Locke Lord LLP

PRIVACY & CYBERSECURITY NEWSLETTER

AUGUST 2018

IN THIS ISSUE

Locke Lord LLP

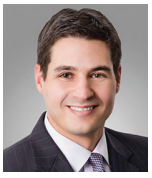
Locke Lord's Privacy & Cybersecurity Newsletter provides topical snapshots of recent developments in the fast-changing world of privacy, data protection and cyber risk management. For further information on any of the subjects covered in the newsletter, please contact one of the members of our privacy and cybersecurity team.

OUR AUTHORS:

Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

Laura L. Ferguson
Partner
Houston
713-226-1590
lferguson@lockelord.com

Brian I. Hays
Partner
Chicago
312-443-1707
bhays@lockelord.com



Ryan M. Holz
Partner
Chicago
312-443-0656
rholz@lockelord.com

Sean Kilian
Staff Counsel
Dallas
214-740-8560
skilian@lockelord.com

Matthew Murphy
Associate
Providence
401-276-6497
matthew.murphy@lockelord.com

P. Russell Perdew
Partner
Chicago
312-443-1712
rperdew@lockelord.com

Douglas R. Sargent
Partner
Chicago
312-443-0384
dsargent@lockelord.com

Chethan G. Shetty
Associate
Chicago
312-443-1887
cshetty@lockelord.com

Andrew Shindler
Partner
London
+44 (0) 20 7861 9077
andrew.shindler@lockelord.com

Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com

Follow the Leader: NYDFS Cybersecurity Regulation Leads the Way for Other States and Industries

The New York Department of Financial Services (NYDFS) blazed a cybersecurity trail with its 2017 regulation for the protection of information collected and processed in, and systems used in the operation of, the financial services and insurance industries. The Empire State's work has already formed the basis for the National Association of Insurance Commissioners' model cybersecurity law, several states' insurance laws, and similar laws for other industries in other states. With "imitation being the sincerest form of flattery," other states and industries are expected to flatter the DFS by adopting similar requirements.

The NYDFS' work has been game-changing and will continue to be highly influential. As important as the NYDFS Cybersecurity Regulation is, however, it would be a disservice not to remember the earlier federal and state governmental laws, regulations and guidances that built a foundation on which the NYDFS has erected its New York cyber skyscraper. Taken together, the legal landscape has been dramatically altered in recent years and more changes are inevitable.

Also, as governmental edicts about cybersecurity proliferate, so too do related requirements about data breach notifications and privacy protections.

The NYDFS Cybersecurity Regulation

After drafts and revisions, and plenty of industry comment, effective March 1, 2017, the NYDFS promulgated its Cybersecurity Regulation (23 NY CRR 500) to address the cybersecurity threats facing "Covered Entities," defined to include all NYDFS licensees, including banks and other lenders, insurance carriers and producers, and others. Beyond other cybersecurity requirements found in existing U.S. laws and regulations, the NYDFS Cybersecurity Regulation expanded the scope of information to be protected by defining "Nonpublic Information" to include the traditional data sets that can expose individuals to identity theft and fraud, as well as information that, if compromised, could cause material harm to the Covered Entity. In addition, the NYDFS Cybersecurity Regulation also expanded the scope beyond information to include "Information Systems," including systems used to process Nonpublic Information, as well as operations systems (including HVAC and telephone systems) needed to operate the Covered Entity's business.

Also beyond other U.S. laws and regulations focused on cybersecurity, the NYDFS Regulation is highly prescriptive in identifying particular written policies and safeguards required to be adopted, particular requirements for general employee awareness and specific employee qualifications and training, and requirements for assessing and managing the cybersecurity risks presented by the Covered Entity's use of third party service providers with access to Nonpublic Information and Information Systems. Most of these requirements are based on a required periodic cybersecurity risk assessment.

In addition, the NYDFS introduced a requirement to notify NYDFS of certain types of cybersecurity events within 72 hours, much quicker than existing U.S. breach notification requirements, but consistent with the notice deadline of the new European Union General Data Protection Regulation (GDPR). The notification requirement is also broader, encompassing certain breaches covered by existing state breach notice requirements, and including certain breaches of systems that could threaten the Covered Entity without compromising the types of information that could expose individuals to identity theft and fraud.

The NAIC Insurance Data Security Model Law

Following the lead of the NYDFS, in October 2017 the NAIC adopted its Insurance Data Security Model Law (NAIC Model) to establish insurance industry standards for data security, and for the investigation and notification of certain cybersecurity events. The NAIC Model applies to any individual or nongovernmental entity licensed, authorized, or registered under the insurance laws, with certain exceptions. An NAIC taskforce had been working on cybersecurity standards for two years, but substantially revised its prior working drafts to follow the concepts and terminology used in the NYDFS Cybersecurity Regulation. The NAIC Model has the potential to affect the entire insurance industry, including InsurTech firms and other service providers with access to the data and systems of insureds and producers.

The NAIC Model, while based on the NYDFS Cybersecurity Regulation, differs from it in several important respects. To address concerns about inconsistency among the states, a drafters' note to the NAIC Model states that Licensees in compliance with the NYDFS Cybersecurity Regulation are deemed to be in compliance with the NAIC Model.

On May 3, 2018, the South Carolina Governor made South Carolina the first state in the nation to adopt a comprehensive cybersecurity statute for the insurance industry, by signing into law the South Carolina Insurance Data Security Act (H4655) based on the NAIC Model, which will become effective January 1, 2019.

Other states can be expected to propose similar legislation based on the NAIC Model. A bill following the NAIC Model was introduced in Rhode Island (Bill 2018 – H7789), although it has been recommended to be held for further study.

Activity by Other Jurisdictions

In 2017, Colorado (3 CCR 704-1 Rules 51-4.8 and 4.14) and Vermont (Vermont 4:4 Vt Code R. § 8:8-4) imposed cybersecurity requirements for the securities industry similar to the NYDFS requirements (which do not apply to securities firms).

In 2018, Colorado (House Bill 18-1128) went further, and adopted general cybersecurity requirements for all entities that maintain, own or license personal identifying information of a Colorado resident. While it does not mandate the same level of specific activity as the NYDFS Cyber Regulation, it does require an entity to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations." (Colo. Rev. Stat. § 6-1-713.5(1)). In this respect, the Colorado statute harkens to the first of the U.S. general cybersecurity requirements, the Massachusetts information security regulation (201 CMR 17), which has since 2009 required all businesses regardless of industry to protect personal information of Massachusetts residents, including by adopting a written information security program, encrypting certain information, managing risks presented by third party service providers, and taking other steps to protect the confidentiality and security of the information.

Colorado is an example of considerable legislative activity in 2018 that focuses chiefly on privacy and notification issues but includes cybersecurity requirements. Other states with new or amended data breach notification and privacy protection laws are Alabama, Arizona, Delaware, Louisiana, Massachusetts, Oregon and South Dakota.

Further, much has been written about the European Union's GDPR that took effect on May 25, 2018. This regulation, with its sweeping privacy considerations, general cybersecurity obligation, and strict notification requirements, should not be overlooked by U.S. enterprises. There are several ways U.S.-based operations can be subject to the GDPR and we encourage all entities to assess carefully its applicability and obligations.

California has taken notice of the GDPR and enacted the California Consumer Privacy Act of 2018 (A.B. 375) on June 28, 2018. [see "Dropping Another Stone in the Pond? California's New Consumer Privacy Act" in this issue.] It is viewed as a compromise to avoid a November statewide ballot on an initiative of the same name. While it does not take up the NYDFS Cybersecurity Regulation's prescriptive security requirements, this law, which takes effect in January 2020, closely tracks the various privacy concepts of the GDPR. Given the role California played in adopting the first breach notification statute in the U.S., which then rippled across the nation to be adopted in one form or another in every state, observers are closely following this new California legislation. Among the requirements of the California Consumer Privacy Act are a duty to maintain reasonable security; an obligation to disclose the types of data being collected about California consumers; the requirement to produce to a consumer the categories, as well as the specific pieces, of information collected; and a right to be forgotten.

What's Next?

Looking ahead, there will certainly be further governmental attention at all levels in response to ever-increasing awareness of cybersecurity risks, the consequences of incidents, privacy concerns, and more. This attention can manifest, for example, in new laws or regulations, changes to existing law, and heightened enforcement. Also, as industry sectors wrestle with their potential challenges and exposures, industry-specific standards will continue to emerge.

The goal of any business should be risk mitigation, not merely compliance with applicable requirements. Therefore, those charged with assessing and managing privacy and cybersecurity risks at their organizations must continually monitor the evolving landscape of standards and requirements. Currently, the NYDFS Cybersecurity Regulation provides a useful model for managing these risks, regardless of industry.

This article was originally published in CPO Magazine July 16, 2018. Used with permission.

Biometrics: Illinois Supreme Court to Decide Whether Injury Is Required for Biometric Information Privacy Act Claims

On May 30, 2018, the Illinois Supreme Court accepted an appeal from an Illinois appellate court's decision rejecting "no-injury" lawsuits under Illinois's Biometric Information Privacy Act (BIPA) [Dkt. No. 123186]. The Court's ultimate decision will likely either sharply restrict claims alleging only technical BIPA violations or reopen the floodgates for putative class actions in Illinois after they were slowed dramatically by the appellate court in *Rosenbach v. Six Flags Entertainment Corp., et al.*, 2017 IL App (2d) 170317. The decision could also substantially impact the massive BIPA litigation currently pending in federal court against Facebook, in which the Ninth Circuit is currently reviewing the propriety of a multi-million member certified class.

BIPA Regulates Private Entities' Collection, Storage, and Use of Biometric Information

BIPA prohibits private entities from obtaining or using an individual's biometric information without first providing defined notices and obtaining written consent to do so. 740 ILCS 14/15(a), (b). BIPA allows any "person aggrieved" by a statutory violation to sue for either actual damages or "liquidated damages" of between $1,000 and $5,000, plus attorneys' fees and injunctive relief. 740 ILCS 14/20.

"Person aggrieved" is not defined in the statute, which has led to conflicting decisions about whether an actual injury is required. Compare *McCollough v. Smarte Carte, Inc.*, 2016 WL 4077108, at *4 (N.D. Ill. Aug. 1, 2016) (dismissing BIPA action for lack of actual damages) and *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 521 (S.D.N.Y. 2017) (dismissing BIPA claim where there was no injury attributable to procedural BIPA violation), aff'd 2017 WL 5592589 (2nd Cir. Nov. 21, 2017) with *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846, at *9 (N.D. Ill. Sept. 15, 2017) (rejecting argument that "person aggrieved" requires an actual injury) and *In re Facebook Biometric Information Privacy Litigation*, 2018 WL 1794295, at *7 (N.D. Cal. Apr. 16, 2018) (holding that a statutory violation is an invasion of privacy sufficient to create statutory standing to sue, and that no further tangible injury (such as identity theft or financial loss) needs to be shown).

The *Rosenbach* Appellate Decision Sharply Limited Who Could Sue Under BIPA

Rosenbach is the first and only Illinois appellate decision to consider whether a plaintiff must allege harm to be "aggrieved" and thus have statutory standing to sue. There, defendants allegedly collected class members' fingerprints in connection with purchases of season passes to defendants' theme park. The appellate court held that "[a]lleging only technical violations of the notice and consent provisions of the statute … does not equate to alleging an adverse effect or harm." 2017 IL App (2d) 170317, ¶ 21. Thus, the court held, "a plaintiff who alleges only a technical violation of the statute without alleging some injury or adverse effect is not an aggrieved person under" BIPA. *Id.* ¶ 23. But an injury or adverse effect need not be pecuniary. *Id.* ¶ 28.

While the *Rosenbach* decision has significantly diminished the number of new BIPA filings in Illinois, its impact has been in question since a California federal court rejected it in *In*

re Facebook Biometric Information Privacy Litigation, 2018 WL 1794295 (N.D. Cal. Apr. 16, 2018). There, a class of individuals suing Facebook under BIPA was certified despite Facebook's argument that each class member would need to show that they had suffered a tangible injury to be "aggrieved" and thus eligible for statutory damages under BIPA. *Facebook*, 2018 WL 1794295 at *6-8. The court disagreed with and distinguished *Rosenbach*, holding that an individual need only show a statutory violation—and need not show a resulting tangible injury—to sue. *Id.* at *6–7.

The Supreme Court's Decision Will Substantially Affect Pending and Future BIPA Litigation

In deciding the *Rosenbach* appeal, the Supreme Court will likely decide whether a "person aggrieved" includes a plaintiff who has experienced only a technical statutory violation or whether an actual injury is required as well. The decision will be binding on Illinois courts as well as federal courts applying BIPA. If the Supreme Court in *Rosenbach* affirms the appellate court, the dozens of class actions currently pending in Illinois state courts will likely be subject to dismissal. At the very least, a *Rosenbach* affirmance will make class certification very difficult because whether each class member suffered an injury would be an individualized determination. Similarly, in the *Facebook* case—which the Ninth Circuit has stayed pending an interlocutory appeal of the class-certification order—Facebook would likely argue that individualized damages issues should preclude class certification. On the other hand, if the Supreme Court finds no actual-injury requirement for a BIPA claim, the class actions pending in Illinois will likely become more treacherous for defendants and the Ninth Circuit will be much more likely to affirm the class-certification order in *Facebook*.

Dropping Another Stone in the Pond? California's New Consumer Privacy Act

California may have again taken the privacy protection lead among U.S. jurisdictions with the Governor's signing on June 28, 2018 of the California Consumer Privacy Act of 2018 (AB 375) (the "Act"). Privacy and security professionals will remember the ripple effect of California's first-in-the-nation data breach notification statute in 2003, which was ultimately taken up with variations throughout each of the United States. This has resulted in a patchwork of state data breach requirements that have been challenging and expensive for businesses to address. With the last of the states only just now on board with some form of data breach notification requirement, has California dropped another stone in the pond?

Unanimous Compromise

The Act unanimously passed both houses of the California legislature as a compromise measure intended to undercut an even more stringent and onerous ballot initiative of the same name scheduled for the November elections. The Act will become effective in January 2020, and may well be subject to further amendments between now and then.

European Inspiration; Broad Application

The new California law was clearly inspired by the privacy and data security protections of the General Data Protection Regulation (GDPR) of the European Union, which took effect on May 25, 2018. It follows several themes of the GDPR, including consumer rights (i) to know what personal information is collected about them; (ii) to prevent the sale of personal information; (iii) to know categories of personal information (if not the actual data) shared with third parties; and (iv) to be forgotten by requiring deletion of personal information. While the GDPR uses the term "personal data," and California uses "personal information," both terms are defined broadly to include essentially any information that identifies or is reasonably identifiable of an individual. Companies that will be subject to both the Act and the GDPR will, however, need to consider several nuances in the definitions. For example, the Act excludes information that is publicly available from its definition of personal information, while the GDPR does not have such an exclusion from the definition of personal data.

Who is Subject? Who is Protected?

The Act applies to any business that collects personal information about California consumers if it does business in California and meets one of the following thresholds:

- Annual gross revenues in excess of $25 million;
- Annually buys, receives for commercial purposes, sells, or shares for commercial purposes, personal information of 50,000 or more consumers, households or devices; or
- 50 percent or more of annual revenues are derived from selling consumers' personal information.

Consumer includes any identifiable natural person who is a California resident.

What is Required?

As noted above, many of the themes of the Act track the GDPR. More specifically, businesses that collect personal information from California consumers must prepare now for the following requirements to become effective in 2020:

Notice Requirement: At or before the time of collecting personal information, the business must provide notice of the categories of personal information to be collected, and the purposes for which they will be used.

Disclosure Requirements: Upon request of a consumer, the business must disclose:

- the categories and specific pieces of the consumer's personal information the business has collected;
- the categories of sources from which personal information is collected;
- the business or commercial purpose for collecting or selling personal information; and
- the categories of third parties with whom the business shares personal information.

Delivery of Personal Information: Upon request of a consumer, up to twice in a 12-month period, the business must deliver to the consumer all of the consumer's personal information collected.

Right to be Forgotten: Each business must notify consumers of their right to request the business to delete all of the consumer's personal information. Certain exceptions permit the business to retain personal information for specific purposes.

Non-Discrimination: With limited exceptions, businesses are prohibited from discriminating against a consumer because the

consumer exercised any of the consumer's rights under the Act, including denying goods or services, charging different prices, providing a different level of quality of goods or services, or suggesting that the consumer will receive a different price or level of quality of goods or services.

Private Right of Action, in Some Circumstances

Under certain circumstances, a consumer can pursue a private right of action if the California Attorney General does not pursue enforcement of the Act and the consumer's personal information was subjected to unauthorized access, exfiltration, theft, or disclosure as a result of a business's violation of the duty under the Act to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the information. A consumer can sue over a violation and recover the greater of actual damages or statutory damages of between $100 and $750. The Act gives a business a 30-day period to cure the violations identified by the consumer. If the business confirms in writing that the situation has been corrected and will not recur, no suits for statutory damages can occur. In addition, the consumer must advise the California Attorney General within 30 days of a lawsuit. The Attorney General then has 30 days to either supersede the private action and pursue its own action or to permit the private action to proceed. It may be the topic of further legislative discussion whether the Act requires a consumer to demonstrate actual injury to file suit or whether an allegation of a violation of the Act involving the consumer's personal information is sufficient. On a related note, the Act bars any contractual limit on a consumer's right to recovery, which could prohibit contracts requiring arbitration as an exclusive form of dispute resolution.

What Should Businesses Do Between Now and 2020?

As noted above, amendments between now and the Act's effective date are possible, but businesses need to start planning now. First, if the history of breach notification laws is any indication, one can expect that other states will follow California's lead in adopting privacy protections that echo the themes established by the GDPR. Second, given the size of California's economy, many businesses will be subject to the requirements of the Act, whether or not other states adopt their own privacy legislation.

Given the nature and extent of the Act's requirements, compliance will take a lot of planning and effort for many businesses. Businesses that collect personal information from California consumers should take the following steps in preparation for the effectiveness of the Act:

- Collection of personal information. Inventory how and from whom personal information is collected.
- Use of personal information. Catalogue all of the current and intended uses for personal information.
- Sale and sharing of personal information. Identify all parties to whom personal information is sold, and with whom personal information is shared.
- Map personal information held by the business and its service providers. If consumers exercise their right to provide personal information collected by the business, or their right to be forgotten, the business will need to know where the information is located.
- Develop policies and protocols for meeting the requirements of the Act. Businesses will need to be organized in order to comply with requests from consumers to provide requested disclosures, or to delete personal data.
- Review safeguards for protecting personal information. Given the private right of action and the potential for Attorney General enforcement, in the event of a breach of the confidentiality or security of personal information, businesses should review their safeguards and make appropriate adjustments to protect personal information and mitigate the risk of a breach that could give rise to litigation or enforcement.

State Legislative Action on Data Breach Laws

The changes keep coming! In 2018, state legislatures have been active in enacting and amending data breach notification laws. With Alabama's recent enactment, all 50 states now have data breach notification laws. The following summary highlights recent legislative action on state data breach notification laws, some of which require immediate action for preparedness and compliance:

Massachusetts: On February 1, 2018, the Massachusetts Attorney General's Office rolled out a new online form for submitting data breach notifications, as an efficient alternative to notifying the AG's office by paper letter or email.

Delaware: On April 14, 2018, Delaware's amendment to its data breach notification law took effect, which, among other changes, expands the definition of "personal information" to include biometric and other health information, imposes a 60-day notice deadline, and requires 1 year of free credit monitoring if an individual's Social Security number is breached.

Alabama: Effective June 1, 2018, Alabama's data breach notification law applies to any person or entity that acquires and uses sensitive personally identifiable information (PII) of Alabama residents. Sensitive PII is defined as an individual's first name or initial and last name in combination with (i) non-truncated SSN; (ii) non-truncated driver's license number/passport number/military ID number/other unique ID number issued on a government document used to verify identity; (iii) financial account number (bank account, credit card, debit card) with security code/access code/PIN/expiration date; (iv) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (v) an individual's health insurance policy number/subscriber ID and any unique ID used by the health insurer to identify an individual; and (vi) a user name or email address with password or security question (and answer) permitting access to an online account affiliated with the person/entity that acquires and uses the sensitive PII. Subject to a harm threshold, notification to an affected individual is required as a result of the unauthorized acquisition of electronic sensitive PII. In the event more than 1,000 consumers are being notified, the Alabama Attorney General and consumer reporting agencies must be notified.

Oregon: Effective June 2, 2018, Oregon amended its data breach notification law to expand the scope of individuals or entities that are required to report breaches to include individuals or entities that "otherwise possess" personal information, require that notice is provided no later than 45 days after discovery (except for HIPAA covered entities), and include biometric and certain other health information in the definition of personal information.

South Dakota: Effective July 1, 2018, South Dakota's data breach notification law applies to any person or entity conducting business in South Dakota that owns or licenses computerized personal or protected information of South Dakota residents. "Personal information" includes (i) Social Security number; (ii) driver's license number or other unique identification number created or collected by a government body; (iii) account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account; (iv) health information as defined in 45 CFR 160.103; or (v) identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes. "Protected information" includes (x) user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and (y) account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account. Subject to a harm threshold, notification to an affected individual and consumer reporting agencies is required as a result of the unauthorized acquisition of unencrypted or encrypted (with the encryption key) computerized personal or protected information. If relying on the harm threshold to avoid notification, notification must be provided to the Attorney General. In the event more than 250 South Dakota residents must be notified, notification to the Attorney General is required.

Virginia: Effective July 1, 2018, Virginia's data breach notification law was amended to require income tax preparers to notify the Virginia Department of Taxation of breaches of unencrypted and unredacted "return information," within a reasonable time. Under the amendment, "return information" is defined as "a taxpayer's identity and the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, assessments, or tax payments. 'Return information' does not include information that is lawfully obtained from publicly-available information or from federal, state, or local government records lawfully made available to the general public."

Louisiana: On August 1, 2018, Louisiana's amendment to its data breach notification law will take effect. The amended Louisiana law expands the definition of "personal information" to include a Louisiana resident's first name or first initial and last name in combination with a state identification card number, a passport number, and/or biometric data, in addition to other previously-specified data elements. Further, Louisiana law will require companies to implement and maintain reasonable security procedures to protect personal information from unauthorized disclosure, including reasonable procedures for destroying personal information that is no longer to be retained. Louisiana law will also generally require data breach notifications no later than 60 days from discovery of a breach.

Arizona: Effective August 3, 2018, Arizona will expand its data breach notification law in several important ways. The amended Arizona law expands the definition of "personal information" to include an individual's first name or first initial and last name in combination with either the individual's private electronic key, health insurance identification number, medical information, passport number, taxpayer ID number, and/or unique biometric data, in addition to other previously specified data elements. Additionally, in the event of a data breach, the owner of the data generally must notify the affected individuals within 45 days, and may face civil penalties in the amount of the economic loss sustained by affected individuals, up to $500,000.

Colorado: On September 1, 2018, Colorado will set a 30-day deadline for notification of data breaches, among the shortest in the country. The amended Colorado law also expands the entities subject to its regulation to any person that "maintains, owns, or licenses personal identifying information in the course of the person's business, vocation, or occupation" that identifies a Colorado resident (regardless of whether the entity does business in the state of Colorado, which was the prior determinant). Additionally, covered entities will be required to implement reasonable and appropriate security procedures to protect the PII it maintains, owns, or licenses, and to ensure that any third-party service providers similarly have procedures that protect the PII.

Vermont: Effective January 1, 2019, an amendment to a Vermont law – the first of its kind – will impose special data breach notification requirements on "data brokers," which are defined as businesses that knowingly collect and sell, or license to third parties, the brokered personal information of a consumer with whom the business does not have a direct relationship. Data brokers will be required to report "data broker security breaches" to the Vermont Secretary of State as part of their annual registrations. A "data broker security breach" is the unauthorized acquisition of unencrypted or unredacted "brokered personal information," which includes a consumer's name, address, date of birth, place of birth, mother's maiden name, biometric data, names or addresses of the consumer's immediate family or household members, social security or government identification number, and other personally identifiable information. The amendment also imposes detailed technical security requirements on data brokers for the protection of brokered personal information. The failure to comply with the security requirements is treated as an unfair and deceptive practice that is subject to enforcement measures, including penalties and civil action.

The on-going process of updating data privacy and security policies and practices to reflect the changing landscape in state data breach and data security laws should incorporate the following actions:

- Inventory: create/update a data map for personally identifiable information and conduct a risk assessment (or update, if last assessment was conducted over a year prior);
- Process: create/update (and implement) a written information security plan;
- Response: create/update (and practice implementing) an incident response plan, including a document retention provision; and
- Training: train key employees on handling personally identifiable information, executing the written information security plan, and executing the incident response plan.

Third Circuit Limits ATDS Definition under the TCPA to Random Number Dialers

In the most significant case to interpret what constitutes an "automatic telephone dialing system" (ATDS or autodialer) under the Telephone Consumer Protection Act (TCPA) in the wake of the D.C. Circuit's decision in ACA Int'l v. FCC, the Third Circuit dealt a major blow to TCPA plaintiffs. *See Dominguez v. Yahoo, Inc.*, 894 F.3d 116 (3d Cir. 2018). The Third Circuit affirmed summary judgment in favor of Yahoo on Dominguez's claim that Yahoo sent him an eye-popping 27,800 text messages in violation of the TCPA. The narrow issue before the appellate court was whether the equipment used by Yahoo to send the text messages qualifies as an ATDS, which is a required element of a TCPA claim.

Answering in the negative, the Third Circuit applied the plain language of the TCPA to hold that dialing equipment must have "present capacity to function as an autodialer by generating random or sequential telephone numbers" when it is used to send text messages.

Background and Procedural History

Dominguez purchased a cell phone that came with a reassigned telephone number. The prior owner of the number used a Yahoo e-mail account and signed up for Yahoo's "Email SMS Service" that provided a text message notification each time an e-mail was received by the user's e-mail account. Unfortunately for Dominguez, the prior owner of the number never canceled the notification service, so Dominguez received a text message every time the prior owner received an e-mail. Despite Dominguez making repeated attempts to have the notification service canceled, Dominguez ultimately received approximately 27,800 text messages in a 17-month span.

Dominguez filed a putative class action alleging that Yahoo violated the TCPA by sending him text messages using an ATDS without his prior express consent. After the district court initially granted summary judgment in favor of Yahoo, Dominguez appealed. During the pendency of this initial appeal, the Federal Communications Commission (FCC) issued a declaratory ruling and order interpreting the word "capacity" in the definition of an ATDS to "include any latent or potential capacity" (2015 Order), causing the Third Circuit to vacate the judgment and remand the case. On remand, the district court again granted summary judgment in favor of Yahoo, and Dominguez again appealed. During this second appeal, the D.C. Circuit issued its much-anticipated opinion in *ACA Int'l*.

The Third Circuit's Decision

The Third Circuit began its analysis by noting that the *ACA Int'l* decision narrowed the scope of Dominguez's appeal. Without providing any real insight into its rationale, the Third Circuit then concisely stated that it would "interpret the statutory definition of an autodialer as we did prior to the issuance of" the FCC's 2015 Order. That interpretation meant that Dominguez would have to provide sufficient evidence to create a genuine issue that Yahoo's dialer had the present capacity to generate random or sequential telephone numbers at the time the disputed messages were sent.

After reviewing several expert reports, the Third Circuit held that Dominguez "cannot point to any evidence that creates a genuine dispute as to whether the Email SPS Service had the present capacity to function as an autodialer by generating random or sequential telephone numbers and dialing those numbers." To the contrary, the court noted that the evidence indicates that the dialer utilized by Yahoo only sent text messages to telephone numbers that had been individually and manually entered into its system. While the Third Circuit acknowledged that Dominguez likely "suffered great annoyance," it affirmed summary judgment in favor of Yahoo because it did not utilize an ATDS to send those messages—"those messages were sent precisely because the prior owner of Dominguez's telephone number had affirmatively opted to receive them, not because of random number generation."

Going Forward

Corporate defendants and telemarketers should take advantage of the *Dominguez* decision to try to eliminate lawsuits based on dialing systems that cannot generate random or sequential numbers. They should do so before the FCC or Congress have an opportunity to expand the definition of an ATDS. A new definition of an ATDS is expected from the FCC in a matter of months. Democrats in Congress have introduced the "Stopping Bad Robocalls Act" that would expand the definition of an ATDS to specifically include equipment that makes a series of calls to stored telephone numbers, including telephone numbers stored on a list. While there is no way to tell for sure how an ATDS will be defined six months or a year from now, it is hard to imagine that the definition will be any narrower than the Third Circuit's interpretation in *Dominguez*.

South Carolina Department Clarifies Confusing Change in Its New Insurance Data Security Act

As reported on Locke Lord's InsureReinsure blog, the NAIC adopted a model law for the protection of the data and systems used by the insurance industry, and South Carolina became the first state to enact legislation based on the NAIC model. In doing so, however, the South Carolina legislature created some uncertainty by changing a couple of words.

The purpose of the NAIC model is to protect the insurance industry and its consumers against cybersecurity threats by requiring licensees to adopt certain cybersecurity measures. Apparently seeking to avoid the confusion and expense related to divergent requirements that could apply to licensees (the inconsistent state breach notification requirements are a perfect example!), the NAIC model contains an express exception for licensees that certify compliance with HIPAA. In the same spirit, it also includes a drafting note stating that compliance with the previously existing New York Department of Financial Services Cybersecurity Regulation is deemed to be in compliance with the NAIC model.

A simple change in wording of the HIPAA exception, however, created some confusing daylight between the South Carolina law and the NAIC model. The South Carolina statute revised the wording of the NAIC model's HIPAA exception from "compliance, with the same" (referring to HIPAA) to "compliance with, the provisions of this chapter." (Emphasis added.) A literal

reading of the South Carolina language would create an inherent inconsistency: licensees that comply with HIPAA are excepted from the South Carolina law if they comply with, and certify compliance with, the provisions of the South Carolina law.

Fortunately, on June 14, 2018 the South Carolina Director of Insurance issued Bulletin Number 2018-02 describing the exceptions from the South Carolina Insurance Data Security Act to include, "Licensees that are able to certify compliance with the requirements of [HIPAA] via a written certification will be deemed to meet the requirements of the [South Carolina law]." This statement clearly reflects the intent of the NAIC model, and indicates that the South Carolina Department of Insurance will implement the South Carolina law in a way that will make sense of the otherwise minor but confusing change in the language of the statute.

Testing the Limits III – Cyber Coverage Litigation Focuses on Computer Fraud Losses

Fraudsters deploy different computer-related techniques but toward the same end – "gaming the system" for their own financial gain. Some victims turn to insurance for recovery. Four recent federal appellate decisions reveal courts' continued analysis of whether policies with computer fraud, funds transfer fraud, crime or other coverages respond to such losses of funds. These recent opinions, which come from four different appellate circuits, stress the significance of specific policy language and the particular facts of the scams.

The federal Ninth Circuit kicked off the recent flurry of activity in April 2018. In *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of America*, 719 F. App'x 701 (9th Cir. 2018), the insured received a fraudulent email from one of its vendors requesting that the insured change the vendor's bank account information. The insured manually changed the account information and future wire transfers were sent to the hacker's account. The insured sought coverage under the computer fraud provision of its crime policy. The trial court granted summary judgment to the insurer based on an exclusion that the policy "will not apply to loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System ...." *Id.* at 702. The appellate court affirmed that the exclusion barred coverage.

In May 2018, the federal Eleventh Circuit ruled for the insurer in *Interactive Communications Int'l, Inc. v. Great Am. Ins. Co.*, No. 17-11712, 2018 WL 2149769 (11th Cir. May 10, 2018). Fraudsters manipulated the insured's computerized interactive telephone system, allowing them to load value onto debit cards from a single redemption multiple times instead of just once. The debit cards were then used for various purchases, which were honored by the debit card bank based on the value in a debit card account. The insured sought coverage under its computer fraud policy (coverage for "loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises: (a) to a person (other than a messenger) outside those premises; or (b) to a place outside those premises."). *Id.* at *2. The trial court, applying Georgia law, found no coverage for losses incurred from unauthorized redemption, holding both that the redemptions were not made through computers and that the redemptions were not the direct cause of the insured's losses. The appellate court affirmed on the grounds that the loss of money did not result "directly" (that is, "straightaway, immediately, and without any intervention or interruption") from the use of a computer system and was also "temporally remote". *Id.* at *4. The reviewing court did, however, disagree with the trial court's finding that computers were not involved.

The busy season ramped up with two decisions in July. The federal Second Circuit in *Medidata Solutions, Inc. v. Federal Insurance Co.*, 729 F. App'x 117 (2d Cir. 2018), agreed with the lower court that the insured was entitled to coverage under New York law. The case concerned fraudulent funds transfers resulting from spoofed emails when the insured's employee believed the requests had come from the company's president. The appellate court agreed with the insured that the computer fraud provision of the policy applied because "the fraudsters ... crafted a computer-based attack that manipulated [its] email system" that resulted in "a fraudulent entry of data into the computer system [the spoofing code]" and which altered "the email system's appearance ... to misleadingly indicate the sender." *Id.* at 118. The appellate court further concurred with the lower court that the insured's loss was the direct result of the computer fraud. Noting that under New York law a "direct loss is equivalent to proximate cause," the court concluded that:

> [T]he spoofing attack was the proximate cause of [the insured's] losses. The chain of events was initiated by the spoofed emails, and unfolded rapidly following their receipt. While it is true that the [insured's] employees themselves had to take action to effectuate the transfer, we do not see their actions as sufficient to sever the causal relationship between the spoofing attack and the losses incurred.

Id. at 119.

And still one more ruling in July. Unlike the other three decisions, all of which affirmed the lower courts, the federal Sixth Circuit reversed the trial court in *American Tooling Center, Inc. v. Travelers Cas. and Sur. Co. of Am.*, No. 17-2014, 2018 WL 3404708 (6th Cir. July 13, 2018). The insured was hoodwinked by emails purporting to be from one of its vendors into sending money to the impersonator's bank accounts. The lower court said that the insured's crime policy covered "direct loss" of funds "directly caused by computer fraud" which was defined as "the use of any computer to fraudulently cause a transfer of money." The lower court concluded, under Michigan law, that the loss was not direct because it was not immediate and due to the intervening steps taken by the insured between the time it received the fake emails and the time it effected the three wire transfers. The Sixth Circuit disagreed, citing Michigan law indicating that "direct" means "immediate or proximate" as opposed to "remote or incidental." *Id.* at *4. Also, although the insurer characterized the use of computers as not enough to render a fraud a "computer fraud," the appellate court noted that "here the impersonator sent [the insured] fraudulent emails using a computer and these emails fraudulently caused 'the insured' to transfer the money to the impersonator." *Id.* While the insurer, according to the court, seemed to want to limit "computer fraud" to "hacking and similar behaviors," the policy's definition did not reflect such a limitation. The court also summarily rejected application of three policy exclusions raised by the insurer.

Another decision awaits treatment by the federal Eleventh Circuit. Oral argument is currently scheduled for November 2018 in *Principle Solutions v. Ironshore Indemnity Co.*, No. 1:15-CV-4130-RWS, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016). There, the trial court determined that, under Georgia law, there was coverage under a crime policy for a funds transfer resulting from spoofed emails. The court said that the policy's computer and funds transfer fraud provision providing coverage for loss "resulting directly from a 'fraudulent instruction' directing a 'financial institution'" to debit the insured's account was ambiguous and that intervening steps between receipt of the fake email and the funds transfer did not bar coverage. *Id.* at *5. According to the lower court's opinion, "[i]f some employee interaction between the fraud and the loss was sufficient to allow [the insurer] to be relieved from paying under the provision at issue, the provision would be rendered 'almost pointless' and would result in illusory coverage." *Id.*

The judicial scrutiny is not over, as coverage actions remain pending throughout the country, seeking a determination under commercial crime/computer fraud policies. Also, new matters continue to be filed. *See, e.g., Quality Plus Services, Inc. v. Nat'l Un. Fire Ins. Co. of Pittsburgh, PA*, No. 3:18-cv-00454 (E.D. Va. filed Jul. 2, 2018).

Although the ways in which these computer-related schemes operate often reflect cutting-edge technologies or new techniques, courts wrestle with coverage issues that have long been at the heart of insurance disputes. What is the policy's language? What jurisdiction's law controls? What constitutes a direct loss or proximate cause? What are the public policy issues concerning the scope of policy provisions? These recent decisions illustrate that insureds and insurers face a wide array of arguments that will mark the legal landscape. Disputed claims will continue to shape the body of law that both insureds and insurers should consider in their insurance transactions going forward.

OCR For the Win: MD Anderson HIPAA Enforcement Action

Once again, an Administrative Law Judge (ALJ) upheld the imposition of civil money penalties charged against a covered entity by the Office for Civil Rights of the Department of Health and Human Services (OCR) for violations of the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). And this time, the penalties are substantial – $4.3 million.

Typically, covered entities cooperate with OCR and enter into a resolution agreement that indicates the covered entities potentially violated HIPAA, sometimes with the payment of a resolution amount. In this case, however, MD Anderson refused to settle and took the position that it had not violated HIPAA because (i) the electronic protected health information (ePHI) was lost or stolen, and (ii) the incident occurred when its employees violated the company's policies against storing ePHI on mobile devices and not taking ePHI offsite. The ALJ relied on uncontested evidence that established MD Anderson had an encryption policy for ePHI, but failed to implement said policy with respect to mobile devices, including laptops and USB drives. MD Anderson argued that it was not required by HIPAA to encrypt all devices and that it implemented other "mechanisms" to protect the ePHI (e.g., passwords, training). The ALJ found that was no defense and stated that "Respondent's [MD Anderson's] liability – and its culpability – emanates from its failure to address the risk that ePHI could be disclosed via the theft or loss of mobile devices containing such information."

The interesting part of this case is the size of the penalties and the arguments put forward by MD Anderson regarding the statutory caps on civil monetary penalties that are permitted to be imposed under HIPAA. Unfortunately for MD Anderson, the ALJ was only delegated authority to review OCR's imposition of penalties under the regulations with respect to reasonableness and was not permitted to declare the regulations to be beyond OCR's authority or to declare proposed penalties to be arbitrary and unconstitutional. In the absence of an appeal, MD Anderson now owes civil money penalties of $4.3 million due to its violations of HIPAA.

You can read the ALJ's opinion here and the OCR press release here.

The GDPR – Some Troublesome Aspects and Misconceptions, Part I: Application of the Regulation

After much publicity, the European Union's General Data Protection Regulation, commonly known as the GDPR, came into effect on May 25 this year.

As most people now know, the GDPR does not just apply to organizations incorporated or located in the EU. The GDPR will apply to a non-EU organization under any one of three criteria:

- it has an "establishment" in the EU;
- it offers goods or services to individuals in the EU; or
- it monitors the behavior of individuals in the EU.

But these criteria can be difficult to apply in practice and the exact effect is not always clear.

Another issue which has caused great confusion is the link between sending marketing materials and consent. You are almost certain to have received multiple communications in the lead-up to May 25th saying that unless you "opt in," a company you have previously dealt with can no longer contact you or keep you on its database. In many cases, this is a misconception.

We explore the first difficulty below. In our next issue, we'll discuss the database question.

Processing by an Establishment in the EU

If an organization has an "establishment" in the EU, the GDPR applies to the processing of personal data in the context of its activities, regardless of where the processing takes place.

The only light that the GDPR shines on the meaning of an establishment is that it *"implies the effective and real exercise of activity through stable arrangements" and that "the legal form of such arrangements, whether through a branch or a subsidiary with a legal personality is not the determining factor."*

Examples typically given of an establishment which does not involve a separate legal personality include an office, however small, or the appointment of an agent. It is also arguable that having a contract with a third party based in the EU might, depending on its nature, give rise to an establishment – for example, an outsourcing or distribution arrangement.

So the first difficulty may be in deciding whether you have an establishment.

The second difficulty with this test is how far it extends into an organization which has an establishment in the EU but also outside the EU. If the organization is a group of companies or limited partnerships, some inside and some outside the EU, or has offices both inside and outside the EU, is it only the processing by those within the EU that is subject to GDPR or the whole organization? Or does it depend on the organization's structure? Alternatively, it may depend, at least in part, where the data subject is located, inside or outside the EU. The possibilities here are multiple; consider the following example:

A U.S. company with London and Paris offices, but no separate legal entity, processes personal data of individuals. Is it only the data processing carried out by its London and Paris offices which is subject to GDPR? Or are these offices part of one larger establishment, thus subjecting all data processing activity throughout the company to GDPR – bearing in mind that for this criterion of GDPR applicability, it does not matter where the processing actually takes place. If the establishment is the whole company, does this mean that, where the Chicago office processes personal data on U.S. resident citizen employees, such employees can claim powerful GDPR rights?

Would the above conclusion be different if the London and Paris operations were conducted through subsidiaries?

Unfortunately the answers to these questions remain unclear and different organizations have taken different approaches.

Offering Goods and Services

The GDPR applies to businesses without an EU establishment if they process the personal data of individuals who are in the EU when offering them goods or services, regardless of whether any payment is charged. This applies to the processing of personal data of any data subjects who are "in" the EU, regardless of their nationality or residency. It therefore covers the personal data of EU citizens, residents and temporary visitors.

What constitutes "offering" goods or services depends on intention rather than mere availability of its goods or services. Simply having a website in local language and currency with products or services available for purchase is not enough, but if the website is in an EU language which is not native, or quotes prices in an EU currency such as euros or GBP, or mentions customers or users in the EU, then GDPR will likely apply.

However, it is important to note here that the application of GDPR here does not seem so wide as where there is an EU "establishment," as described above. GDPR only applies in this case where the processing activities are related to offering goods or services to data subjects in the EU. It is fairly clear that if a U.S. company had a U.S.-based website targeted at the EU as well as the U.S., it would only have to worry about GDPR compliance in relation to its users based in the EU. But there is a danger here that in carrying out such compliance and providing data subjects with information provided by GDPR, the U.S. company might by contract inadvertently offer U.S. resident citizens' rights they would not otherwise have.

Monitoring

Finally, the GDPR applies where an organization processes personal data of data subjects who are in the EU where it relates to monitoring their behavior which takes place within the EU.

"Monitoring" is not defined in the GDPR, but the Recitals state: "to determine whether processing can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling ...."

So the meaning seems to be following someone's internet activity, such as their browsing or purchasing activities, but it is not clear if it could be wider than that to include monitoring of other activities, or whether it is necessary for there to be subsequent profiling, although it seems not.

As with the offering of goods and services, the GDPR will only apply here to internet activity which takes place in the EU by individuals located there and not to the monitoring of U.S. resident citizens. However, since the test is not of citizenship or residency, but rather where the data subject is located at the time, GDPR will apply if the internet activity is of U.S. citizens while on a business trip or vacation in the EU.

Locke Lord Presents Workshops on Cybersecurity Risk in Vendor Management in Chicago and Hartford; Will Reprise in Houston and Dallas in the Fall

Third party vendors, outsource providers, and cloud providers are critical to the operations of all organizations. Yet they also introduce a significant cybersecurity risk. A recent survey indicates that as many as 63% of all data breaches may be caused by such third-party vendors and service providers. In response, cybersecurity regulations increasingly focus on the need to address the risks introduced by such service providers, and require that vendor management be a key component of all business security programs. Highly publicized examples include the New York Department of Financial Services Cybersecurity Regulation and the EU General Data Protection Regulation (GDPR).

Locke Lord tackled these issues during workshops offered on April 10 in our Chicago office and on April 12 in our Hartford office to CEOs, CFOs, CIOs, CISOs, CPOs, CCOs, GC's, In-house Counsel, and Risk Managers. Members of Locke Lord's Privacy & Cybersecurity Group Ted Augustinos, Pat Hatfield, Andrew Shindler, Tom Smedinghoff and Molly McGinnis Stine, along with Locke Lord Director of Security Andy Sawyer, presented an in-depth review of the key regulatory requirements for vendor cybersecurity, followed by a presentation of the Firm's seven-point guide for implementing an effective and compliant Vendor Management Program to address this critical cybersecurity risk. The workshops covered the following:

- "Legs and Regs" – Vendor management is not only essential good business practice but also, in many cases, a fundamental and ongoing legal requirement
- Due Diligence and Selection – How to vet and select potential suppliers
- Onboarding – Explore terms and conditions to include in contracts and ways to implement them
- Monitoring – How to ensure vendors and suppliers are assessing the cyber risks they face, both internally and with their own service providers
- Governance – How the program can work within your organization's larger cyber risk management program
- Off-Boarding – Developing a process for handling termination of the relationship with a given service provider
- Equipoising – Balancing a number of competing factors to arrive at a compliant and sensible program for your organization

The workshops were very well received, and the Locke Lord Privacy & Cybersecurity Group is now planning to repeat for audiences on **Wednesday, September 12 in Houston** and **Thursday, September 13 in Dallas**. For more information, or to sign up, please contact Maureen McNair at Maureen.mcnair@lockelord.com.