and answer that would permit access to an online account ... that is reasonably likely to contain or is used to obtain sensitive personally identifying information."[22]

None of these definitions are contemplated by the current iteration of the DBNA, but these types of data are routinely targeted for data breaches.

2. Tie "reasonable security procedures and practices" to a regularly-updated national standard and include a "safe harbor" provision

The U.S. Department of Commerce's National Institute of Standards and Technology ("NIST") is required by federal law to develop and revise cybersecurity protocols and standards for the monitoring of information security within the federal government. *See* 15 U.S.C. § 7406(c)(1). On April 16, 2018, NIST issued its "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1,"[23] designed to assist organizations with assessing current cybersecurity postures, identifying cybersecurity goals, identifying weaknesses in their networks, assessing progress, and communicating risk. Tying the DBNA's definition of "reasonable security procedures and practices" to something like the NIST framework would ensure standardized practices and ensure that security procedures and practices get updated regularly.

However, bear in mind that the NIST framework was created for the federal government, an entity much larger and better funded than any private business. If a framework like NIST is adopted, entity size and resources should be considered when determining to what extent a regulated entity must conform to that framework. It may be advisable to create tiers or industry-specific recommendations based on NIST that entities could select based on their industry, the type and quantity of data they collect, and other factors. Some states have bridged the gap

[22] *See* Ala. Code 1975 § 8-38-2; *see also* Delware's 6 Del.C. § 12B-101(7) (defining PII to include medical data, health insurance data, and email addresses).

[23] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

between tying regulated entities to a standard like NIST and "reasonable security procedures and practices." Like the DBNA, Alabama's statute also requires reasonable security measures, but goes on to require the following:

- Designation of an employee to coordinate security measures;
- Identification of risks;
- Adoption and assessment of safeguards to address identified risks;
- Contractually requiring all service providers to maintain appropriate safeguards;
- Evaluation of security measures to account for changes in circumstances; and
- Informing management of security status.

Ala. Code 1975 § 8-38-3.

Relatedly, the Conference of Western Attorneys General ("CWAG") recently recommended the inclusion of a "safe harbor" provision in state data breach statutes.[24] CWAG's Cybersecurity Working Group studied this issue for two years and found generally that if regulated entities are able to use their investments in data security as a means of avoiding legal liability and litigation expense in the wake of a breach, such entities are much more likely to make those investments. For example, if an entity constructed a data security system that was then approved by an appropriate regulator or that adhered to a NIST-type framework as described above, that entity would have *per se* satisfied the DBNA's "reasonable and appropriate" standard contained in Section 57-12C-4. This would not insulate the entity from other statutory violations like failure-to-notify or from liability for fraudulent concealment like in the Uber case, but the entity would be relieved of the duty to prove up the reasonableness of its

[24] Similar provisions can be found in the Children's Online Privacy Protection Act and attendant regulations, 15 U.S.C. § 6501 *et seq.* and 16 CFR Part 312.

data security protocols. A safe harbor might also include provisions waiving the safe harbor for repeat offenders or for breaches affecting above a certain threshold number of consumers.

B. Enforcement Authority and Reporting Requirements

1. Make a violation of the DBNA a violation of the New Mexico Unfair Practices Act, NMSA 1978 Sections 57-12-1 to -26

This change addresses several issues identified in this Report, and reflects the way 29 other states have addressed enforcement of their data breach statutes.[25] First and most importantly, this change would enable the NMOAG to issue confidential civil investigative demands to independently investigate and confirm that a breach has occurred and that it has been

[25] *See, e.g.* Alabama's Ala. Code 1975 § 8-38-9(a) (imposing civil penalties in accordance with Alabama's consumer protection statute); Alaska's AS § 45.48.080 (defining violation of data breach statute as "unfair or deceptive act or practice"); Arizona's A.R.S. § 18-552(L) (defining knowing and willful violations as unlawful practices under Arizona's consumer fraud statute); Arkansas' § 4-110-108 (enabling attorney general to enforce under the Deceptive Trade Practices Act); Connecticut's C.G.S.A. § 36a-701b (defining violations as unfair trade practices); Delaware's 6 Del.C. § 12B-104 (enabling attorney general to enforce data breach notification statute pursuant to Delaware's consumer protection statutes); Florida's F.S.A. § 501.171 (defining violation of data breach notification statute as an unfair or deceptive trade practice prosecutable under Florida's consumer protection statute); Illinois' 815 ILCS 530/20 (defining violation of data breach notification act as unlawful practice under Illinois' consumer protection statute); Indiana's IC 24-4.9-4-1 (defining failure to disclose breach as deceptive act actionable under Indiana's consumer protection statute); Iowa's I.C.A. § 715C.2 (defining any violation of data breach statute as an unlawful practice under Iowa's consumer protection statute); Louisiana's LSA-R.S. 51:3074 (as amended by 2018 La. Sess. Law Serv. Act 382 (S.B. 361) (May 20, 2018)) (defining violation as unfair trade practice); Maryland's MD Code, Commercial Law, § 14-3508 (defining any violation of data breach statute as an unfair or deceptive trade practice under Maryland's consumer protection statute); Massachusetts' M.G.L.A. 93H § 6 (incorporating causes of action available under Massachusetts' consumer protection statute); Minnesota's M.S.A. § 325E.61 (incorporating enforcement provisions allowing attorney general to investigate "unfair, discriminatory, and other unlawful practices in business, commerce, or trade"); Mississippi's Miss. Code Ann. § 75-24-29 (defining noncompliance with data breach statute as unfair trade practice); Montana's MCA § 30-14-1705 (incorporating consumer protection penalties into data breach statute); Nebraska's Neb.Rev.St. § 87-806 (defining violations of data breach statute as violations of consumer protection statute); New Hampshire's N.H. Rev. Stat. § 359-C:21 (incorporating enforcement provisions of New Hampshire's consumer protection statute); New Jersey's N.J.S.A. 56:8-166 (defining violations of data breach statute as violation of consumer protection statute); North Carolina's N.C.G.S.A. §§ 75-62 to -65 (defining violations of sections as violations of unfair or deceptive acts statute); North Dakota's NDCC § 51-30-07 (defining violations as violations of unlawful sales or advertising practices statute); Oklahoma's Okl.St.Ann. § 165 (attorney general may prosecute violations as unlawful practices under Consumer Protection Act); Pennsylvania's 73 P.S. § 2308 (violation deemed an unfair or deceptive act or practice); South Dakota's SDCL § 22-40-25 (violations prosecutable as deceptive acts or practices); Tennessee's T.C.A. § 47-18-2106 (violation of data breach notification statute also a violation of Tennessee Consumer Protection Act); Texas' V.T.C.A. § 521.152 (defining violation of data breach statute as deceptive trade practice); Vermont's Vt. Stat. Ann. Title 9 § 2435(g) (providing authority to investigate, prosecute, and impose remedies for violations consistent with Vermont's consumer protection statutes); Washington's RCWA 19.255.010(17) (defining violations as unfair or deceptive act in trade or commerce and an unfair method of competition); West Virginia's W. Va. Code § 46A-2A-104 (failure to notice defined as an unfair or deceptive act or practice).

properly dealt with. *See* NMSA 1978, § 57-12-12 (NMOAG's authority to issue civil investigative demands pursuant to a UPA investigation). This grants the NMOAG the independent investigative authority needed to confirm compliance and discover non-compliance. Second, it would provide additional civil penalties of up to $5,000 per violation with no cap, a powerful monetary deterrent. *See* NMSA 1978, § 57-12-11 (penalty section). Third, it would provide private remedies for consumers harmed by the violation, including injunctions, actual damages, and treble damages. *See* NMSA 1978, § 57-12-10. Fourth, this change would provide courts interpreting the DBNA with a large body of published case law from which to draw, and would allow courts to look to FTC interpretations as well. *See* NMSA 1978, § 57-12-4 (instructing courts to look to FTC interpretations for guidance). Finally, this change would enable the NMOAG to promulgate regulations effecting the Legislature's intent and purpose in enacting the statute. *See* NMSA 1978, § 57-12-13 (enabling NMOAG to promulgate UPA regulations).

However, the civil penalty structures of the two statutes (the DBNA on one hand and the UPA on the other) are inconsistent with each other, as outlined below:

DBNA Penalty Structure	**UPA Penalty Structure**
Burden of proof for simple violation: State must prove violation occurred, no culpability required (strict liability).	Burden of proof for simple violation: State must prove violative conduct was engaged in "knowingly."
Relief available, simple violation: Injunctive relief and actual costs or losses, including consequential financial losses.	Relief available, simple violation: Injunctive relief and restitution.[26]
Burden of proof to obtain civil penalties: State must prove defendant engaged in violative conduct "knowingly or recklessly."	Burden of proof to obtain civil penalties: State must prove defendant engaged in violative conduct "willfully."
Relief available, civil penalties: The greater of $25,000 per violation or, for failure-to-notify violations, $10 per instance of failed notification up to $150,000.	Relief available, civil penalties: Up to $5,000 per violation with no cap.

[26] This does not include remedies available to private citizens under the UPA's private right of action. *See* NMSA 1978, § 57-12-10.

UPA violations are triggered by "knowingly" engaging in prohibited conduct, *see* § 57-12-2(D), however the UPA does not grant civil penalties of up to $5,000 for those violations unless the violative conduct was "willful," *see* § 57-12-11. By contrast, DBNA violations are triggered simply by proving that a violation occurred, *see* Section 57-12C-11(A), with civil penalties of up to $150,000 available if the defendant violated the statute "knowingly or recklessly," *see* Section 57-12C-11(C). Further, under the UPA, there is no statutory cap on civil penalties whereas the DBNA is capped at a maximum of $150,000 and then only for failure-to-notify violations. In other words, the UPA's civil penalties are more difficult to reach from an evidentiary standpoint but are uncapped, while the DBNA's civil penalties are easier to reach but are capped significantly.

It is the NMOAG's recommendation that if violations of the DBNA are to be defined and prosecuted as violations of the UPA, the UPA's civil penalty structure should be adopted as the penalty structure for both statutes. Assuming clear statutory definitions of what constitutes a violation of the DBNA (discussed in more detail below), the DBNA could easily define such violations as UPA violations and incorporate by reference the UPA's up-to-$5,000-per-violation penalties for willful conduct, private remedies, injunctive remedies, civil investigatory powers, and so on.[27] Further, the UPA's lack of a cap on civil penalties and "up to" flexibility may help resolve the issue of how to properly tier penalties for DBNA violations. Because UPA penalties are calculated per violation, the more violations an entity incurs (however those violations are defined), the steeper the penalty. This means that if an entity conceals a small data breach

[27] *See, e.g.* NMSA 1978, §§ 32A-5-42.1, -42.2 (referencing UPA for violations of the Adoption Act); NMSA 1978, § 47-15-7(A) (referencing UPA for violations of the Mortgage Foreclosure Consultant Fraud Prevention Act); NMSA 1978, § 57-2A-5 (referencing UPA for violations of the Cigarette Enforcement Act); NMSA 1978, § 58-7-8(C) (referencing UPA for violations of the Bank Installment Loan Act); NMSA 1978, § 58-15-3(G) (referencing UPA for violations of the Small Loan Act).

placing a small number of consumers at risk and violations are defined on a per-consumer basis, the civil penalties will be relatively small. Conversely, if an entity conceals a large data breach, the penalties will be larger.

One possible drawback to this arrangement is the increased evidentiary burden on the State to prove up violations of the DBNA in order to secure civil penalties. In its current form, the DBNA permits civil penalties for "knowing" or "reckless" conduct, which are lower levels of culpability than the UPA's "willful" standard.

2. Alternatively, grant the NMOAG investigatory authority under the DBNA and consider other penalty schemes

Rather than defining DBNA violations as UPA violations, the Legislature could authorize the NMOAG to issue civil investigative demands to entities to both confirm compliance and discover non-compliance without incorporating other provisions of the UPA. This authority has been separately granted to the NMOAG under other consumer protection statutes.[28] While there are significant additional benefits to be gained by defining DBNA violations as UPA violations as discussed above, the addition of investigatory authority would significantly increase the DBNA's effectiveness while preserving the DBNA's lower evidentiary burden needed to obtain (albeit limited) civil penalties.

This arrangement does not, however, address other issues with the DBNA's penalty structure. Even if the DBNA does not incorporate the UPA by reference, the NMOAG recommends additional changes to the DBNA's existing penalty structure as discussed in Section C below.

[28] *See, e.g.* NMSA 1978, § 6-4-22 (Tobacco Escrow Fund Act); NMSA 1978, § 57-1-5 (Antitrust Act); NMSA 1978, § 57-13-1 (Pyramid Promotional Schemes Act); NMSA 1978, § 57-15-6 (False Advertising Act); NMSA 1978, § 57-22-9.1 (Charitable Solicitations Act).

3. Require entities to report investigations to the NMOAG and retain records related to those investigations

In Alaska and Louisiana, like in New Mexico, entities are not required to provide notice to consumers if, after an appropriate investigation, the entity determines that "there is not a reasonable likelihood that harm to the consumers ... has resulted or will result from the breach." Alaska Stat. Ann. § 45.48.010; *see also* LSA-R.S. 51:3074 (as amended by 2018 La. Sess. Law Serv. Act 382 (S.B. 361) (May 20, 2018)). However, Alaska and Louisiana both require entities to document these determinations in writing and retain those records for five years. Alaska requires that entities notify the state attorney general that such an investigation was undertaken and provide these written records automatically, while Louisiana requires that entities turn over these written records on request. In order to incentivize entities to provide these records and avoid penalizing responsible reporting, both states exempt these reports from open records laws.

4. Reduce or eliminate the 1,000-resident threshold

As explained in previous sections, the majority of data breaches reported by regulated entities affect fewer than 1,000 residents, irrespective of the populations of the states receiving the reports. While the DBNA does typically require notice be provided to any resident that is affected (subject to an investigation and other exceptions), the NMOAG is not required to receive notice unless (i) the breach affects more than 1,000 residents, or (ii) if the breached entity satisfies the requirements for providing a substitute notification under Section 57-12C-6(D)(3) (the cost of providing individual notice would exceed $100,000, more than 50,000 residents were affected, or the breached entity does not have sufficient contact information for each affected resident). For breaches affecting fewer than 1,000 residents for whom the entity has contact information, the DBNA does not require notice to the NMOAG or any other state regulator.

In addition to ensuring the NMOAG has a full picture of data security affecting New Mexicans, lowering or eliminating the threshold also allows the NMOAG to identify repeat offenders, i.e., entities that are breached repeatedly due to lax security measures. Under the current DBNA, if an entity is breached repeatedly because of antiquated security measures but the breaches affect fewer than 1,000 residents (as the majority of breaches seem to do), the NMOAG has no way to identify such an entity. For example, a nationwide provider of hotel reservation software reported seven separate data breaches between July and August 2017 to the NMOAG, each affecting a different hotel client. None of these breaches affected more than 30 known New Mexican residents, so the entity likely was not required under the DBNA to provide the NMOAG with notice. If the entity had decided not to provide notice, the NMOAG would have no record of these repeated breaches and would have no way of knowing if these breaches were part of a single concerted attack or if this entity gets breached regularly because it has refused to implement reasonable security measures to protect PII.

5. Void waiver attempts as against public policy

At least ten states have language in their data breach statutes declaring that any attempt by a regulated entity to convince consumers to waive data breach reporting protections is void as against public policy.[29] With the advent of consumer arbitration agreements, waivers of collective action rights, and other attempts by private companies to convince consumers to waive legal protections as a condition of any agreement, this type of protection will become increasingly important.

[29] These states include, but may not be limited to, Alaska, California, Colorado (as amended), Hawaii, Illinois, Minnesota, Nebraska, Nevada, Utah, Washington, and the District of Columbia.

6. Include additional requirements related to data disposal

As noted above, the DBNA's requirement in Section 57-12C-3 that entities dispose of PII once it is no longer needed is vitally important, however the language could be read as overly permissive. While some states have adopted language similar to New Mexico's, other states require entities to adopt written policies and procedures relating to proper disposal and actively monitor compliance with those policies and procedures.[30]

C. Penalties

1. Incorporate UPA penalties

As discussed in detail above, if violations of the DBNA were considered violations of the UPA, then UPA-type civil penalties could be assessed which provide true deterrence no matter the size of the entity. The NMOAG uses the UPA's civil penalty and injunctive provisions to hold corporations large and small accountable for unfair or deceptive conduct affecting New Mexico consumers, from local car dealerships and charter schools to multinational pharmaceutical manufacturers and banking conglomerates.

2. Alternatively, implement a tiered penalty system

As discussed above, the DBNA makes little distinction between a data breach affecting 1,000 residents and a data breach affecting 1 million residents. If incorporating UPA penalties is not possible or practical, New Mexico should consider implementing a tiered penalty system that accounts for (i) how long the breach occurred before detection, (ii) the quantity or character of the PII that was compromised, (iii) the culpability of the breached entity in causing the breach or

[30] *See, e.g.* Alaska Stat. § 45.48.500 *et seq.*; Haw. Rev. Stat. § 487R-2; Mass. Gen. Laws Ch. 93I, § 2; Colo. Rev. Stat. Ann. § 6-1-713 (as amended by H.B. 18-1128).

covering it up, (iv) the size of the breached entity, and (v) the number of consumers ultimately placed at risk.

3. Clearly define what a "violation" is

If penalties (other than failure-to-notify) are to be assessed per violation, it is vital to clearly delineate what constitutes a violation. This is separate from what constitutes a data breach which, standing alone, typically is not a violation of the DBNA. In other words, entities are not in violation of the DBNA simply because they were breached unless that breach occurred due to unreasonably lax security measures. Other than failure-to-notify, statutory violations only clearly occur when (i) an entity fails to properly dispose of information under Section 57-12C-3, or (ii) an entity or its subcontractor fail to implement reasonable security procedures under Sections 57-12C-4 and -5. However, as discussed above, it is unclear whether an entity that fails to properly dispose of five consumers' PII has committed one violation or five. If an entity fails to implement reasonable security procedures, and that failure results in 1,000 New Mexicans having their PII compromised, that entity may have committed one violation or 1,000 violations.

Further, it is unclear whether a failure to perform an appropriate investigation per Section 57-12C-6(B), which then might result in a failure to notify violation, would itself be a separate stand-alone violation of the statute or a failure-to-notify violation. It is also unclear whether a failure to include requisite information in a notice per Section 57-12C-7 would be a stand-alone violation or a failure-to-notify violation. If an entity fails to notify the NMOAG as required under Section 57-12C-10, the statute could be read to impose no more than the ten-dollars-per-instance civil penalty imposed by Section 57-12C-11(C) for failing to notify.

V. CONCLUSION

The DBNA is a vitally important piece of legislation. As more and more New Mexicans live their lives online, more of their sensitive personal data will be placed at risk for unauthorized access and use. Large-scale hacks like those befalling Equifax, Uber, and others are becoming more common, not less. The credit freeze requirements included in the federal Economic Growth, Regulatory Relief, and Consumer Protection Act are helpful after the fact, but these requirements do nothing to prevent breaches in the first instance or ensure proper notice is provided. The proposals contained herein would, if incorporated, (i) provide the NMOAG with the tools needed to more accurately answer the Legislature's questions presented in Senate Memorial 12, and (ii) ensure that owners and licensees of PII have a powerful and enforceable incentive to protect New Mexicans' information and, if those protections fail, to arm New Mexicans with the information they need to protect themselves.