











IN THIS ISSUE

- 2  [Our Authors](#)
- 3  [Tax Season Brings Resurgence in Form W-2 Tax Scam](#), by Matthew Murphy
- 3  [GDPR - 50 Days to the Great Data Protection Revolution](#), by Andrew Shindler and Thomas J. Smedinghoff
- 4  [Cybersecurity - The Victim Becomes the Law Breaker](#), by Andrew Shindler
- 5  [Standing — On Its Head — in Privacy Cases After CareFirst](#), by Molly McGinnis Stine
- 5  [Cybersecurity Disclosures: Takeaways from the SEC's New Guidance](#), by Michael J. Blankenship, Michelle Earley, Eric Johnson and Stanley Keller
- 7  [NYDFS Cybersecurity Update: Two Transition Dates Remaining](#), by Theodore P. Augustinos
- 8  [Biometrics: California Federal Court Denies Spokeo Motion to Dismiss Facebook Biometric Information Privacy Act Case](#), by P. Russell Perdew and Michael McGivney
- 9  [CGL and Aviation Insurers: Filling Gaps or Staking Space in the Race for Drones](#), by T. Patrick Byrnes and Matthew J. Kalas
- 9  [A Closer Look at the NAIC Insurance Data Security Model Law](#), by Theodore P. Augustinos

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](mailto:ted.augustinos@lockelord.com)



**Michael McGivney**  
Associate  
*Chicago*  
312-443-0208  
[michael.mcgivney@lockelord.com](mailto:michael.mcgivney@lockelord.com)



**Michael Blankenship**  
Partner  
*Houston*  
713-226-1191  
[michael.blankenship@lockelord.com](mailto:michael.blankenship@lockelord.com)



**Matthew Murphy**  
Associate  
*Providence*  
401-276-6497  
[matthew.murphy@lockelord.com](mailto:matthew.murphy@lockelord.com)



**T. Patrick Byrnes**  
Partner  
*Chicago*  
312-443-0286  
[pbyrnes@lockelord.com](mailto:pbyrnes@lockelord.com)



**P. Russell Perdew**  
Partner  
*Chicago*  
312-443-1712  
[rperdew@lockelord.com](mailto:rperdew@lockelord.com)



**Michelle Earley**  
Partner  
*Austin*  
512-305-4818  
[mearley@lockelord.com](mailto:mearley@lockelord.com)



**Andrew Shindler**  
Partner  
*London*  
+44 (0) 20 7861 9077  
[andrew.shindler@lockelord.com](mailto:andrew.shindler@lockelord.com)



**Eric Johnson**  
Partner  
*Houston*  
713-226-1249  
[ejohnson@lockelord.com](mailto:ejohnson@lockelord.com)



**Thomas J. Smedinghoff**  
Of Counsel  
*Chicago*  
312-201-2021  
[tom.smedinghoff@lockelord.com](mailto:tom.smedinghoff@lockelord.com)



**Matthew J. Kalas**  
Senior Counsel  
*Chicago*  
312-443-0458  
[mkalas@lockelord.com](mailto:mkalas@lockelord.com)



**Molly McGinnis Stine**  
Partner  
*Chicago*  
312-443-0327  
[mmstine@lockelord.com](mailto:mmstine@lockelord.com)



**Stanley Keller**  
Of Counsel  
*Boston*  
617-239-0217  
[stanley.keller@lockelord.com](mailto:stanley.keller@lockelord.com)

## Tax Season Brings Resurgence in Form W-2 Tax Scam

There are three certainties in life: death, taxes, and the knowledge that Ben Franklin's famous adage will be co-opted. A twenty-first century version of it may be that "in this world nothing can be said to be certain, except death and taxes ... and cybercrime."

As the tax season is fully underway, employers face an annual onslaught of scams designed to steal employee data. In recent years, cybercriminals have embarked on phishing expeditions in an attempt to trick company payroll personnel into forwarding information contained on W-2 forms. Cybercriminals use email spoofing to masquerade as C-suite executives or other persons of authority to request W-2 information from the personnel department. The IRS and state agencies have warned that cybercriminals may begin with an initial email that may appear to be personalized. If there is a response, the cybercriminals will respond with a request for all W-2 data for employees, including full Social Security numbers, salary, and withholding information. If the information is disclosed, the cybercriminals file false tax returns or sell the information.

Recently, cybercriminals, posing as company executives, have expanded the scam to ask payroll personnel to execute a wire transfer to an account. The IRS has also [warned](#) of new schemes to dupe taxpayers into believing they had received refunds in error and returning those funds to what turn out to be accounts set up by criminals.

The IRS cautions that these email phishing scams can be dangerous as they can result in the large-scale theft of sensitive data. The IRS reports that cybercriminals are not just going after large corporations – small businesses, schools, hospitals, tribal governments and charities have also been targeted.

In 2016, the IRS received 100 reports about the W-2 scam. By 2017, [that number had jumped to 900](#), resulting in the disclosure of information on hundreds of thousands of employees.

Education and vigilance are key. Employers should train personnel who handle employee information, including W-2s, to be wary of unsolicited emails that request personal information, even if an email appears to originate from a known source. Two-factor authentication provides a simple solution: any email requesting personal information should first be confirmed with a phone call to confirm that the email request is legitimate. Moreover, employers could also create an internal policy to restrict the distribution of W-2 information and require more than a simple email request as authorization for a wire transfer. The FBI has [recommended](#) these and other best practices.

Employers that have been a victim of a W-2 scam can [notify the IRS](#) at [dataloss@irs.gov](mailto:dataloss@irs.gov) with "W2 Data Loss" in the subject line and file a complaint with the FBI's Internet Crime Complaint Center. Of course, a breach of personal information may also implicate state breach notification requirements.

## GDPR – 50 Days to the Great Data Protection Revolution

In just a few weeks, on May 25, 2018, the EU's new data protection law goes live. The General Data Protection Regulation, commonly known as the GDPR, is the biggest change to European data protection law in over 20 years and will seriously impact businesses across the U.S. and around the world.

Time is running out for proactive compliance activity.

In this article, we briefly highlight some of the most far-reaching changes and burdensome requirements.

### 1. Worldwide Application

The first thing for non-EU businesses to consider is whether they are subject to the GDPR; this new law may apply even if you don't have a legal or physical presence in the EU.

Now you will have to comply if you offer goods or services to individuals in the EU or monitor their behavior on the Internet. A recent international report found that more than 70% of non-EU respondents said the GDPR would apply to their organizations.

Over recent months, Locke Lord has advised numerous U.S. and internationally-headquartered clients on whether the GDPR applies to their businesses.

### 2. Fines and Other Sanctions

The maximum fine for breaching the GDPR is up to 40 times larger than under the previous law and even more for big business – EU data authorities have been given the power to levy fines up to €20 million or 4% of the annual worldwide gross revenue of the whole group, whichever is greater.

That said, fines must be proportionate and are discretionary and applied on a case-by-case basis.

However, fines are only part of the story. In cases of breach, adversely affected individuals can claim compensation and the company may suffer negative publicity which can have a severe financial impact and, in extreme cases, can destroy a business.

### 3. Enhanced Rights of Data Subjects

Individuals have a right to obtain copies of all their personal data you are processing, generally within 30 days. They also have the right to have it ported to another provider or to object to its processing on certain grounds. They may also be able to require its erasure – the "right to be forgotten."

### 4. Reporting Data Breaches

There is a legal obligation to report a personal data breach to the authorities without undue delay – generally within 72 hours. This includes instances of hacking or where you have lost personal data you were holding, wherever there is a risk to individuals.

In serious cases, all individuals potentially affected by the data breach must also be notified, unless the data accessed is properly protected, e.g., by encryption.

### 5. Information Notices

You must provide individuals with extensive information about how you will process their data – in a transparent, intelligible and easily accessible way, using clear language.

## 6. Higher Standard for Consent

The GDPR has raised the bar if you rely on “consent” for processing personal data. Separate consents are now required for different processing activities. Pre-ticked boxes and blanket consents are not valid and individuals must be able to easily withdraw consent at any time.

For children under 13, and potentially up to 15, consent from a parent is required.

## 7. Processors Now Liable

Under the previous law, where a business processed personal data strictly on someone else’s instructions, it was a data “processor” rather than a data “controller” and not directly subject to EU data protection law. This is no longer the case. Data processors have many of the same obligations as data controllers and both are jointly liable for breaches in which they are involved.

## 8. Data Protection Officers – “DPOs”

Public authorities and organizations whose core activities require regular and systematic monitoring of data subjects on a large scale, or which process special categories of data on a large scale, must appoint a DPO. Other organizations which process significant personal data are recommended to make such an appointment.

The DPO must carry out a variety of data protection advisory, monitoring and other functions. DPOs must be suitably skilled and experienced, properly resourced and report to the highest levels of management without receiving any instructions and without conflict of interest.

A recent international study found that in Europe alone, 28,000 DPOs will need to be appointed by May 25, 2018.

## 9. Privacy Impact Assessments

If you are engaged in “high” risk processing – processing that presents a risk of infringing a person’s rights and freedoms, such as large scale processing of sensitive data or monitoring and profiling individual activities – you must carry out a Privacy Impact Assessment or “PIA.” This is a thorough exercise and organizations are likely to require guidance on how to undertake it.

## 10. Cybersecurity

Organizations must have appropriate security measures in place to protect personal data. In particular, this requires technical cybersecurity, such as ISO 27001 certification, but also includes organizational policies and staff training. More detail on this requirement can be found in our article, [“Cybersecurity – The Victim Becomes the Law Breaker.”](#)

# Cybersecurity – The Victim Becomes the Law Breaker

Every organization, however large or small, faces the threat of cyber-attack. Cybercrime is prevalent, and cybercriminals are becoming more and more sophisticated and operating for a variety of reasons, financial and political.

One might expect the law to have some sympathy with businesses that are victims of such crimes. After all, the victim will have suffered substantial inconvenience and may well have faced direct financial loss, including the payment of ransomware demands to cybercriminals and compensation to customers, as well as reputational damage and loss of goodwill. These

factors alone make it imperative for businesses to have first class cybersecurity measures in place.

But there is another reason to be cyber-prepared – the law has no such sympathy, at least not under the new European Data Protection law, the GDPR. The GDPR applies to all organizations established in the European Union, but also has potential application to many based outside. (See [“50 Days to the Great Data Protection Revolution”](#)). It comes into force on May 25, 2018.

Cybersecurity is a fundamental requirement of the GDPR. The GDPR demands that all organizations which come within its ambit must implement “appropriate technical and organisational measures” to ensure a level of security appropriate to the risks arising from holding and processing personal data. These are, in particular, the risks of accidental or unlawful destruction, loss, alteration and unauthorized disclosure or access.

The GDPR spells out in general terms some of the cybersecurity measures that are expected and what they must achieve, namely:

1. Pseudonymisation and encryption;
2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

However, the GDPR gives no more detail as to the precise cybersecurity measures to be taken to achieve the required standard of “appropriate,” other than to say that the state of the art, the costs of implementation and the nature of processing should be taken into account. To that extent, some may find this law disappointingly vague.

It is therefore left to organizations to determine for themselves what level of security is appropriate – taking expert advice if required. The starting point, though, must be the state of the art. This will change as technology marches forward, but current technical measures must, as a minimum, include:

- anti-virus, malware and spyware software
- firewalls
- encryption of data in transit and all portable devices
- intrusion detection and prevention systems
- regular software updates
- data backup
- user access control management
- unique complex passwords with expiry on all devices on a not-too-frequent basis.

Certification to the ISO/IEC 27001:2013 standard will go a long way to showing that appropriate measures have been taken and demonstrates adoption of information security best practice.

The GDPR not only requires high standards of data security. It also brings many more non-EU businesses within its ambit, and makes two other directly relevant and fundamental changes to data protection law.

First, it requires that organizations that suffer a breach of data security in almost every case to report that breach to their data protection authority without “undue delay” and, where feasible, within 72 hours of becoming aware. All relevant details must be provided. In many cases, organizations must also report to the individuals whose data has been compromised.

Second, the penalties for not having the appropriate security in place, or, indeed, for not complying with the above reporting obligations are now much stiffer. Whereas the maximum fine was previously on the order of hundreds of thousands of pounds or euros, the maximum for a breach of the provisions which specifically relate to data security is now the higher of €10 million and 2% of the annual worldwide gross revenue of the entity concerned.

To conclude: while all organizations should be keeping their cybersecurity arrangements under constant review, those which fall within the GDPR are strongly recommended to carry out a major review immediately. In doing so, they must focus not only on their technology and everyday practices, they must also create and document procedures for complying with applicable law and reporting data breaches to their data protection authority and affected individuals.

## Standing – On Its Head - in Privacy Cases After CareFirst

The U.S. Supreme Court recently declined to review *CareFirst Inc. v. Attias*, a data breach standing case. For those hoping for resolution of a notable circuit split over what constitutes Article III standing at the pleading stage, the wait continues.

In *CareFirst Inc. v. Attias*, the Supreme Court's rejection leaves intact a decision by the District of Columbia Circuit Court of Appeals. Plaintiffs asserted that a data breach suffered by their health insurer exposed their personal information and created risk of harm to them. The federal district court dismissed the putative class action, holding that the plaintiffs' allegations were "too speculative to establish injury in fact." In August 2017, the D.C. Circuit [reversed](#), chiding the lower court for "an unduly narrow reading" of the law and holding that plaintiffs had "cleared the low bar to establish their standing at the pleading stage." According to the appellate decision, "all [of the] plaintiffs ... have standing to sue CareFirst based on their heightened risk of future identity theft ...." The opinion also stated that the court had "little difficulty concluding that their injury in fact is fairly traceable to CareFirst."

The *CareFirst* appellate decision – recognizing Article III standing from a substantial risk of future injury – joins similar outcomes from several other circuits. One such very recent decision came from the Ninth Circuit Court of Appeals in *In re: Zappos.com, Inc., Customer Data Security Data Security Breach Litigation*. The court [reversed](#) the lower court's dismissal of plaintiffs' action, and stated that plaintiffs had "sufficiently alleged standing based on the risk of identity theft."

The competing position from other circuits is illustrated by the Eighth Circuit Court of Appeals. In *In re: SuperValu, Inc., Customer Data Security Breach Litigation*, various plaintiffs sued several supermarket defendants following the theft of credit and debit card information from defendants' systems. In August 2017, the Eighth Circuit [affirmed](#) the lower court's dismissal of a class action for all but one specific plaintiff. The court held that the plaintiffs' complaint did not "adequately allege[] that plaintiffs face a 'certainly impending' or 'substantial risk' of identity theft as a result of the data breaches purportedly caused by defendants' deficient security practices." As noted by the court, "a mere possibility [of injury] is not enough for standing." On March 7, 2018, the lower court on remand [dismissed](#) the action as to the lone plaintiff remaining after the appellate decision.

Absent guidance from the U.S. Supreme Court, divergent decisions are likely to continue to emerge from the various circuits. It remains to be seen whether plaintiffs will engage in forum shopping to seek out the jurisdictions that are more likely to hold that the risk of future harm satisfies standing requirements. Uncertainty may also arise where circuits that have tended to one position or the other on the future harm issue may rule differently based on the facts of a particular case. The decisions will continue to be influenced by the specific details of a breach, the information affected, and the allegations about harm and risk of harm. Further, it bears watching whether there is a case that will one day pique the U.S. Supreme Court's interest. Finally, it is worth remembering that this debate over standing is just one step of the litigation journey. Even if or when cases survive standing challenges, there will still be disputes over motions to dismiss and motions for summary judgment and battles over proof at trial.

## Cybersecurity Disclosures: Takeaways from the SEC's New Guidance

On February 21, 2018, the Securities and Exchange Commission (the SEC) issued interpretative guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.<sup>1</sup> The guidance refreshes previous staff guidance,<sup>2</sup> adds emphasis by being a statement of the Commission and addresses new topics. The SEC guidance details how public companies should disclose cybersecurity events that represent a material risk to their investors. The SEC also emphasizes the importance of timely disclosing to senior management cybersecurity risks and incidents. In addition, the SEC suggests ways a company can prevent insider trading, such as by creating a blackout in trading following a cybersecurity event. Finally, the SEC cautions companies to avoid selective disclosure. We summarize below the new guidance, the SEC's previous staff guidance and our takeaways.

### The New

The new guidance addresses two new issues that the SEC did not address in the previous staff guidance. First, the SEC stresses that cybersecurity risk management policies are key elements of a company's general disclosure controls and procedures.<sup>3</sup> For companies that have not already done so, the SEC strongly encourages them to adopt and maintain comprehensive disclosure controls and procedures that relate to cybersecurity risks. This includes having policies and procedures in place to ensure that timely notifications of cybersecurity incidents are reported up to senior management.

### Disclosure and Control Procedures

The focus on cybersecurity disclosure and control policies is important in the context of the required certification by a company's CEO and CFO (or principal financial officer) regarding the design and effectiveness of a company's disclosure controls and procedures. These certifications should now take into

- 1 SEC Rel. Nos. 33-10459; 34-82746, located [here](#).
- 2 CF Disclosure Guidance Topic No. 2, Cybersecurity located [here](#).
- 3 Public companies are required to maintain effective disclosure controls and procedures pursuant to Exchange Act Rules 13a-15 and 15d-15.

account the adequacy of the company's cybersecurity disclosure controls and procedures.

### Insider Trading Policies

The SEC cautions that a company's undisclosed cybersecurity incident may involve material, nonpublic information that could cause a company's officers, directors and other insiders to violate the antifraud provisions of the Exchange Act if they trade in the company's securities while the cybersecurity incident remains nonpublic information. The SEC encourages companies to consider establishing certain policies, such as restrictions on insider trading following a cybersecurity incident, to avoid the appearance of improper insider trading. This is an especially important caution in view of the recent Equifax hack and the probe surrounding executives' stock sales after the hacking incident. The SEC also reminds companies of the requirements of Regulation FD to avoid selective disclosures of material cybersecurity matters.

### The Old

In October 2011, the SEC's Division of Corporation Finance issued interpretive guidance to assist public companies in assessing their disclosure obligations concerning cybersecurity risks and incidents in registration statements and periodic reports. Given the increased risks that cybersecurity poses to companies in nearly every industry now, the SEC has provided an update

on its previous guidance. The following chart highlights when existing disclosure requirements may impose an obligation on a company to make certain cybersecurity disclosures.

### Takeaways

Given the increased magnitude and frequency of cybersecurity incidents, public companies should revisit their cybersecurity disclosures and disclosure controls and procedures. Despite the criticism by some that the SEC's new guidance does not go far enough,<sup>4</sup> that guidance should serve as a wake-up call for companies that have not yet put in place a comprehensive cybersecurity disclosure policy. A public company without such a policy is urged to put one in place so that it is in a position to timely report and to alert investors of any data breaches or other cybersecurity incidents.

Those public companies that have a cybersecurity disclosure policy in place should review and update that policy, having in mind that cybersecurity incidents are becoming more and more common and that increased attention by the SEC and others on cybersecurity disclosure is assured. In addition to disclosure and governance considerations, companies should continue to treat the subject of cybersecurity as a critical operational issue deserving of focused attention.

4 <https://www.law360.com/articles/1014661/new-sec-cybersecurity-guidance-dinged-by-dems-as-rehash>

REGULATORY ITEM	SEC GUIDANCE
Item 503(c) – Risk Factors	<p>Companies should consider the following to determine whether disclosure of cybersecurity risks is necessary:</p> <ul style="list-style-type: none"> <li>• prior cybersecurity incidents, including their severity and frequency</li> <li>• probability of an incident and potential magnitude of the incident</li> <li>• whether the company's business or industry gives rise to material cybersecurity risks</li> <li>• costs associated with cybersecurity protection</li> </ul> <p>If a company has experienced a specific cybersecurity incident, it may not be enough to disclose the potential risk of another incident occurring. The company should discuss in further detail the occurrence and its consequences, alongside a broader discussion of cybersecurity risks inherent in the company's business or industry.</p>
Item 303 – MD&A of Financial Condition and Results of Operation	<p>In disclosing information the company's management believes necessary to understanding its financial condition and results of operations, management may want to consider whether the costs of cybersecurity (such as loss of IP, reputational harm, and cybersecurity insurance) and the potential risks and consequences of an incident could further inform management's discussion and analysis. In addition, the SEC expects companies to consider cybersecurity issues and their impact on each of the company's reportable segments.</p>
Item 101 – Description of Business	<p>The SEC expects companies to discuss cybersecurity incidents or risks if it would materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions.</p>
Item 103 – Legal Proceedings	<p>Any litigation arising out of a cybersecurity incident must be properly disclosed. For example, if a company is hacked and all of its customers' information is stolen, the company must disclose any material litigation, including suits brought by the affected customers against the company.</p>
Financial Statement Disclosures	<p>A company's financial reporting and controls system should be designed so that information relating to the financial impact of a cybersecurity incident is reflected on the financial statements in a timely manner. For example, an operational event such as a hack could result in a possible loss contingency requiring financial statement accrual or disclosure.</p>
Item 407(h) – Board Risk Oversight	<p>If cybersecurity risks are material to the company's business, the discussion on the Board's risk oversight should include a discussion on the Board's role in overseeing cybersecurity risks.</p>

## NYDFS Cybersecurity Update: Two Transition Dates Remaining

Several of the new requirements of the New York State Department of Financial Services (DFS) Cybersecurity Regulation are now operative for firms and individuals engaged in financial services (including insurance companies and producers, banks and others) licensed by the DFS (Covered Entities). Covered Entities should now be working on the regulation's remaining and ongoing requirements. The next transition date, September 3, 2018, requires the compliance with five of the regulation's requirements and the final transition date is March 1, 2019. While Covered Entities are focused on meeting these deadlines, the regulation also contains several ongoing requirements that demand continued attention.

### Satisfying the September 3, 2018 Transition Date

In addition to the requirements that were phased in by the first two transition dates of August 28, 2017 and March 1, 2018, by September 3, 2018, Covered Entities must have policies and procedures in place for the *secure disposal* of certain Nonpublic Information no longer necessary to be retained for business operations or other business purposes. In addition, Covered Entities that are not subject to one of the limited exemptions described in our previous [article](#) must satisfy the following requirements:

- *Audit Trail* requirements, based on the Risk Assessment, including the maintenance of systems designed to reconstruct material financial transactions, and to detect and respond to certain Cybersecurity Events. Records related to material financial transactions and certain Cybersecurity Events must be maintained for five years and three years, respectively.
- *Application Security* requirements for written procedures, guidelines and standards for secure development, evaluation, assessment and testing of applications.
- *Training and Monitoring*, based on the Risk Assessment, procedures and controls for monitoring activities of authorized users, and detecting unauthorized access, use or tampering; and regular cybersecurity awareness training for all personnel.
- *Encryption* of nonpublic information, based on the Risk Assessment, controls, including encryption to protect nonpublic information, both in transit and at rest, unless infeasible, in which case, effective alternative compensating controls approved and annually reviewed by the CISO.

These requirements, together with the provisions that had earlier transition dates, must be satisfied in order to put the Covered Entity in a position to file the next required compliance certificate, due February 15, 2019.

### The Final Transition Date

The last remaining transition date of March 1, 2019 will require compliance with the regulation's third party service provider requirements. These requirements will, for many Covered Entities, require a great deal of work and attention, as they affect the relationship between each Covered Entity and any third party that touches its Nonpublic Information or its Information Systems. It is important to note that these terms are defined in the regulation much more broadly than most Covered Entities

have been thinking about them, and will involve more third party service providers than have typically been considered in vendor management programs.

### Ongoing Requirements

In addition to meeting the provisions of the regulation with upcoming transition dates, Covered Entities must continue to observe the regulation's periodic and ongoing requirements, including those identified below. Note that many of these ongoing requirements do not apply to partially exempt Covered Entities, as indicated by asterisk.

- Access privileges to Information Systems must be periodically reviewed.
- Risk Assessments of Information Systems must be conducted periodically.
- Cybersecurity Events must be evaluated on an ongoing basis to comply with applicable notification requirements.
- Annual compliance certifications are required to be submitted to the Superintendent by February 15.
- Exemptions must be monitored, as exemption notifications must be updated if new exemptions apply, and the regulation requires full compliance within 180 days of the end of a fiscal year end if the Covered Entity ceases to qualify.
- Third Party Service Providers with access to Information Systems and Nonpublic Information must be vetted and contracted, and periodically assessed, in accordance with policies and procedures for addressing cybersecurity risks.
- Limitations on Data Retention must be continually applied to securely eliminate certain Nonpublic Information that is no longer necessary for business purposes, unless otherwise required to be maintained for certain purposes.
- Cybersecurity personnel are required to receive updates on relevant cybersecurity risks, and must maintain current knowledge of changing cybersecurity threats and countermeasures.\*
- Application Security safeguards are to be periodically reviewed, assessed and updated.\*
- CISO's ongoing responsibility for overseeing and implementing the cybersecurity program and enforcing the cybersecurity policy.\*
- CISO's annual requirement to report to the board of directors on the cybersecurity program and cybersecurity risks.\*
- Monitoring and testing on an ongoing basis to assess the effectiveness of the Cybersecurity Program, using either continuous monitoring, or periodic penetration testing and vulnerability assessments.\*
- Audit trail requirements for the ongoing maintenance of systems to be able to reconstruct certain material financial transactions, and to detect and respond to certain Cybersecurity Events, including the maintenance of certain financial records for at least five years, and information related to certain Cybersecurity Events for at least three years.\*
- Monitoring of the activities of Authorized Users must be conducted on an ongoing basis, including detection of unauthorized access to or misuse of Nonpublic Information.\*
- Cybersecurity Awareness Training is required to be provided for all personnel, and updated regularly.\*

- Encryption technology, or compensating controls to protect data in motion and data at rest may require ongoing attention, including training and monitoring, depending on the particular safeguards deployed.\*

Generally, it is important for Covered Entities to build in periodic review, reassessment, and refreshing of their Cybersecurity Program and Cybersecurity Policies to keep up with regulatory developments; evolution in the threat landscape; developments in business needs, operation and personnel; progress in security techniques and technologies; and results of the periodic Risk Assessment.

## Biometrics: California Federal Court Denies Spokeo Motion to Dismiss Facebook Biometric Information Privacy Act Case

On February 26, 2018, a California federal court denied Facebook's motion to dismiss claims under Illinois's Biometric Information Privacy Act (BIPA), finding the plaintiff had Article III standing despite the absence of tangible injury. *Patel v. Facebook, Inc.*, 2018 WL 1050154 (N.D. Cal. Feb. 26, 2018). The court distinguished the claim from other BIPA cases finding no Article III standing under the Supreme Court's 2016 decision in *Spokeo v. Robins*, 136 S. Ct. 1540 (2016). The *Patel* decision is a reminder that, despite recent defense victories in BIPA cases, defendants continue to face substantial potential liability even where plaintiffs incurred no discernible injury from alleged technical violations of BIPA's requirements.

### Wave of class actions filed against companies under BIPA

BIPA prohibits private entities from obtaining or using 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 BIPA 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.

The availability of liquidated damages has prompted dozens of recent class-action filings alleging BIPA violations, mostly in Illinois state court. These cases have mostly been filed against employers who allegedly collected and used employee fingerprints for time clocks. Significantly, plaintiffs in these cases typically do not allege any tangible injury (e.g., identity theft); plaintiffs simply allege the violation of BIPA's notice-and-consent requirements and seek to collect the \$1,000 to \$5,000 liquidated damages for themselves and all other putative class members.

### Several courts dismissed BIPA claims for lack of tangible injury

Three significant decisions have dismissed BIPA claims where the plaintiff did not allege any injury beyond an alleged violation of BIPA's notice-and-consent requirements. In *Vigil v. Take-Two Interactive*, the U.S. Court of Appeals for the Second Circuit affirmed the dismissal of a BIPA claim because the plaintiff's failure to allege a concrete injury deprived the plaintiff of Article III standing under *Spokeo*. No. 17-303, 2017 WL 5592589 (2nd Cir. Nov. 21, 2017). Plaintiffs in *Take-Two* played a video game made by defendant; the game scanned plaintiffs' faces to create in-game avatars. While plaintiffs knew their faces were being scanned and used, they claimed they didn't receive the notice or provide the written consent required by BIPA. Because plaintiffs knew their biometric information was being taken and

used, the Second Circuit affirmed the dismissal because there was "no material risk that Take-Two's procedural violations have resulted in plaintiffs' biometric data being used or disclosed without their consent." *Id.* at \*2.

In *Rosenbach v. Six Flags Entertainment Corp.*, the Illinois Appellate court held that a BIPA plaintiff cannot state a claim under the statute without a resulting injury beyond a statutory violation. 2017 IL App (2d) 170317. There, defendant collected plaintiff's fingerprints when plaintiff bought a season pass to the defendant's theme park and allegedly failed to provide the notice and obtain the written consent required by BIPA. *Id.* at ¶¶ 7-10. Because plaintiffs did not allege any injury beyond the alleged violations, the appellate court held that plaintiffs were not "aggrieved" by the violation, as required by the statute, and thus had no statutory standing to sue. *Id.* at ¶ 23 ("A determination that a technical violation of the statute is actionable would render the word 'aggrieved' superfluous.").

Finally, a federal district court dismissed a BIPA claim based on lack of Article III and statutory standing in *McCullough v. Smarte Carte, Inc.*, 2016 WL 4077108, at \*1 (N.D. Ill. Aug. 1, 2016). There, the defendant was a locker-rental company that collected plaintiff's fingerprints to use in lieu of a key to get into the locker. The court found the absence of any consequential injury beyond the alleged lack of notice and consent deprived plaintiff of both constitutional standing under Article III and *Spokeo* and statutory standing under BIPA.

In *Patel*, the court found the alleged collection and use of biometric information without plaintiff's knowledge was a sufficient injury to satisfy *Spokeo*.

Plaintiffs in *Patel* sued based on Facebook scanning uploaded photos and creating a digital representation and "template" of each face in the photos, including faces of non-Facebook users. Facebook does this to allow users to "tag" (i.e., identify) people in uploaded photos, which Facebook can then use to identify those people in other photos based on the biometric information Facebook extracts from the photos. Plaintiffs claimed Facebook violated BIPA's notice-and-consent requirements.

The court in *Patel* denied defendant's motion to dismiss under *Spokeo* and found plaintiff had alleged a sufficient injury. 2018 WL 1050154, *Id.* at \*1. The court found that Illinois's passage of BIPA gave plaintiff a right to protect their biometric information and that the violation of that right was a sufficiently concrete harm to satisfy *Spokeo*. *Id.* at \*4 ("The abrogation of the procedural rights mandated by BIPA necessarily amounts to a concrete injury"). The court distinguished *Take-Two* and *McCullough* because plaintiffs there "indisputably knew that their biometric data would be collected before they accepted the services ...." *Id.* at \*5. By contrast, plaintiff in *Patel* alleged "Facebook afforded plaintiffs no notice and no opportunity to say no" to the data collection. *Id.*

*Patel* can be distinguished but should cause defendants to be wary of BIPA litigation.

Many defendants in the current wave of BIPA class actions have moved to dismiss based on a lack of actual injury, and plaintiffs in those cases will undoubtedly cite *Patel* in response. But *Patel's* facts were unique: plaintiffs there allegedly did not know their biometric information was being taken from uploaded photos and used to identify them. By contrast, most plaintiffs in pending BIPA cases knew their biometric information (typically fingerprints) was taken and used, and thus should not be able to use *Patel* to fight dismissal. But defendants will need to carefully distinguish *Patel* to defeat no-injury BIPA cases.



## CGL and Aviation Insurers: Filling Gaps or Staking Space in the Race for Drones

Insurers searching for new sources of premium have increasingly looked to drones. But one question has dominated the conversation: who will benefit: the aviation market or traditional general liability insurers? Recent reports suggest the answer to that question may be “both.”

During a recent webinar hosted by *Insurance Journal*, a panel of experts estimated that coverage for drones will grow exponentially, potentially causing the largest growth in aviation insurance in 50 years. This would be a welcome development for aviation insurers, who have experienced a sustained period of soft markets and shrinking premiums. Meanwhile, in January of this year, the International Underwriting Association (IUA) issued a report titled “Unmanned Aerial Vehicles (UAVs) – Opportunities and Challenges for General Liability Insurers” and concluded that traditional aviation policies will not address all elements of this emerging risk. The IUA opined that general liability underwriters will have a key role to play in providing cover for drone risks, particularly with respect to areas that generally fall outside the traditional aviation realm, such as privacy, cybersecurity and nuisance / trespass. Nonetheless, traditional aviation insurers would appear to have the corresponding opportunity to innovate with their own products.

While the outlook for insurers is positive, recent events serve as a reminder that participating in this emerging area is not without risk. To date the vast majority of the claims experienced, at least in the aviation market, involve hull claims, either as a result of fly-aways, operator error, or otherwise. But that may soon be changing. In February of this year alone, there were two separate reports of incidents involving helicopters and drones. In one incident, it was alleged that an air-tour helicopter in Hawaii clipped a drone while flying over Kauai. In the second, a student pilot and instructor in South Carolina suffered a crash landing when a small drone allegedly appeared directly in front of them. According to published reports, the tail of the helicopter struck a tree while the student pilot and instructor were taking evasive action to avoid the drone, causing significant damage to the helicopter. Thankfully, there were no injuries. And, on February 1, 2018, the *sUASNews* website posted alarming video footage appearing to be from a drone that flew within a few feet of an airliner over Las Vegas.

These incidents warn of the significant risks that drones can pose to traditional commercial aviation. Putting to the side for the moment these headline-grabbing incidents, the potential also remains for substantial property damage and business interruption claims from commercial drone uses, particularly in the event of a mishap while conducting inspections of sensitive equipment and infrastructure. Finally, the specter of privacy and nuisance / trespass claims persists, which may be the most difficult risks for insurers to address in these early days of drone cover. Thus, it is clear that both general liability and aviation insurers writing drone risks can expect to be involved in claims that will involve new and challenging issues.

In sum, while it appears there will be plenty of market share for both aviation insurers and general liability insurers looking to write drone coverage, there is also plenty of risk as well. As larger and more complex claims come forward, which they almost certainly will, there will undoubtedly be a learning curve for

all involved as insurers continue to examine and consider their approach to writing risks associated with this new technology. While insurers work through that learning curve, it will be critical to apply best practices to handling drone claims as well as to seek out and rely on service providers with expertise in this emerging area.

## A Closer Look at the NAIC Insurance Data Security Model Law

Following New York’s lead after the Department of Financial Services (the NYDFS) promulgated its Cybersecurity Regulation,<sup>1</sup> in October 2017 the NAIC adopted its Insurance Data Security Model Law (the NAIC Model)<sup>2</sup> to establish 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 will prompt state legislatures to enact cybersecurity requirements that will affect the entire insurance industry, including InsurTech firms and other service providers with access to the data and systems of insureds and producers. Legislation based on the NAIC Model has already been introduced in Rhode Island<sup>3</sup> and South Carolina,<sup>4</sup> and other states are expected to follow in the coming months.

Concerns about the potential for inconsistent, or conflicting, cybersecurity requirements have been expressed by various insurance industry participants and commentators. The NAIC Model, while based on the NYDFS Cybersecurity Regulation, differs from it in several important respects, as highlighted in our previous article available [here](#). To address these concerns, a drafters’ note to the NAIC Model states that Licensees in compliance with the NYDFS Cybersecurity Regulation are deemed to be compliance with the NAIC Model. It remains to be seen whether and to what extent states may incorporate this language; the pending Rhode Island and South Carolina bills referenced above do not. Although the Rhode Island and South Carolina bills follow the NAIC virtually *verbatim*, other states may introduce their own variations, which could complicate compliance efforts for the insurance industry.

Nevertheless, given the importance and reach of the NAIC Model, and the likelihood that states will act soon to adopt it in some version, a close review of its requirements is warranted.

### Applicability of the NAIC Model

#### Licensees

The NAIC Model applies to “Licensees,” which are defined to include any individual or entity (other than nongovernment agencies) operating, or required to operate, under a license, registration, or other authorization under the insurance laws of a state. Purchasing groups and risk retention groups chartered and licensed in another state as well as assuming insurers that

1 23 NYCRR 500.

2 NAIC Model Law 668.

3 S. 2497 and H. 7789 (RI 2018).

4 H. 4655 (S.C. 2018).

are domiciled in another jurisdiction are not included in the definition of Licensee for purposes of the NAIC Model.

Given the requirements concerning the security of Third Party Service Providers, defined as described below, many providers of services to Licensees should also review the provisions of the NAIC Model Law.

The NAIC Model Law imposes various obligations to protect the security of “Nonpublic Information” and “Information Systems.”

### *Exemptions*

Licensees with fewer than 10 employees, including independent contractors, are exempt from the NAIC Model. This exemption from all of the requirements of the NAIC Model is in contrast to the limited exemptions for small businesses under the NYDFS Cybersecurity Regulation, in which several of the Regulation’s requirements apply to otherwise exempt small businesses. In addition, HIPAA-covered entities that maintain an Information Security Program under HIPAA are deemed to be in compliance with the NAIC Model requirement for an Information Security Program, provided that a written statement of compliance is submitted. In addition, employees, aides, representatives, and designees of a Licensee are not required to develop their own Information Security Programs to the extent they are covered by the Information Security Program of another Licensee.

### *Nonpublic Information*

“Nonpublic Information” is defined to include nonpublic information that is commonly defined as personal information for purposes of breach notification statutes: Social Security number, driver’s license or other non-driver identification number; account number, credit or debit card number; security code access code or password that would permit access to a consumer’s financial account; or biometric records. In addition, the definition includes certain health and medical information, and business-related information if the tampering, unauthorized disclosure, access or use of the business information will cause a material adverse impact to the business, operations or security of the Licensee. Therefore, similar to the approach taken by the NYDFS, these new cybersecurity requirements go beyond requiring the protection of information that is important to consumers, and extends to information that is important to the Licensee’s business, and by extension the industry.

### *Information Systems*

Also similar to the NYDFS cybersecurity regulation, the NAIC Model Law requires protection of “Information Systems,” defined to include industrial/process control systems, telephone switching and private branch exchange systems, and environmental control systems, in addition to systems used for processing data.

## **Requirements of Licensees**

### *Information Security Program*

The backbone of the NAIC Model Law is the requirement for a written Information Security Program, based on the Licensee’s risk assessment. This is consistent with prior data protection regimes, including the NYDFS Cybersecurity Regulation and the Massachusetts Data Security Regulation.<sup>5</sup> The Information Security Program must include administrative, technical, and physical safeguards for the protection of nonpublic information and Information Systems.

### *Risk Assessment*

Licensees must designate one or more employees, an affiliate, or an outside vendor to be responsible for the Information Security Program. Unlike the NYDFS, the NAIC Model does not specify particular qualifications for this designee. The risk assessment required of each Licensee must identify reasonably foreseeable threats to Nonpublic Information and Information Systems, including those that are accessible to, or held by, Third Party Service Providers. It must also assess (i) the likelihood and potential damage of these threats; and (ii) the sufficiency of policies, procedures, Information Systems and other safeguards. The effectiveness of the Licensee’s safeguards must be assessed no less than annually.

### *Risk Management*

Based on the Risk Assessment, the Licensee must design its Information Security Program to mitigate identified risks, commensurate with the size and complexity of the Licensee’s activities, and the sensitivity of the Nonpublic Information. Third Party Service Providers are required to be included in the Risk Management Program. The NAIC Model lists 11 security measures to be implemented, as the Licensee deems appropriate. These include access controls, systems and data inventory, physical security, encryption of data and transmission over external networks and on mobile devices, application security, multi-factor authentication, testing and monitoring of systems and procedures, maintenance of audit trails, disaster recovery, and secure disposal.

The Risk Management requirements include obligations for awareness training, and the inclusion of cybersecurity risks in the enterprise risk management process of the Licensee.

### *Board Oversight*

For Licensees with a Board of Directors, the Board or a Board committee must require the development, implementation and maintenance of an Information Security Program, and a written report, at least annually. The written report must cover the overall status of the Information Security Program and the Licensee’s compliance with the NAIC Model, and material matters related to the Information Security Program, including Cybersecurity Events, violations of the Information Security Program, and recommendations for changes.

### *Third Party Service Providers*

The NAIC Model requires Licensees to exercise due diligence in selecting Third Party Service Providers. Third Party Service Providers are defined as persons (other than government agencies) that are not Licensees that contract with a Licensee to maintain, process, store or otherwise access Nonpublic Information in providing services to the Licensee. Each Licensee must require its Third Party Service Providers to implement appropriate administrative, technical and physical measures to secure Information Systems and Nonpublic Information. As a result, many businesses that are not Licensees, but that provide a variety of services to Licensees, will be contractually held to new standards of cybersecurity driven by the NAIC Model.

### *Program Adjustments*

Licensees are required to keep their Information Security Programs up to date to reflect changes in technology, threats, business arrangements (specifically including mergers and acquisitions, and other business relationships), and Information Systems.

5 23 NYCRR 500; 201 CMR 1700

### *Incident Response Plan*

Each Licensee is required to establish a written incident response plan designed to promptly respond to and recover from any Cybersecurity Event (as defined below) that compromises the confidentiality, integrity, or availability of nonpublic information in its possession, Information Systems, or the continuing functionality of any aspect of the Licensee's business or operations. The NAIC Model requires eight specific elements to be addressed in the incident response plan.

### *Annual Certification*

Each year, by February 15, each domestic insurer is required to submit to the Commissioner a written certification of compliance with the NAIC Model. Note that, unlike the NYDFS Cybersecurity Regulation, this requirement applies only to insurers, and not to other Licensees.

### **Cybersecurity Events**

The NAIC Model includes certain, specific requirements in connection with a Cybersecurity Event, including specific requirements for investigations and a requirement to notify the Commissioner within 72 hours of determining that certain Cybersecurity Events have occurred. "Cybersecurity Event" is defined by the NAIC Model to mean an event resulting in unauthorized access to, disruption or misuse of an Information System or information stored on an Information System, other than (i) encrypted information (unless the security of the encryption is also jeopardized), or (ii) where the Licensee determines that the Nonpublic Information affected by the Cybersecurity Event has not been used or released, or has been returned or destroyed.

### *Investigations*

Licensees are required to investigate potential Cybersecurity Events promptly. At a minimum, the investigation by the Licensee or its outside vendor is required to determine the following facts to the extent possible:

- Whether a Cybersecurity Event has occurred;
- The nature and scope of the Cybersecurity Event;
- Nonpublic Information that may have been affected; and
- Reasonable measures to restore security of the compromised Information Systems.

### *Notice*

Once a Cybersecurity Event has been determined, the Licensee must provide notice (i) to the Commissioner of the department regulating insurance in the Licensee's state of domicile or home state; or (ii) to the Commissioner of another state if the Licensee reasonably believes that the Cybersecurity Event affects the nonpublic information of 250 or more consumers residing in the state and either (a) requires notice to a government agency, or (b) has a reasonable likelihood of materially harming any consumer in the state, or any material part of the normal operations of the Licensee.

The notice must provide as much information concerning the Cybersecurity Event as possible, and the Model law includes thirteen specific data points to be provided in the notification. While there is no independent obligation under the NAIC Model to notify consumers, the Licensee is required to comply with applicable state breach notification laws, and to provide the copy of such notices to the Commissioners of the implicated states. As for Cybersecurity Events involving Third Party Service Providers, the NAIC Model requires Licensees to treat such events as their own, provided that the obligation to investigate and provide notice can be delegated by agreement between the Licensee and the Third Party Service Provider.

The Model Law also specifically provides that the reinsurers must provide notice to insurers of Cybersecurity Events.

Similarly, insurers are required to notify producers of record of Cybersecurity Events.

### **Confidentiality**

The NAIC Model provides that information provided to the department pursuant to the NAIC Model is confidential and privileged, and not subject to Freedom of Information Act and other similar requests, to subpoena, or to discovery in a civil case.

---

Practical Wisdom, Trusted Advice.



[www.lockelord.com](http://www.lockelord.com)

Atlanta | Austin | Boston | Chicago | Cincinnati | Dallas | Hartford | Hong Kong | Houston | London | Los Angeles  
Miami | Morristown | New Orleans | New York | Providence | San Francisco | Stamford | Washington DC | West Palm Beach

---

Locke Lord LLP disclaims all liability whatsoever in relation to any materials or information provided. This brochure is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. If you wish to secure legal advice specific to your enterprise and circumstances in connection with any of the topics addressed, we encourage you to engage counsel of your choice. (041018)

Attorney Advertising © 2018 Locke Lord LLP