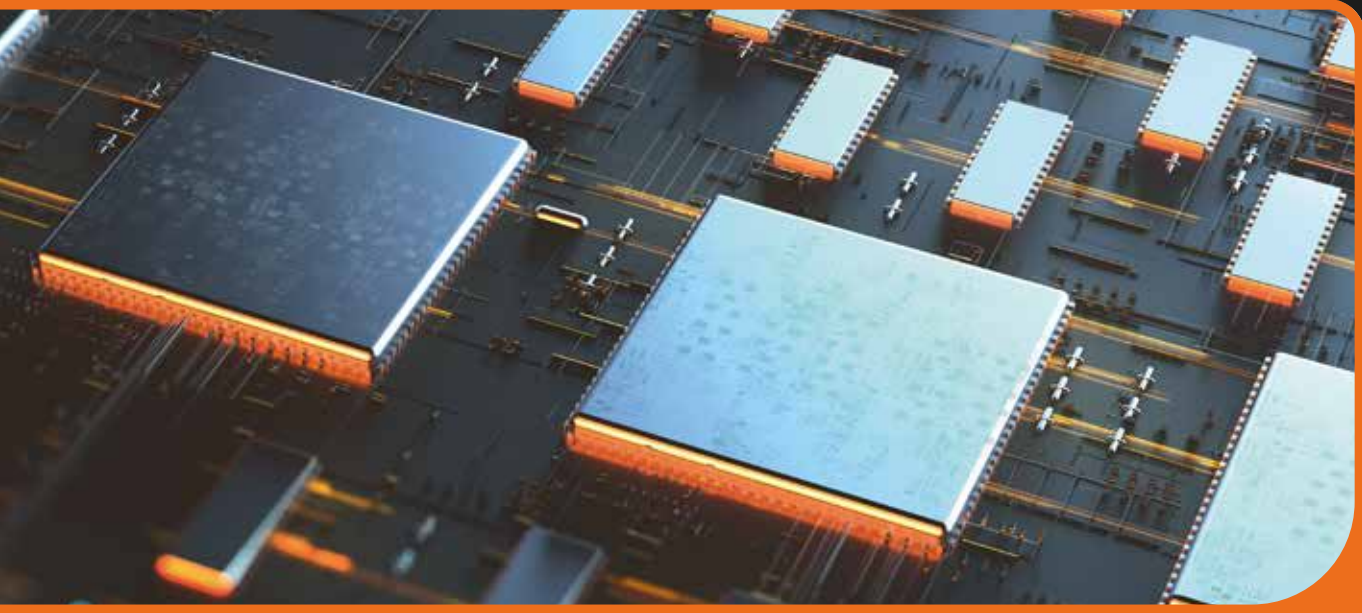
International
Comparative
Legal Guides



Practical cross-border insights into cybersecurity

Cybersecurity 2022

Fifth Edition

Contributing Editor:
Nigel Parker
Allen & Overy LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Phantom Responsibility: How Data Security and Privacy Lapses Can Lead to Personal Liability for Officers and Directors

Rothwell Figg

Christopher Ott

2021 has made it clear: boards of directors ignore data security and privacy risks to companies at the peril of their companies and – increasingly – their own personal liability. A business has its operations halted by ransomware approximately every 10 seconds. Just in this last year, a United States oil pipeline was shut down by these cybersecurity threats. The global costs of these breaches and online crime exceeds trillions of dollars every year. These potential costs have elevated data security and privacy issues from mere "IT issues" to the centrepiece of strategic risk management. As a result, boards face expanding personal legal liability for the company's data security and privacy failures.

The upward liability trend is not new. As early as 2014, the National Association of Corporate Directors (NACD) Director's Handbook on Cyber-Risk Oversight provided core cybersecurity principles to members of public companies, private companies, and non-profit organisations of all sizes and in every industry sector. The NACD directed board members to understand and approach cybersecurity as an enterprise-wide risk management issue and not just an issue for the IT team. As an established enterprise-wide risk, cybersecurity therefore began triggering boards' existing legal obligations. In the same year as the NACD handbook's admonition, 2014, SEC (Securities and Exchange Commission) Commissioner Luis Aquilar stated that "boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility do so at their own peril". The new regulators at the SEC, led by Director of Enforcement, Gurbir Grewal, have taken an even more aggressive stance in the last year.

Those perils are changing in real time, just as cybersecurity and privacy threats are changing. However, we can identify certain concrete areas of established liability and strategically identify the emergent risks. Right now, the main liability risks to boards include:

- SEC liability for cyber risks;
- SEC liability for privacy risks;
- officers' and directors' civil liability for breached fiduciary duties;
- direct liability for violation of state data security and privacy statutes, with a special emphasis on California;
- criminal liability for cybersecurity and privacy failures; and
- global civil and regulatory liability, with a special focus on the New York Department of Financial Services (NYDFS) and EU Regulations.

In this chapter, we attempt to explore all of these current trends. At the very end, we will also tackle a few harder-to-classify risks related to United States national security oversight of cyber readiness.

United States: Officers' and Directors' Personal Liability for Cybersecurity and Privacy Failures

On February 21, 2018, the SEC "voted unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents".[1] The SEC did not wait long for the public to absorb this guidance. On April 24, 2018, the SEC "announced that the entity formerly known as Yahoo! Inc. has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts".[2] In the space of two months, the SEC went from "companies also may have disclosure obligations" for breaches to paying $35 million for failure to disclose.[3] When the expectations change so quickly, it is important for officers and directors to understand both the current and developing state of cyber and privacy risks, especially when it comes to personal liability.

SEC liability

The SEC maintains broad (and expanding) authority over directors. This authority begins the moment that a director is named. SEC proxy disclosure rules, among other requirements, mandate that companies disclose, for each director and nominee, the specific experience, qualifications, attributes or skills that led to the conclusion that the individual should serve as a director of the company in light of its business and structure.[4] This disclosure must be made on an individual basis and be specifically linked to the biographical description of each director and nominee. These new disclosure requirements theoretically expose directors to greater potential liability if they are identified in an SEC filing as having a particularly valuable skill or expertise that is valued and relied upon by the company.

The pitfalls of director "cyber hype"

Directors and their companies often tout directors' particular skills that they bring to the board. It makes sense, therefore, that a director may tout their particular cybersecurity *bona fides*. However, overselling one's cyber skills can bring individual liability. In 2003, the SEC amended the proxy disclosure rules to require that a company disclose whether it has at least one "audit committee financial expert" on its audit committee.[5] Prior rules indicated that identifying a director as an expert did not increase their liability for registration statements pursuant to Section 11 of the Securities Act of 1933 (Securities Act), dealing with

liability in connection with registration statements. The safe harbour covered more than merely directors' financial expertise. However, the entire safe harbour language was removed in the wake of the Sarbanes-Oxley Act. Therefore, real individual liability risks flow from whenever a board member touts their expertise in any field, including cybersecurity and privacy.

Section 11 of the Securities Act imposes civil liability on directors of an issuer if "any part of the registration statement, when such part became effective, contained an untrue statement of a material fact or omitted to state a material fact required to be stated therein or necessary to make the statements therein not misleading". Therefore, directors face a real dilemma in that they feel that they should tout their material skills to current and potential shareholders but responsibility and liability flow from those representations. Fortunately, there are many defences available to directors that turn on their level of knowledge.[6] These same defences could be utilised to defend against a Section 11 claim levelled against a director.

Overstatements of cyber readiness now regularly result in SEC liability. For example, in August 2021, the SEC announced a $1million fine against a London-based public company that allegedly misled investors about a 2018 cyber intrusion involving the theft of millions of student records.[7] To avoid a similar outcome:

1. avoid making subjective public statements about an organisation's cybersecurity or data privacy (e.g., the company has "strict" protections in place). These types of statement are very difficult to affirmatively prove as "true";
2. do not describe information as a "potential" risk, if you know that the risk has become reality. For example, it is impermissible to report that a breach "may" include dates of births, where the organisation knows it did;
3. implement a formal process for timely identifying and patching known vulnerabilities (e.g., the company allegedly failed to patch a critical vulnerability for six months after it had been notified); and
4. design disclosure controls and procedures to ensure that those responsible for making disclosure determinations are adequately and timely informed before making and approving public statements. These procedures can and should include:
    a. Initial Investigation:
        i. steps to identify and investigate cybersecurity incidents;
        ii. a plan to automatically assess and analyse the impact of the incident on the company's business and customers;
        iii. a plan to automatically ensure careful analysis of whether the cybersecurity incident is material, giving rise to disclosure obligations;
        iv. a plan to automatically refer potentially material cybersecurity incidents to appropriate committees, including the disclosure committee, for assessment and analysis;
        v. a plan to automatically ensure that material cybersecurity incidents are reported to senior management and to the board of directors; and
        vi. a plan to automatically ensure that material cybersecurity incidents are disclosed to investors and that existing disclosures are reviewed and, if necessary, updated if new facts render them incorrect or misleading.
    b. Mitigation and Remediation:
        i. steps and deadlines to remediate incidents based on severity;
        ii. expressly stating the circumstances under which trading restrictions should be imposed on company personnel who are in possession of material non-public information (MNPI) regarding the incident; and
        iii. provide for the issuance of a document preservation or litigation hold for material incidents or other incidents where the company anticipates litigation.

Board cybersecurity and privacy risk oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure.[8] The SEC has previously said that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company".[9] The SEC has expressly stated that cybersecurity risks are among those that must be reported to directors, with all of the criminal and civil liability that may flow from that notice.[10]

In addition to the cybersecurity actions just discussed, the SEC has also imposed liability upon executive directors for privacy failures. In September 2021, the SEC hit "alternative data provider" App Annie with a $10 million fine and its CEO with a $300,000 fine.[11] Among other failures, the SEC alleges that App Annie misrepresented to users how it would use their data, which constitutes a privacy violation, not a cybersecurity lapse. Specifically, App Annie told customers that it would only use their data in an "aggregated and anonymized form", when it also used such data in a "non-aggregated and non-anonymized form". This misrepresentation, which was obviously fairly technical, resulted in a personal fine upon the CEO. For this reason, officers and directors must take pains to avoid overstating what your company is doing with respect to security or privacy. This includes even these technical aggregation characterisations. If your company does not fully anonymise data or only uses data in an aggregated form, take care to describe your actual uses. Also, officers and directors need to be aware if the company makes a material change in its approach to handling data privacy. Companies must build mechanisms that will alert users to these changes with a clear notice. The SEC has since begun enforcing these requirements with gusto. Of particular note, the SEC has concluded that merely having a policy is insufficient.

On August 30, 2021, the SEC announced the sanctions of eight firms in three actions for alleged "failures in their cybersecurity policies and procedures that resulted in email account takeovers exposing the personal information of thousands of customers and clients at each firm".[12] These actions all also alleged violations of the "Safeguards Rule", Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), which is designed to ensure that investment advisers and broker-dealers protect confidential customer information. All were SEC-registered as broker dealers, investment advisory firms, or both. The SEC Enforcement Division's Cyber Unit noted that "[i]t is not enough to write a policy requiring enhanced security measures if those requirements are not implemented or are only partially implemented, especially in the face of known attacks".

According to the SEC's order against the Cetera entities, between November 2017 and June 2020, cloud-based email accounts of over 60 Cetera Entities' personnel were taken over by unauthorised third parties, resulting in the exposure of personally identifying information of at least 4,388 customers and clients. Cetera protected none of the affected accounts consistent with their own policies. The SEC's order also finds that Cetera sent breach notifications to the firms' clients that included misleading language regarding the promptness of the notifications after discovery of the breach.

According to the SEC's order against Cambridge, between January 2018 and July 2021, cloud-based email accounts of over 121 Cambridge representatives were taken over by unauthorised third parties, resulting in the PII exposure of at least 2,177 Cambridge customers and clients. The SEC's order concluded that Cambridge, despite notice of breaches in 2018, failed to adopt and implement firm-wide enhanced security measures for cloud-based email accounts of its representatives until 2021, resulting in the exposure and potential exposure of additional customer and client records and information.

According to the SEC's order against KMS Financial Services (KMS), between September 2018 and December 2019, unauthorised third parties hijacked cloud-based email accounts of 15 KMS financial advisers or their assistants, resulting in the data exposure of approximately 4,900 KMS customers and clients. KMS failed to adopt written policies and procedures requiring additional firm-wide security measures until May 2020, and did not fully implement those additional security measures firm-wide until August 2020, placing additional customer and client records and information at risk.

Cybersecurity risks and scrutiny of board trading activities

Directors also will face scrutiny for their trades after they are advised of cybersecurity risks. In the wrong situation, a trade could be considered to be an insider trade on non-public information. There is a delicate balance that must be reached here. After all, directors should righteously be informed of significant risks, such as cybersecurity or accounting matters. However, directors must internalise that their cybersecurity briefings can be every bit as material as their regular briefings on accounting controls or other vintage risks. Currently, however, director understanding may be lagging behind their responsibilities.

In the massive Equifax breach, multiple insiders have been charged for trading on the breach information.[13] The SEC has signalled that it will make this type of trading a particular focus.[14] For this reason, the SEC advises that "[c]ompanies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents".[15] That may be easier said than done.

As a practical matter, companies can start to protect their officers and directors from this type of scrutiny (and prevent the underlying suspect behaviour) by establishing policies and procedures in place that:

1. provide regular training to all insiders about cybersecurity risks must be treated like any other material enterprise risks and ensure that the company makes quick and timely disclosure of any material non-public cybersecurity information; and
2. expressly address trading blackouts or similar procedures that will prevent directors, officers, and other corporate insiders from trading during the heightened period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on MNPI about the incident.

Other United States Federal Regulators

This year, the Financial Industry Regulatory Authority (FINRA) issued a lengthy "notice" to "remind member firms of their obligation to establish and maintain a supervisory system, including written supervisory procedures, for any activities or functions performed by third-party vendors, including any sub-vendors that are reasonably designed to achieve compliance with applicable securities laws and regulations and with applicable FINRA rules".[16]

The notice "reiterates applicable regulatory obligations; summarises recent trends in examination findings, observations and disciplinary actions; and provides questions member firms may consider when evaluating their systems, procedures and controls relating to Vendor management".

The FINRA also notes that the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency recently published and requested comment on proposed guidance designed to help banking organisations manage risks associated with third-party relationships.[17]

There are also additional risks from unfamiliar regulatory arms. As part of its reckoning with ransomware events, the United States is turning to sanctions remedies. The Office of Foreign Assets Control (OFAC) is an arm of the U.S. Treasury Department that administers and enforces economic and trade. The OFAC is therefore now administering sanctions in pursuit of private companies' cybersecurity objectives. This may be a necessary step but the intersection of sanctions penalties and private cybersecurity has the potential to be messy. Among other things, this raises the possibility that merely paying the ransomware demand may violate United States laws. A fraught situation has potentially become even more complicated.

Officer and director fiduciary duty law and personal civil liability

Officers and directors can face civil liability if they breach their fiduciary duties, which can lead to a shareholder derivative action wherein the shareholders sue the officers and directors for breaches that harmed the company. Technically, every state has its own standards regarding the fiduciary duties that officers and directors owe to companies and, by extension, the shareholders. Because so many companies are incorporated there, Delaware generally leads the way of fiduciary duty issues. Under Delaware law, directors owe fiduciary duties of care and loyalty to the company.[18] This fiduciary duty of care requires directors to act with a degree of care that ordinary careful and prudent men would use in similar circumstances.[19] Under this standard, directors must act on an informed basis, in good faith, and in the honest belief that the action was in the best interests of the company.[20] Courts have interpreted that this duty of loyalty further includes a duty of oversight, which will be breached if directors "utterly fail" to implement any reporting or information systems or controls or if, after implementing these systems, directors fail to monitor or oversee the operation of these plans.[21] Therefore, Delaware law clearly establishes that officers and directors must set up informational and reporting systems and monitor the results of those systems.

It does not take much imagination to see how these standards could be applied to the new information technology and cybersecurity systems that boards oversee in various companies. A number of derivative actions have been filed following high-profile data breaches. These actions are typically based on claims that, by failing to implement adequate information security policies, the directors allowed a breach to occur that damaged shareholders through decreased stock prices. Although claimants in these cases face a high pleading standard, which we will discuss below, the cases remain expensive and disruptive. Indeed, they can often to lead to resignations by officers and directors.

Civil liability for false and misleading public cybersecurity statements

Companies' public cybersecurity statements or even certain kinds of silence can also create officer and director liability. Section 10(b) and Rule 10b-5 of the Exchange Act prohibit, *inter alia*, making untrue or misleading statements of material fact. These laws further prohibit selective silence about these material facts. Therefore, omitting material facts must not be left unstated if they are necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading. This last requirement is a mouthful. However, in more accessible language: one must tell the truth about anything that is important to the company and one must volunteer facts wherever silence on those facts will actually mislead someone. These requirements to be truthful and forthcoming with the public could conceivably create significant officer and director cyber liability in civil class actions. However, this type of liability will not attach merely when someone wishes to second-guess the content and omissions of companies' cybersecurity statements. As with many liability issues, the quantum of one's knowledge matters.

Unlike Section 11 of the Securities Act discussed earlier, when it comes to exaggerating directors' cybersecurity skills, Section 10(b) requires the intent to deceive, manipulate or defraud, otherwise known as "scienter". Without proof that the director acted with that corrupt scienter, there can be no Section 10(b) liability. That proof of scienter will be absent for many, although not all, officers and directors.

Expert experience and director liability

Experience and context matter when it comes to scienter. Directors with a particular technical or cybersecurity expertise may have difficulty getting Rule 10b-5 claims dismissed because it may be easier for plaintiffs to plead scienter as to them. The *In re U.S. Bioscience Securities Litigation*[22] involved a class action by purchasers of a company's stock against the directors. The judge denied a motion to dismiss Section 10(b) claims against certain outside directors of the company for alleged misstatements, contained in the annual Form 10-K, suggesting that one of the company's products was more effective and further along in clinical trials than was warranted by the facts. In rejecting the motion, the judge explained that "[o]utside directors can be of two very different kinds", those whose role is not intended to be hands on and those who have valuable expertise in the industry.[23] In that case, the directors' "valuable expertise in [the company's] industry" made it reasonable to assume that the directors had inside director knowledge for which they could be held liable.[24]

Similarly, in *Tischler v. Baltimore Bancorp*[25] a class action brought by purchasers of Baltimore Bancorp stock alleged, in relevant part, that the outside directors were liable under Section 10(b) of the Exchange Act and Rule 10b-5, for a purportedly false press release about the adequacy of an offer for the company. In evaluating the defendants' motion to dismiss, the Court dove into the different types of directors and their level of regular briefings. For this reason, audit committee members substantively briefed about the purchase offer had liability. The judge did not stop there, however. Where the outside directors had special knowledge of the company's field the judge concluded that they knew, or should have known, of the risks to the company.[26]

We would also add that certain specialised industries may have pitfalls that will increase the risk of director liability. A good example is the franchise industry. Specifically, if franchisors prescribe the technology that franchisees must use (including for payment card processing), they must ensure that the technology they prescribe is sufficiently secure and kept up to date. This lesson was learned by Sonic Drive-In. After its 2017 data breach, in which hackers stole customer payment card information from more than 700 Sonic franchised Drive-Ins, consumers brought a class action in the Northern District of Ohio. Sonic then moved for summary judgment on the negligence claim. The Court found that under Oklahoma law, parties generally do not have a duty to "anticipate and prevent the intentional or criminal acts of a third party" but can be held responsible for a data breach if their "own affirmative act has created or exposed [plaintiffs] to a recognizable high degree of risk of harm through such misconduct, which a reasonable [person] would have taken into account".[27] The court found four possible "affirmative acts" there that warranted a trial because of the manner in which the technology was imposed upon franchisees by the franchisor.[28]

Second-guessing board decision-making

As mentioned above, some of these risks flow directly from the content of public disclosures but others come from evaluating the objective quality – in light of the attendant circumstances – of officer and director decisions. Officers and directors have a duty of care to the corporation. "Duty of care" refers to a fiduciary responsibility held by company directors to live up to a certain baseline standard of care. This ethical and legal duty requires officers and directors to render their decisions in good faith and in a reasonably prudent manner. That second clause, "reasonably prudent manner", provides the legal ammunition to second-guess failed decisions. Shareholders can probe the reasonableness of officer-and-director decision-making by bringing shareholder derivative actions. These derivative actions argue that officers and directors violated their duty of care when it comes to one or more decisions and therefore injured the company itself. The areas of decision-making failures have run the gamut from poor business decisions, to accounting fraud, to bribery, to rampant officer looting, and – increasingly – failures to provide adequate cybersecurity safeguards.

The Delaware Chancery Court held in *In re Caremark International Inc. Derivative Litigation*[29] (*Caremark*), that the board has an obligation to at least attempt in good faith to invest in or implement a monitoring system that is sufficient to identify legal breaches by the corporation. In *Caremark*, shareholders brought derivative suits against the company, alleging that Caremark's directors breached their duty of care by failing to adequately oversee the conduct of Caremark's employees regarding kickback payments to doctors for Medicare or Medicaid referrals – which is a crime – thereby exposing the company to significant civil and criminal penalties. *Caremark*'s holding outlined director liability for a breach of the duty to exercise appropriate care in two distinct contexts: (1) "from a board decision that results in a loss because that decision was ill advised or 'negligent'"; or (2) "from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss".[30] The *Caremark* court further held that: "it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility." While all of these individual parts of the *Caremark* decision are important, the board must have failed to provide reasonable oversight in a "sustained and systematic fashion", or the information reporting system must be an "utter failure".

Cybersecurity crises of all stripes, including (but not limited to) ransomware response, have now become a staple of derivative lawsuits. Indeed, these claims have become so prevalent that we now have formal court opinions holding that derivative actions against boards for ransomware failures constitute the types of central case that must be covered by directors and officers (D&O) liability insurance.

This does not mean that the cases are always successful. For example, in *Corporate Risk Holdings LLC, v. Rowlands*,[31] the court concluded that case solely "amounts to an allegation that the Board knew about the risk posed by a cyberattack, but did not adequately monitor [the company]'s cybersecurity efforts".[32] Where plaintiffs "focus on a specific, industry-wide risk [the allegations are]… not sufficient to support a *Caremark* claim".[33] For example, directors of banks who failed to recognise the risks associated with the subprime lending market could not be found, merely by ignoring the publicised risks, to have acted in bad faith.[34]

Still, there must be a reporting system so that the board can exercise oversight, and companies often have weak reporting systems. Recently, the Delaware Chancery Court in *In re the Boeing Company Derivative Litigation*, suggests important steps organisations and their boards should take to help protect themselves from shareholder litigation-based security or compliance incidents.[35] This particular litigation arises from two crashes of 737 MAX airplanes manufactured by Boeing in October 2018 and March 2019. Investigations revealed that: (a) the 737 MAX tended to pitch up due to its engine placement; (b) a new software program designed to adjust the plane downward depended on a single faulty sensor and therefore activated too readily; and (c) the software program was insufficiently explained to pilots and regulators. In both crashes, the software directed the plane down. Because this was a derivative action alleging that the board was at fault, the question before the Court was whether "the Company's directors face a substantial likelihood of liability for Boeing's losses" based either on "the directors' complete failure to establish a reporting system for airplane safety", or based on "turning a blind eye to a red flag representing airplane safety problems". The Court concluded that the shareholders sufficiently pled both sources of liability.

One can easily translate plaintiffs' core allegations in Boeing into the arena of cybersecurity and data privacy: (1) "[t]he Board had no committee charged with direct responsibility to monitor airplane safety"; (2) "[t]he Board did not monitor, discuss, or address airplane safety on a regular basis"; (3) "[t]he Board had no regular process or protocols requiring management to apprise the Board of airplane safety; instead, the Board only received *ad hoc* management reports that conveyed only favorable or strategic information"; and (4) "[m]anagement saw red, or at least yellow, flags, but that information never reached the Board". These allegations alone suffice to raise the spectre of officer and director liability and many companies could be described in the same manner.

With these standards in mind, organisations should ensure that appropriate processes are in place to keep boards and management timely and adequately informed about cybersecurity risks that might impact the company. Organisations should also consider providing board members and management with an appropriate level of D&O insurance to help protect these leaders in the event of such litigation, and so that talented management is not deterred from taking such important oversight positions. Most importantly, companies and their management should embrace an agile approach to these issues. The goal of a company is not to hope that things stay the same. Rather, the dynamic, forward-thinking company tries to anticipate the next risk before their directors face personal liability.

However, for now, directors can and should allege that all such allegations of the breach of cyber duty of care constitute "a classic example of the difference between allegations of a breach of the duty of care (involving gross negligence) as opposed to the duty of loyalty (involving allegations of bad-faith conscious disregard of fiduciary duties)".[36] These standards are even more daunting for plaintiffs when "the claims involve a failure to monitor business risk, as opposed to legal risk".[37]

Special director knowledge, Delaware law, and the Section 141(e) "safe harbor"

Delaware case law paints a slightly different outlook as to whether independent directors will be held to a higher fiduciary duty standard because of their special expertise. The *In re Citigroup Inc. Shareholder Derivative Litigation*[38] showed that audit committee financial experts on the board violated their fiduciary duties by allowing the company to engage in subprime lending. The Delaware Chancery Court stated that "[d]irectors with special expertise are not held to a higher standard of care in the oversight context simply because of their status as an expert".[39] Rather than a failure of management oversight, the court viewed the operative issue as a failure to recognise a business risk, emphasising that "[e]ven directors who are experts are shielded from judicial second guessing of their business decisions".[40]

A similar "business decision" deference did not apply to the court's decision regarding *In re Emerging Communications, Inc. Shareholders Litigation*,[41] wherein a director with financial expertise was held to have a duty to voice concerns about the fairness of a proposed transaction's price. The meaning of this case has been widely debated. One interpretation is that, although directors possessing special expertise might not be held to a higher standard under Delaware fiduciary duty law, they may lose the safe harbour protection afforded by Section 141(e) of the Delaware General Corporation Law.

Section 141(e) provides that a director's good faith reliance upon "such information, opinions, reports or statements presented to the corporation...as to matters the member reasonably believes are within such other person's professional or expert competence and who has been selected with reasonable care..." will be afforded legal and factual deference. However, if a director has a particular expertise, then he or she may be unable to rely in good faith on an expert's report (or omission). As companies' SEC proxy disclosures expand upon directors' particular qualifications and expertise, they also effectively limit the scope of Section 141(e) deference. Where a director's cyber *bona fides* are trumpeted, even under Delaware law, they will enjoy less "business decision" deference in matters involving cybersecurity.

There is currently tension developing between these director disclosures, which grow ever more elaborate and more prominent, and the protections of the "business decision" deference. If nothing else, civil plaintiffs may endeavour to weaponise a director's publicly touted expertise to argue that the same director either violated the federal securities laws or his or her fiduciary duties. While all such claims require proof (in this specific context) of the director's knowledge about specific cybersecurity risks, a company's own admissions about a director's cybersecurity knowledge and expertise make the cases easier to allege and prove. Drafting these director cybersecurity disclosures has therefore become a high-stakes balancing act: companies must provide truthful and informative disclosures while also taking care to keep those disclosures lean enough to not create greater litigation risks.

The changes in legal risks appear to *In National Ink and Stitch, LLC v. State Auto Property and Casualty Insurance Company*,[42] a federal court held that a ransomware attack was covered by standard business loss language in a contract. In other words, the risks of a cyber event are so commonplace that any mention of business risk should contemplate these types of losses.

California liability

The California Consumer Privacy Act (CCPA) came into effect on January 1, 2020. The CCPA gives California residents expansive rights[43] over businesses' collection, use and sharing of their personal information. The CCPA: (1) vests general enforcement

authority with the California Attorney General (AG);[44] and (2) creates a private right of action that can only be brought against certain data breach incidents "and shall not be based on violations of any other section of" the CCPA.[45] *More than 50 lawsuits were filed in the first six months after the CCPA came into effect.* Roughly half of these lawsuits related to data breaches. The CCPA created no other types of civil or regulatory liability. However, the CCPA has been used to augment certain existing civil liability theories.

Plaintiffs in the other cases premise claims on alleged violations of consumer rights, often asserting that non-compliance with the CCPA, by extension, constitutes a violation of California's Unfair Competition Law (UCL), Consumer Legal Remedies Act (CLRA) or other causes of action. Many of the suits, whether for data breach or hybridised with another theory, were filed as class action lawsuits.

CCPA enforcement against directors

As mentioned above, the AG has broad authority to enforce all violations of the CCPA. Businesses that violate the CCPA will be subject to civil enforcement actions by the AG. Violating businesses will be given a notice of non-compliance and a 30-day opportunity to cure the non-compliance. Businesses who fail to comply within the 30 days will be subject to an injunction and a civil penalty: $2,500 for each unintentional violation; and $7,500 for each intentional violation. Because of the nature of privacy and cybersecurity events, these violations, and the related penalties, can compound quickly.

The AG has exercised broad authority to enforce California laws against directors in the past.[46] However, enforcement of the CCPA only began on July 1, 2020. The regulations issued after enforcement began.[47] These regulations provide no insight as to whether the AG will seek to hold officers and directors personally liable for a company's violations. Furthermore, active enforcement is still so new that we have few cases to examine that would suggest such authority will be exercised in the future. In general, officers and directors should be aware of the risk that the AG will seek to utilise the CCPA against them if there are systemic failures under that statute.

CCPA civil suits filed in connection with data security incidents

Most CCPA civil cases allege a data breach and then generally contend that the breach was a violation of the CCPA without offering additional details.[48] The CCPA claims usually join negligence, breach of contract, unjust enrichment and violation of the UCL claims.[49] Other cases include greater factual and procedural specificity.[50] However, thus far, none of these cases have sought to hold the officers or directors personally liable.

A number of cases also assert a violation of California's UCL *based upon* a data breach violating the CCPA.[51] The UCL defines "unfair competition" broadly to "mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by [California's false advertising law]". While these cases may seek injunctive relief and restitution, they, like the pure CCPA cases, have not yet articulated any claims against the officers and directors.

These class action cases are not the only types of civil liability that may draw upon the CCPA. One recently filed case is between competing businesses engaged in market research that involves the collection and sale of personal information.[52] The plaintiff alleges that the defendant (the plaintiff's former business partner and now competitor) violated the CCPA by failing to provide sufficient notice of its privacy practices to consumers, and as a result, has gained an unfair and unlawful advantage in violation of the UCL. It is not hard to see insider directors wrapped up in similar theories.

Alleging compliance with the CCPA could even form the basis of some of the derivative actions based upon fiduciary duties discussed earlier. Basically, such cases would allege that violating the CCPA constitutes a gross dereliction of oversight that amounts to a breach of fiduciary duties. Cases utilising these cases are coming but, as we shall see below, the cases filed thus far have not reached a high level of sophistication.

Privacy litigation under the CCPA

In 2021, CCPA liability appears to have been firmed and broadened. For example, it may be safe for an organisation to state on its website and public disclosures that it "take[s] privacy and security seriously" and it is "[d]edicated to maintaining the highest security standards" because this is mere "puffery". However, things become actionable quickly. A claim that the organisation uses "security measures that comply with federal law", however, can be actionable because "a reasonable consumer could rely on this statement as representing that [the organization's] safeguards, which were represented to comply with federal law, were sufficient to protect users' information from ordinary data security threats".[53] In this case, plaintiffs alleged that "[c]ontrary to its representations, [the organization did] not keep its promise to use security measures that comply with federal laws", because the organisation's systems: (a) "lack[ed] simple and almost universal security measures used by other broker-dealer online systems"; (b) "fail[ed] to verify changes in bank account links"; and (c) "failed to store user credentials in an encrypted format". The court found that these allegations were sufficient to withstand a (second) motion to dismiss.

In March 2020, plaintiffs filed *Cullen v. Zoom Video Comm., Inc.*[54] Since filing, the judge in this Northern District of California federal civil action related and consolidated separate actions. This recaptioned Frankenstein monster of a class action lawsuit claims that Zoom illegally shared millions of users' personal information with Facebook and failed to protect their personal information, thus violating the CCPA. Plaintiffs also allege that Zoom's privacy policy contained misrepresentations, that Zoom made inadequate privacy notices about its data collection and use, and that Zoom failed to implement and maintain reasonable security procedures and thus committed fraud in violation of the UCL. The lawsuit also alleges violations of California's CLRA and of California consumers' constitutional privacy rights. The viability of these claims will not be tested soon: a hearing on class certification is scheduled for May 27, 2021.

The *Consolidated Ambry Genetics Cases*[55] are the collective name for the consumer class action cases filed against genetic testing company Ambry Genetics for a January 2020 data breach. Plaintiffs allege that the breach resulted in unauthorised access to customers' personally identifiable information and protected health information, and that Ambry failed to timely report the breach to the government or to customers. These cases were consolidated in June 2020. Despite the wide variety of legal theories on display here, none of the *Consolidated Ambry Genetics Cases* articulate personal liability claims against the officers or directors. The same is true for *Gupta v. Aeries Software, Inc.*,[56] wherein plaintiffs allege that Aeries did not adequately safeguard the personally identifiable information of thousands of vulnerable students, resulting in unauthorised third parties accessing that data. *G.R. v. TikTok*[57] provides yet another CCPA lawsuit that fails to bring claims against the officers and directors. While this case does not directly impact them, officers and directors should take note of the data security and privacy issues that are explored in this case, which alleges unlawful harvesting of biometric identifiers from minor and adult users. These types of issues do not seem to involve data security or privacy, but the

laws and regulations – including the CCPA – increasingly cover both biometrics and the protection of minors. The lawsuits will follow the same path as these laws and regulations.

Other state liability

New York State

The NYDFS, which is responsible for the regulation of banks, insurers and other financial institutions that do business in New York, has a growing role in pushing cybersecurity standards. The NYDFS also possesses an expansive view of its own jurisdictional limits, the entities that it regulates, and their respective officers and directors.

New rules developed by the NYDFS under 23 NYCRR Part 500 (the Regulation), which came into effect on March 1, 2017, require entities that NYDFS regulates to implement specific cybersecurity standards. These standards include establishing a comprehensive cybersecurity policy, completing a written incident response plan (focusing upon reporting breaches within 72 hours to the NYDFS), and promulgating security policies for third-party vendors. The rules require officers and directors to not only designate a chief information security officer (CISO), but also to certify to the NYDFS that the company is in compliance with the regulations.

The CISO must prepare an annual report to the board of directors of the regulated entity regarding its cybersecurity program. The report must: (1) specifically address the identification of material cyber risks to the regulated entity, including any past material cybersecurity event; and (2) report on penetration testing and vulnerability assessments. The CISO must also report to the board of directors about, *inter alia*, multifactor authentication and cyber awareness training for all personnel. In short, the boards of covered companies likely received far more cyber information than they ever received prior to the NYDFS rules. With this deep cyber information in hand, officers and directors were required to submit the first cybersecurity compliance certification to the NYDFS by February 15, 2018. This is a yearly requirement[58] that will annually put directors into the cybersecurity weeds. Moreover, by certifying compliance with these detailed cybersecurity requirements, directors become primary targets of these regulators if a breach occurs.

Other states

A number of other states are considering enhanced cybersecurity and privacy regulations. In the privacy sphere, many states are considering adopting aspects of California's sweeping CCPA. Other states, like Washington, are likely to adopt a framework similar to that utilised by the EU,[59] discussed in further detail below. In any case, the two main risks to directors are the same as they are in California: (1) enforcement actions against officers and directors brought by individual state attorneys general; and (2) private actions alleging either substantive violations of the statute or qualitative violations of the duty of care premised upon a failure to comply with the statute.

Global Personal Cyber Risks for Officers and Directors

New legislation in a range of jurisdictions, most notably in the EU under the new General Data Protection Regulation (GDPR),[60] will hold organisations to higher cybersecurity and cyber standards than ever. With those growing risks in mind, it is useful to consider the potential liability landscape in all jurisdictions in which they are active.

The UK

In the UK, directors' fiduciary duties to the company are largely codified under the Companies Act 2006 (the 2006 Act).[61] Among other things, directors of UK companies possess a duty to promote the success of the company and to exercise reasonable care, skill and diligence in the conduct of their role.[62] Similar to United States civil liability theories, the board's failure to understand and mitigate cyber risks could constitute a breach of these duties. In evaluating these types of claims, UK law requires that we consider the standard of a reasonably diligent person with the knowledge and skill of the director in question. These standards will be tested, as in the United States, via derivative actions.

Recent UK case law has established that civil lawsuits may be brought against violations of the UK Data Protection Act 1998.[63] Perhaps most concerning to companies assessing their civil cyber risks in the UK, is that these Data Protection Act cases can proceed even when the plaintiff has not suffered pecuniary loss. Stated differently, companies face civil losses even where they did not cause anyone to actually lose money. These UK cybersecurity and privacy lawsuits may be brought against the company or the individual directors.

Doing business in the UK will also expose companies to the GDPR. The UK's "Brexit" from the EU will not alter the applicability of the GDPR. The GDPR imposes broad regulations upon companies that control or process personal data. Penalties for GDPR violations can be staggering: non-compliance penalties extend up to the higher of €20 million or 4% of the organisation's worldwide revenue. Moreover, directors of public companies bear the responsibility for compliance with the GDPR and personal liability for any fines and penalties.[64] In addition, the Information Commissioner's Office, the UK's data privacy regulator, can compel future conduct from senior board members to ensure that the company complies with its ongoing data protection obligations.

Directors of regulated entities also need to be aware of their UK personal regulatory obligations. In the financial services sector, the Financial Conduct Authority closely scrutinises directors, and will take action if a director fails to discharge his or her regulatory duties as a result of not properly managing the organisational cyber risks. Similarly, directors of publicly traded companies must appropriate disclosures under the UK Listing Rules. These disclosures may include a wide range of adverse cyber events. Directors face personal liability for any failure to disclose such events.

The EU

In addition to the GDPR, which we discussed with regard to the UK, the EU is developing a number of new laws and regulations regarding cybersecurity and privacy. For example, the EU Network and Information Security Directive (NIS Directive)[65] will require companies in certain industries (including such far-flung industries as financial services and "water transport")[66] to implement certain minimum cybersecurity standards. While enforcement of the NIS Directive is still unclear, and its effectiveness is under review as of October 2020, the mere fact that the NIS Directive will be implemented in the EU should alter the way that directors think about cybersecurity implementation.

Ireland's Data Protection Commission recently announced a whopping €225 million fine against WhatsApp for allegedly failing to comply with GDPR transparency requirements.[67] The fine follows a lengthy July 28, 2021 decision issued by the European Data Protection Board. The decision was largely driven by the extent to which "hashed" consumer data constitutes "personal

data" for the purposes of the GDPR. Among other things, the answer seems to depend upon "when" the data is hashed and whether or not the hashing "guarantee[s] the anonymisation of data". These fine distinctions further raise the heat on companies.

Amazon announced in August 2021 that it had been hit with a record $888 million fine for purportedly violating the GDPR. In its July 30 SEC 10-Q filing, Amazon stated that "On July 16, 2021, the Luxembourg National Commission for Data Protection [the "CNPD"] issued a decision against Amazon Europe Core S.à r.l. claiming that Amazon's processing of personal data did not comply with the EU General Data Protection Regulation. The decision imposes a fine of €746 million and corresponding practice revisions. We believe the CNPD's decision to be without merit and intend to defend ourselves vigorously in this matter." 10-Q at 13. The CNPD Complaint apparently alleges that Amazon analyses users' behaviour to build profiles for targeted advertising without user consent and in violation of the GDPR.

Germany

German law provides similar personal liability pitfalls for directors. Under German law, directors can be held liable for breach of their duties. These cybersecurity duties include, *inter alia*, a duty to ensure that there is adequate IT infrastructure to protect data security and to avoid cyber risks. Directors must therefore ensure that certain technical standards are met, which are actually spelled out in the German Data Protection Act (*Bundesdatenschutzgesetz*) and the German IT Safety Act (*Bundessicherheits- und Informationstechnikgesetz*). The German laws also require a high level of ongoing systems monitoring. This can mean that the failure to note intrusions, which can sometimes last months, can itself constitute an organisational failure. While all of these regulatory responsibilities should concern directors, it bears noting that German law generally only permits director liability to the company not to third parties, although the risk exists.

United Arab Emirates

Under United Arab Emirates (UAE) law, officers and directors of a company can face personal liability for matters relating to cyber risk. The board of directors of a public joint stock company is liable to the company, its shareholders and third parties for certain acts, including fraud, misuse of power, breach of the UAE Commercial Companies Law or the company's articles of association, or an error in management.[68] While little case law exists on how these provisions may be applied, there is a possibility that cybersecurity and privacy failures may fall under the law.

Of more concern should be potential criminal liability under UAE law. Officers and directors should be mindful that potential criminal liability exists for the unauthorised disclosure of personal information. Reportedly, in March 2015, three executives in the UAE were all temporarily imprisoned on the grounds of a breach of privacy in connection with the installation of CCTV. Jail time is therefore a real possibility in the UAE.

Canada

Canadian law can impose personal liabilities upon officers and directors of a company for matters relating to cybersecurity and privacy risk under Canadian law. The Canada Business Corporation Act RSC 1985 (CBCA) requires every director to exercise their powers and duties honestly and in good faith, with a view to the best interests of the corporation; and exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances.[69] The CBCA provides for shareholder derivative actions for breaches of duties owed by directors to the company and the recovery of monetary damages on behalf of the company.[70] Thus, in theory, companies operating in Canada bear many of the same litigation risks for their cybersecurity and privacy failures.

As in the United States, Canada imposes liability upon directors for omissions or misrepresentations in public disclosures. Moreover, since September 2013, the Canadian Securities Administrators have instructed that issuers should expressly disclose their cyber-crime risks, any cyber-crime incidents, and characterise their cybersecurity controls in a prospectus or a continuous disclosure filing.[71]

Officers and directors also face statutory liabilities for under privacy statutes in Canada. These statutes only exist in certain discrete Canadian jurisdictions, however. Breaching Quebec's privacy statute can lead to monetary fines against directors who ordered or authorised the breaches.[72] Likewise, Ontario's Personal Health Information Protection Act 2004 contains penalties to officers and directors for the wilful collection of health information without reasonable protections.[73]

South Africa

South African law also creates personal liabilities for officers and directors in connection with cybersecurity and privacy risks under South African law. As in other countries utilising a derivation of the English legal system, the failure to implement reasonable cybersecurity measures could constitute a breach of directors' fiduciary duties. As in countries like the United States and England, these fiduciary duties were established by way of the common law and have later been codified. Just as in these other countries, officers and directors have a duty to maintain certain minimal cybersecurity and privacy procedures and oversight. Officers and directors could theoretically face personal liability to the company and to third parties for a breach of these duties. A breach of directors' fiduciary duties could lead to claims being brought against officers and directors. Similarly, just as in the UK and the United States, directors may face personal liability in contract or tort. This risk is even more acute in South Africa, where the governing laws permit great personal liability, even when working through the "legal fiction" of a corporation.

Moreover, a breach of fiduciary duty could lead to South African regulators taking action against officers and directors. For example, the Companies and Intellectual Property Commission (CIPC). The CIPC can investigate these complaints and various mechanisms allow action to be taken against a company or its directors.

Common law, rather than a statute, primarily protects the South African right to privacy However, South Africa has also passed the Protection of Personal Information Act, of 2013 (POPI).[74] Under the POPI, regulatory action may be taken against an organisation or person for any violation. Therefore, depending on the nature of each violation, a director may face civil fines, administrative fines, penalties and even a period of imprisonment. The POPI does not fully become effective until July 2021, which is when the "grace period" ends.

Australia

As in the UK, United States, and South Africa, officers and directors face certain familiar personal liability risks for a company's cybersecurity and privacy failures. All officers and directors have

a key responsibility to ensure that companies adopt appropriate risk management strategies to protect the company and its shareholders via their duty of care and due diligence, under both Section 180 of the Corporations Act 2001[75] and the common law. The Australian corporate regulator, the Australian Securities and Investments Commission (ASIC), has the power to bring an action against officers and directors for a breach of their duties. The consequences are potentially serious, and include a declaration of contravention, pecuniary penalties, compensation orders and disqualification of the director or officer from managing a corporation. ASIC Report 429[76] states that: it considers board participation important to promoting a strong culture of cyber resilience; and a failure to meet obligations to identify and manage cyber risks may result in stiff penalties. Finally, a failure by officers and directors to take reasonable steps to prevent, or respond appropriately to, a cyber or privacy incident may also give rise to Australian civil proceedings, either via derivative action brought by the shareholders or by affected individuals.

Emergent Areas of Special Cybersecurity and Privacy Concern to Officers and Directors

Data and privacy security is not just the target of criminals. Foreign governments utilise their military and intelligence resources to actively attack the privacy and data assets of private companies. These state actors carry special risks that officers and directors must acknowledge. For example, Chinese military hackers stole U.S. Steel's trade secrets and gave them to Chinese steel companies so that they could better compete in western markets.[77] U.S. Steel attempted to meet this threat by filing an action in the International Trade Court.[78] After a long and costly fight, U.S. Steel withdrew its cybertheft action, but the legal fight is far from over.[79] Whenever nations endeavour to interfere with businesses, the officers and directors should take note.

State actor privacy and data security concerns can even lead to the forced liquidation of assets. The saga of TikTok is well known at this point. However, it bears repeating that the United States' insecurity about the state of TikTok's privacy and data security procedures and controls has led directly to a likely "forced" liquidation of United States assets. Russia's potential control over private data led to similar insecurity over the viral FaceApp.[80] In other words, state actors are now colliding with data security and privacy in a manner that provides an existential threat to many companies. Where the risks to companies are great, the personal liability risks to officers and directors can be correspondingly large.

Certain business sectors can also face outsized risks of which officers and directors must be aware. If a company services sensitive or classified governmental contracts, they will be both a target of bad actors and also subject to increased regulatory oversight. The dimensions of those standards, whether under the Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity requirement or under government contracting requirements that the National Institute of Standards and Technology (NIST) guidelines be met, should be the subject of a different article. However, for our purposes, we should acknowledge that officers and directors must be aware that these standards exist – and work to satisfy them – or else they face the loss of extremely valuable contracts.

Not only traditional defence or governmental industries face these threats. State-sponsored hackers hacked Yahoo![81] and the World Anti-Doping Agency.[82] Zappos was hacked by a hacker who works for the successor to the KGB.[83] While Zappos is a very successful online commerce company, one would not usually think of them as a geopolitical target – that is all changing. Similarly, as discussed above, one response to the ransomware threat has been to sanction certain ransomware payments, which means the expedient act of paying ransomware may now place officers and directors at odds with the OFAC. This is a significant wrinkle that further complicates companies' decisional calculus. Officers and directors must address these risks now or they face the prospect of personal liability for their failures later.

Endnotes

1. https://www.sec.gov/news/press-release/2018-22.
2. https://www.sec.gov/news/press-release/2018-71.
3. https://www.sec.gov/rules/interp/2018/33-10459.pdf; see also 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (August 15, 2000) [65 FR 51716 (August 24, 2000)].
4. Proxy Disclosure Enhancements, SEC Release Nos 33-9089, 34-61175, IC-29092; 74 FR 68334 (December 23, 2009).
5. Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002, SEC Release Nos 33-8177, 34-47235; 68 FR. 5110 (January 31, 2003).
6. Director liability under the operative sections of the federal securities laws turns on the director's knowledge or the reasonableness of his or her beliefs in a specific situation and can presumably be impacted by his or her particular qualifications, background or expertise. A director has a "due diligence" defence to liability under Section 11 if he or she sustains the burden of proof that, with regard to any part of the registration statement not made under the authority of an expert, the director "had, after reasonable investigation, reasonable ground to believe and did believe, at the time such part of the registration statement became effective, that the statements therein were true and that there was no omission to state a material fact". Federal courts have generally taken the view expressed in *Feit v. Leasco Data Processing Equipment Corp.*, 332 F. Supp. 544, 577 (E.D.N.Y. 1971) that "[w]hat constitutes 'reasonable investigation' and a 'reasonable ground to believe' will vary with the degree of involvement of the individual, h[er] expertise and h[er] access to the pertinent information and data". Thus, directors who are insiders, or directors who are attorneys involved in preparation of the registration statement, generally are expected to make a more complete investigation and have more extensive knowledge of the facts at issue.
7. https://www.sec.gov/news/press-release/2021-154.
8. 17 CFR 229.407(h); 17 CFR 240.14a-101 – Schedule 14A.
9. Final Rule: Proxy Disclosure Enhancements, Release No. 33-9089 (December 16, 2009) [74 FR 68334 (December 23, 2009)], available at http://www.sec.gov/rules/final/2009/33-9089.pdf.
10. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos 33-10459; 34-82746, (February 26, 2018), available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.
11. https://www.sec.gov/news/press-release/2021-176.
12. https://www.sec.gov/news/press-release/2021-169.
13. https://www.sec.gov/litigation/complaints/2018/comp-pr2018-40.pdf, https://www.sec.gov/litigation/complaints/2018/comp-pr2018-115.pdf.
14. https://www.sec.gov/news/testimony/testimony-oversight-us-securities-and-exchange-commission.
15. *Id.* at 3-4.
16. https://www.finra.org/rules-guidance/notices/21-29.
17. https://www.federalreserve.gov/newsevents/pressreleases/bcreg20210713a.htm.
18. Section 141(a), Delaware General Corporation Law.

19. *Graham v. Allis-Chalmers Mfg Co.*, 188 A 2d 125, 130 (Del 1963).
20. *Smith v. Van Gorkom*, 488 A 2d 858, 872 (Del 1985).
21. *Stone v. Ritter*, 911 A 2d 362, 370 (Del 2006).
22. 806 F. Supp. 1197 (E.D. Pa. 1992).
23. *Id.* at 1203.
24. *Id.* at 1204.
25. 801 F. Supp. 1493 (D. Md. 1992).
26. *Id.* at 1501.
27. https://media-exp1.licdn.com/dms/document/C4D1FAQEv_akeXkjhTQ/feedshare-document-pdf-analyzed/0/1631188958350?e=1632236400&v=beta&t=S4tMjTX3B4d-KhDSWkcNMsdOGgdy85TV7V7ZkQGtCSMI.
28. First, "Sonic created a permanently-enabled VPN tunnel that did not block foreign IP addresses that gave [its required POS vendor] and anyone with [its] credentials—access to each [POS]-served franchise point-of-sale systems". Second, "Sonic created, [a] remote user credential [for its POS vendor]...without multi-factor authentication enabled". Third, Sonic "required franchisees to use middleware that did not support point-to-point encryption". Finally, Sonic "controlled middleware upgrades, and caused delays that left franchisees operating vulnerable systems".
29. 698 A.2d 959 (Del. Ch. 1996).
30. *Id.*
31. No. 17-cv-5225(RJS), 2018 WL 9517195 (September 29, 2018).
32. *Id.* at *6.
33. *Id.* (citing *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d 106, 128 (Del. Ch. 2009)) ("[A] showing of bad faith is a necessary condition to director oversight liability".)
34. *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d at 112 ("[A] showing of bad faith is a necessary condition to director oversight liability".)
35. https://casetext.com/case/in-re-the-boeing-co-derivative-litig.
36. *In re Gen. Motors Co. Derivative Litig.*, C.A. No. 9627-VCG, 2015 WL 3958724, at *17 (Del. Ch. June 26, 2015).
37. *Wayne Cty. Emp.'s Ret. Sys. v. Dimon*, 629 F. App'x 14, 15 (2d Cir. 2015).
38. 964 A.2d 106 (Del. Ch. 2009).
39. *Id.* at 128 n.63.
40. *Id.*
41. C.A. No. 16415, 2004 BL 1814 (Del. Ch. May 3, 2004).
42. 435 F.Supp.3d 679 (D. Md. 2020).
43. The Act provides California residents with the right to seek access to, or deletion of, their personal information, as well as the right to object to the sale or sharing of such information with third parties.
44. See Cal. Civ. Code § 1798.155(b).
45. See Cal. Civ. Code § 1798.150(c) ("The cause of action established by this section shall apply only to violations as defined in subdivision (a) [regarding data breaches] and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.")
46. https://oag.ca.gov/news/press-releases/attorney-general-sues-remove-stakeholder-members-iso-board.
47. https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.
48. See, e.g., Complaint, *Albert Almeida, Mark Munoz, and Angelo Victoriano v. Slickwraps Inc.*, No. 2:20-at-00256, at 28, 48 (E.D. Cal. March 12, 2020); Complaint, *Daniela Hernandez v. PIH Health*, No. 2:20-cv-01662, at 6, 19, 38 (C.D. Cal. February 20, 2020); Complaint, *Bernadette Barnes v. Hanna Andersson, LLC, and Salesforce.Com, Inc.*, No. 4:20-cv-00812-DMR, at 3, 15 (N.D. Cal. February 3, 2020); Complaint, *Juan Maldonado v. Solara Medical Supplies, LLC*, No. 3:19-cv-02284-H-KSC, at 3, 21 (S.D. Cal. November 29, 2019).
49. See, e.g., Complaint, *Slickwraps* at 39, 44, 46 and 48; Complaint, *Hernandez* at 22, 27, 30 and 37; Complaint, *Barnes* at 16 and 22; Complaint, Maldonado at 23, 30, 33 and 34; see also *Rahman v. Marriott International, Inc.*, Case No. 8:20-cv-00654 (C.D. Cal. April 3, 2020) (This putative class action on behalf of California residents against Marriott for a data breach that was announced on March 31, 2020 alleges violation of the CCPA and UCL, as well as breach of contract and implied contract, negligence, and unjust enrichment.)
50. See, e.g., Complaint, *Michele Pascoe v. Ambry Genetics*, No. 8:20-cv-00838, at 50 (C.D. Cal. May 1, 2020) at 50; Complaint, *Lopez* at 44.
51. See, e.g., Complaint, *Slickwraps* at 48; Complaint, *Hernandez* at 37–38.
52. See Complaint, *Bombora v. ZoomInfo*, No. 20-cv-365858 (Cal. Super. Ct. June 10, 2020).
53. https://www.linkedin.com/posts/brian-levine-49579348_mehta-v-robinhood-nd-cal-sept-8-2021-activity-68420814-64369061889-jyRm.
54. Case No. 20-cv-02155 (N.D. Cal. March 30, 2020).
55. Case No. 8:20-cv-00791 (C.D. Cal.).
56. Case No. 8:20-cv-00995-FMO-ADS (C.D. Cal. May 28, 2020).
57. Case No. 2:20-cv-04537 (C.D. Cal.).
58. https://www.dfs.ny.gov/industry_guidance/cyber_filings/requirements.
59. https://fpf.org/2020/01/13/its-raining-privacy-bills-an-overview-of-the-washington-state-privacy-act-and-other-introduced-bills/#:~:text=The%20Act%20would%20be%20a,creates%20a%20nuanced%20approach%20to.
60. https://eur-lex.europa.eu/eli/reg/2016/679/oj.
61. https://www.legislation.gov.uk/ukpga/2006/46/contents.
62. *Id.* (sections 172 and 174, 2006 Act).
63. *Google Inc v. Vidal-Hall and other* [2015] EWCA Civ 311 **.
64. Per the first and second paragraphs of Article 169, the members of the management board must act as thorough and diligent owners, and they are jointly and severally liable for the damage inflicted on company by their actions.
65. 2016/1148/EU**.
66. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.
67. https://lnkd.in/dbEF98Gx.
68. Article 162, UAE Federal Law No 2 of 2015 on Commercial Companies.
69. https://laws-lois.justice.gc.ca/eng/acts/C-44/page-21.html?txthl=duties+duty#s-122.
70. https://laws-lois.justice.gc.ca/eng/acts/C-44/page-41.html?txthl=derivative#s-239.
71. https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20130926_11-326_cyber-security.htm#:~:text=To%20manage%20the%20risks%20of,and%20their%20clients%20or%20stakeholders.
72. http://legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1.
73. https://www.ontario.ca/laws/statute/04p03.
74. https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf.

75. http://www5.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s180.html#:~:text=Care%20and%20diligence%2D%2Dcivil%20obligation%20only,-Care%20and%20diligence&text=The%20director's%20or%20officer,in%20their%20position%20would%20hold.
76. https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf.
77. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
78. https://www.wsj.com/articles/u-s-steel-accuses-china-of-hacking-1461859201.
79. https://www.wsj.com/articles/u-s-steel-withdraws-hacking-claim-against-chinese-rival-1487183293.
80. https://www.pbs.org/newshour/science/is-faceapp-a-security-risk-3-privacy-concerns-you-should-take-seriously.
81. https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html.
82. https://www.nytimes.com/2019/10/28/sports/olympics/russia-doping-wada-hacked.html.
83. https://www.forbes.com/sites/thomasbrewster/2017/03/20/alexsey-belan-yahoo-fbi-hacker-allegations/#bc236cd76f24.

Christopher Ott, CIPP/US, leads data security, privacy, and white-collar litigation and investigations. Leveraging his experience from more than 13 years at the U.S. Department of Justice (DOJ), including successfully litigating complex data security matters, conducting hundreds of investigations, and winning dozens of appeals, Mr. Ott works with clients on disputes and strategy relating to data security, privacy, blockchain, and AI issues. Mr. Ott has handled hundreds of matters involving the intersection between white-collar matters (accounting, securities, money laundering) and cybercrimes (from international criminal gangs to state actors). For example, much of his current work involves business litigation and investigative matters involving stablecoin and PoS blockchain technologies. In his most recent governmental role, Mr. Ott acted as Supervisory Cyber Counsel to the National Security Division of the DOJ. Mr. Ott consulted extensively with the intelligence community and coordinated extensively with regulators such as the U.S. Treasury Department, the Federal Communication Commission (FCC), the Federal Trade Commission (FTC), and the SEC.

Rothwell Figg
607 14th Street NW, Suite 800
Washington, D.C. 20005
USA

Tel: +1 202 783 6040
Email: cott@rfem.com
URL: www.rothwellfigg.com

The Privacy, Data Protection & Cybersecurity team at Rothwell Figg helps clients understand and navigate these rapidly evolving areas of law. We work with our clients to prepare, integrate, and implement compliance strategies, frameworks for risk management, and best practices. We have experience working closely with our clients: to build data inventories and assess their legal obligations; to implement back-end and structural changes that are not only compliant, but also workable; to prepare written policies, assessments, forms, and notices to effectuate legal requirements and best practices; to negotiate, draft, and review agreements for compliance; and to help train staff. We can assist with the design and implementation of incident response plans and, if there ever is an incident, we can serve as trusted advisors, from the investigation stages through to litigation, helping you navigate disclosure requirements to public authorities. Most of the attorneys in the practice group are experienced litigators with deep technical backgrounds, and have represented clients in a wide variety of venues, including before numerous government agencies, and in state courts, federal district courts and courts of appeal, and the United States Supreme Court.

www.rothwellfigg.com

ROTHWELL FIGG
IP Professionals

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: glg global legal group