Welcome to the inaugural edition of the **FINEX Observer**.

We are proud to bring you the first of what we hope is a useful resource. Written for today’s global risk managers, general counsel, board members and executives, the **FINEX Observer** shares our insights into noteworthy trends, developing concerns and, most importantly, opportunities that are hidden in the financial and executive risks of today’s global business environment.

A central theme for this inaugural edition is the evolving risk of individual accountability. Regulators, investors and customers around the world are trending toward holding individuals — as opposed to corporate entities — liable for perceived wrongdoing. An understanding of this exposure and how one’s risk transfer/insurance program may respond is, therefore, essential, as is recognizing and managing other very particular and developing risks, such as transactional-related exposures and cyber-related threats.

You will see that many of the topics discussed are relevant to organizations in any jurisdiction around the world, while some topics are clearly more laser-focused to specific jurisdictions (i.e., the U.K.).

This publication would not be possible without the tireless efforts of our external and internal contributors, our fellow editors and the entire Willis Towers Watson team. This was a truly global effort, and we thank everyone for their work.

**Editors**

- **Rob Yellen**, D&O and Fiduciary Liability Product Leader, FINEX NA
- **Brian Weiss**, Head of Claims, FINEX NA
- **Anthony Rapa**, Western Regional Leader, Claims, FINEX NA
- **Andy Doherty**, Thought and Product Leader, FINEX NA
Content

Individual accountability
Protecting D&Os from “informal” investigations ......................................................... 05
Personal accountability of senior managers in the U.K. .................................................... 09
FCA v. Macris: A problem for senior managers in the U.K.? .......................................... 11
A conflict over privilege: The U.K. Senior Managers Regime and the legal function ...... 14

Individual risks – transactions
Private vs. public D&O coverage in M&A ........................................................................ 18

Emerging risks
D&O risk in the age of cyber insecurity ............................................................................. 23
Fee litigation plague spreads to universities and mid-market companies ...................... 30
Will emissions disclosures remain a hot D&O risk? ......................................................... 33
Individual accountability
Protecting D&Os from “informal” investigations

By Gina Macari (FINEX Claims and Legal, Chicago)

Since well before the 2010 innovation of “inquiry” coverage (a/k/a “pre-claim” investigation coverage), D&O insurance had been expected to respond well to investigations of directors and officers. The dot-com tech bubble cleanup, followed by the financial crisis resulted in heightened investigation risk for individuals, particularly company executives. Insurance carriers responded by detaching investigation from the coverage conditions of a claim (in some cases) and a stated wrongful act, thus putting more focus on this increasing exposure.

Today, we are in an “age of accountability.” While some wonder whether the new administration in Washington is likely to have a reversing impact on this mindset, others believe that the societal and regulatory focus on holding individuals accountable is like a bell that cannot be unrung. Regulatory enforcers, lawyers, directors, officers and corporate insurance buyers have continuously learned as the nuances around investigations have laid bare potential flaws in how traditional D&O insurance responds, particularly for publicly traded companies and their D&Os. Even today, carriers are not consistent in their approach in extending coverage to individuals for investigations. Some have updated their entire base forms to make sure administrative provisions align well with the coverage extension (and to market their commitment to covering these exposures), while others offer cobbled solutions that fall short of providing the protections needed. This note highlights some of the key issues to consider in reviewing the adequacy of your D&O coverage for inquiries and investigations.

Before digging into investigation coverage, here is a quick look at investigations and the terms that describe them.

Investigation semantics

Securities and Exchange Commission (SEC) enforcement (investigations and inquiries)

The October 28, 2016 edition of the SEC’s Enforcement Manual [Link] (the Manual) articulates these stages of investigation:

1. Complaints, tips and other referrals: Before SEC activity rises to a level it deems an “investigation,” the SEC will engage in activity designed to vet complaints, tips and other referrals and, of course, its own hunches. For example, the staff reviews complaints for “apparent reliability, detail and potential violations of the federal securities laws.”

2. Inquiries: A complaint, tip or other referral that appears to be serious and substantial could result in a “matter under inquiry.” Although still not an “investigation” by SEC standards, the decision to designate activity as a matter under inquiry (a/k/a an inquiry) turns on the SEC’s determination of:

   “(1) whether the facts underlying the Inquiry show that there is potential to address conduct that violates the federal securities laws; and

   (2) whether the assignment of an Inquiry to a particular office will be the best use of resources for the Division as a whole.”

   (The Manual §2.3.1 “Opening a MUI”)

Inquiries are preliminary in nature (should last no more than 60 days) and typically involve incomplete information. So, the bar for an Inquiry is pretty low. In the SEC’s view, an inquiry is NOT an investigation.

3. Informal investigations: SEC “investigations” are opened in two ways:

   “(1) when an Inquiry is converted to an Investigation, or

   (2) an Investigation is opened independent of an Inquiry.”

   (The Manual §2.3.2 “Opening an Investigation and Converting or Closing a MUI”)

The opening of an investigation requires the staff to “conduct an evaluation of the facts to determine the Investigation’s potential to address conduct that violates the federal securities laws.” This is different from an inquiry in that an investigation is typically opened only after the staff “has done some additional information-gathering and analysis.”

Essentially, an SEC “Investigation” is generally opened only after the SEC conducts a preliminary investigation.
Formal orders of investigation:

The Manual does not parse SEC “investigations” into “formal” and “informal” investigations. Rather, that colloquial distinction essentially differentiates between SEC investigations in which the Commission has issued a formal order of investigation and those where no such order has been issued.

A formal order of investigation empowers the SEC staff to issue subpoenas requiring a witness to provide documents and testimony under oath pursuant to the authority granted by law to the Commission. (See Section 19(c) of the Securities Act of 1933, Section 21(b) of the Securities Exchange Act of 1934, Section 209(b) of the Advisers Act of 1940, and Section 42(b) of the Investment Company Act of 1940.)

This can be an important distinction to have in mind when reviewing D&O coverage for investigations. Informal investigations have no subpoenas and, as an evidence-gathering process, often specify no target. Nevertheless, unlike inquiries, which generally are limited to 60 days, “informal” investigations have no limit on their duration. Complying with an “informal” SEC request is hardly trivial as the practical consequences of perceived cooperation can have a material impact on outcomes, and, naturally, the scrutiny of the SEC in any context is no light matter. The fact is — informal investigation costs can be the bulk of the cost of any investigation. This is true not just for the organization, but for its directors and officers too.

2017 — A new administration

It has been reported that the SEC recently revoked subpoena authority from about 20 senior enforcement officials and limited that authority to the enforcement division director. Pulling back subpoena authority may not, however, result in fewer or less expensive SEC investigations, or less need for counsel. Rather, it could merely mean that insureds will spend more time and money responding to informal investigations and inquiries. With respect to D&O exposure, this authority pullback could actually reverse a trend in recent years — the increased likelihood of FORMAL investigations — that consequently made informal investigation coverage somewhat less important.

Other enforcement

The SEC is not the only authority that enforces securities laws, rules and regulations. The Department of Justice (DOJ), state and foreign authorities and exchanges may also conduct investigations.

Internal investigations

A company may investigate internally, too. In fact, as a defense to whistleblowing accusations and/or to maximize cooperation credit with the authorities, it is more likely than ever that a company will perform its own investigation of alleged wrongdoing.

None of these potential sources of investigations use the same semantics as the SEC. Their investigations are never designated as “formal” investigations. So beware of coverage that only triggers upon a “formal” investigation.

Coverage for investigations of public company directors and officers

Investigation vs. claim

“Claims-made” directors and officers insurance liability coverage has traditionally triggered upon claims first made against insureds during the policy period. While the definition of “claim” has evolved and become far more complex over the years, at its core, a “claim” is a written demand seeking monetary or non-monetary relief and it includes lawsuits, alternative dispute resolution requests, and other requests for other proceedings.

Answers to the question of whether an investigation or inquiry is covered, and to what extent, as a “claim” will vary based on the product and how it has been amended. Also, that question may be answered differently depending on who is investigating (i.e., the SEC vs. the DOJ), who is being investigated (the company vs. its directors or officers) and who is looking for the answer (a carrier, an insured or the courts).

Traditional, standard D&O policies typically include some coverage for investigations of individuals in the standard definition of “claim.”

For example:

A Chubb policy includes in the definition of “claim” any:

“(C) investigation of an Insured Person for a Wrongful Act, commenced by the Insured Person’s receipt of a written document from an Enforcement Unit identifying such Insured Person as the target of an investigation, including a Wells Notice, target letter or search warrant; or

(D) written request upon an Insured Person for witness testimony or document production, commenced by the service of a subpoena or other similar document compelling such testimony or production of documents in connection with any matter described in Subsections (A) through (C) above; provided that in such event the Company shall pay, on behalf of such Insured Person, Defense Costs incurred solely by such Insured Person in responding to such request.”
The main issue with this type of language is WHEN the coverage is triggered. By the time the insured person is subpoenaed or identified in writing as a target of the investigation, the investigation may have already progressed significantly, meaning that the need for, and cost of, legal counsel started long before that point in time.

As a coverage trigger, a person is subpoenaed or identified in writing as a target. Enforcement authorities often ask for information and cooperation that is not legally compelled through informal requests for information, documentation and interviews. Importantly, that cooperation extends, as is reflected in the Yates Memo, to the company as a tool for enforcement—well before the SEC or others legally compel production via a subpoena. Coverage that starts before testimony is “compelled” would help to avoid gaps.

Wrongful act dilemma

Another place where traditional D&O coverage may fall short of ideal for investigations/inquiries is the traditional coverage condition of a wrongful act — the requirement of an actual or alleged act, error or omission in an insured capacity (or in some cases, a claim asserted against an insured by virtue of an insured capacity). For an investigation conducted as an evidence-gathering process, often no allegations are made, no target may be identified and it may be unclear whether insured capacities are relevant.

Ideal coverage for investigations triggers when the need for counsel begins, not when enforcement has already built a case and approached their target.

Inquiry coverage

In 2010, “pre-claim inquiry” coverage was introduced and, over time, became readily available in standard and endorsed D&O policies. With that enhancement, coverage began to respond better and provide broader investigation coverage for individual insureds.

Common “pre-claim inquiry” terms trigger the policy early enough to cover the costs of preparing and defending an insured person (importantly, not the company) for an interview by governmental investigators. A reasonable form of inquiry coverage will cover both the insured person(s)’s expenses directly (non-indemnified loss, or “Side A” coverage) and the company’s advancement/indemnification of an insured person’s expenses (indemnified, or “Side B” loss). While inquiry coverage typically triggers upon less formal, less targeted investigations, it is not meant to cover industry-wide or sector-wide regulatory inquiries, or routine or regular governmental regulatory reviews. This is an especially important distinction for companies and D&Os in the most highly regulated industries, such as the financial services industry.

Coverage trigger

The “trigger” for inquiry coverage varies by policy language. In some policies, coverage may be triggered by an insured person “volunteering” to meet with governmental investigators. In most instances, however, a “verifiable request” from the investigator is required. In less liberal policies, inquiry coverage appears to require a formal, written, even compulsory demand of an insured person to submit to an interview or provide documents.

Document production

There can be various levels of coverage for the costs associated with document production under D&O policies.

- Some will cover the insured person's production of documents to government investigators.
- Some will exclude from that coverage the costs of producing documents if those same documents also exist in the files of the organization.
- Some exclude the costs of production if the documents have already been produced by the organization.
- Some exclude costs of production altogether, from any source.

Important: An early version of inquiry coverage that eliminates coverage for the costs of preparing for and “defending” the “interview” when a document request was included, is still in the market today.

Notice, relation back and applications

A key characteristic of inquiries and investigations that can have a dramatic impact on coverage is the challenge of identifying when they start (or stop). For versions of investigation and inquiry coverage that seek to extend such coverage by expanding the definition of “claim,” that extension potentially implicates notice requirements and the policy’s “claims first made” limitations. This creates a potential Catch-22 for insureds. On one hand, it seems better to have coverage (and the definition of claim) trigger earlier. Yet, an early investigation trigger may also give carriers an opportunity to assert a late notice defense if minor investigations later become more significant or expansive.
A common solution: make investigation coverage elective. Today, many inquiry coverage terms are designed to permit the insured a choice:

- Provide notice of the investigatory inquiry, with coverage provided under the terms of the policy. Benefit: if the inquiry ripens into a covered claim, notice will have been deemed to have been provided in the policy period in which the pre-claim inquiry was tendered.
- Not reporting the investigation/inquiry: An insured might not perceive the likelihood of covered costs, or the insured may believe that the inquiry is particularly unlikely to proceed past an early stage. Or, the insured may believe that insurance premiums will go up unnecessarily if the pre-inquiry claim is tendered for inquiry coverage. In such circumstances, the policy would permit the insured to choose not to tender the claim while retaining the right to later tender a claim on the same facts. Benefit: flexibility, depending on the specifics of the inquiry.

Important: Because of the variability in wordings, great care should be exercised in reviewing policy terms and conditions not just when faced with an inquiry or investigation, but during policy placement as well.

- There are some policies that expressly assure the policyholder that the decision not to report a pre-claim inquiry is not a breach of any notice provisions of the policy, and, at a minimum, such language is recommended. However, even with the assurance provided by such language, policyholders should be aware that difficulties may still arise and seek expert coverage advice:
  - Circumstances: Forms without permissive investigation notice generally allow the policy to be tagged with a notice of circumstances. That notice will not trigger coverage, but it will tie related future claims back to that policy if any arise.
  - Public company disclosure: For publicly traded companies, the decision whether to tender the pre-claim inquiry to insurance carriers may be intertwined with other disclosure obligations and considerations.
  - Claim vs. investigation: When an insured chooses not to tender the pre-claim inquiry, the insured may take the risk that the pre-inquiry inquiry or investigation may be asserted by a carrier to be a defined "claim" The failure to timely report that claim and adhere to all the notice requirements may jeopardize coverage.

Insurance grant: Definition of claims vs. separate investigation grant

D&O insurance forms grant investigation coverage in one of two ways. (i) Either they expand the definition of “claim” to pick up investigations, or (ii) the entire form has been reworked to separately grant coverage for inquiries and investigations. The latter is clearer than the former as the entire form is designed with the character and nuances of investigations and inquiries in mind, reducing the chances for unintended consequences. That said, some policies that expand the definition of “claim” do address these nuances, but need extra vigilance.

Proactive recommendations

With it likely that the “age of accountability” will continue in some form, today’s investigation threats remain dynamic and, therefore, today’s directors and officers can expect they will remain under the regulatory and enforcement microscope. With that, investigation and pre-claim inquiry coverage should be a top priority when securing insurance. Five key considerations:

1. Coverage grant: Make sure coverage triggers are the broadest possible.
2. Administration: Make sure the policies' administrative features (notice requirements, consent to incur costs and attorneys, cooperation with the insurance company requirements) are clear, flexible and optimized.
3. Side-A: Make sure to have Excess Side-A (non-indemnified loss coverage) difference-in-conditions coverage above your traditional "A-B-C" directors and officers liability coverage. Under traditional policies, Side A limits of liability are shared with B & C limits (coverage for the organization) and therefore can be eroded by organizational losses. Also, coverage for individuals may become more difficult to access in extreme events like bankruptcy/insolvency of the organization.
4. Wording/placement: Enlist your trusted broker, your insurance counsel and your defense counsel to make sure, at the placement stage, you have coverage that will respond if confronted by investigations or inquiries.
5. Actual investigations: In the event of an inquiry or investigation, make sure to take your D&O insurance into account early. Talk to your broker, including your claim advocate, and your counsel. Consider attorney/client privilege. With your insurance professionals and counsel, work as a team to discuss policy provisions and get insights into potentially applicable insurance coverage.

Taking proactive steps through your insurance professionals will help maximize existing investigation coverage, including inquiry coverage, and keep you aligned with your insurance company as the situation unfolds.

Note: The DOJ’s Individual Accountability for Corporate Wrongdoing Memorandum (known as the “Yates Memo”) outlines six measures aimed at strengthening the pursuit of individual corporate wrongdoing: (i) Facts — Must provide the DOJ with all relevant facts about the individuals involved in corporate misconduct; (ii) From The Beginning — Criminal and civil corporate investigations should focus on individuals from the inception of the investigation; (iii) Better Communication — DOJ Criminal and civil attorneys need to routinely communicate; (iv) Corporate Only Settlements — No corporate resolution will provide protection from criminal or civil liability for any individuals; (v) Plan Required — The DOJ will not settle with the company without a clear plan to resolve related individual cases before the statute of limitations expires. Decisions not to pursue individuals must be memorialized; (vi) Consistent Civil Focus — Civil Attorneys should “consistently” focus on individuals. The DOJ will decide whether to bring suit against an individual on factors beyond ability to pay.
Personal accountability of senior managers in the U.K.
By Claire Nightingale (FINEX Claims, Financial Institutions, London)

The first phase of the Senior Managers and Certification Regime came into force in the U.K. in March 2016. This regime is designed to impose personal accountability upon those working in and, especially, running financial institutions in the United Kingdom. Its origins lie in the banking crisis of 2008 and in the conclusions of the Report of the Parliamentary Commission on Banking Standards. Below we explore the background and first year of the regime.

Background
The Commission on Banking Standards was established in 2012 and was chaired by the influential Conservative Member of Parliament Andrew Tyrie, also chair of the highly regarded Treasury Select Committee. In June 2013 the Commission published its final report “Changing Banking for Good” at which time Mr Tyrie commented

“A lack of personal responsibility has been commonplace throughout the industry. Senior figures have continued to shelter behind an accountability firewall…”

The Commission’s recommendations encompassed a range of areas, including creating better functioning and more diverse markets; but the first recommendations were enhancements to the regulatory regime, directly addressing personal responsibility as follows:

1. **Senior Managers Regime:** A new Senior Persons Regime (replacing the Approved Persons Regime) to ensure that the most important responsibilities within banks are assigned to specific, senior individuals so they can be held fully accountable for their decisions and the standards of their banks in these areas.

2. **Certification Regime:** A new licensing regime underpinned by Banking Standards Rules to ensure those who can do serious harm are subject to the full range of enforcement powers.

3. **Conduct Rules:** A new criminal offence for senior persons of reckless misconduct in the management of a bank, carrying a custodial sentence.

The first phase of the new regime regulates individuals performing a senior management function in U.K. incorporated banks, building societies, credit unions, certain investment firms and U.K. branches of foreign banks. The regime will be extended to all financial services firms from 2018. The rules now specify that

“A firm must ensure at all times one or more of its Senior Management Function (“SMF”) managers have overall responsibility for each of the activities, business areas and management functions of the firm” (SYSC 4.7.8R)

Both the Financial Conduct Authority and the Prudential Regulatory Authority have specified functions that fall within the regime. These roles include the members of the board and individuals who hold key roles, such as chairs of risk, audit and remuneration and those responsible for compliance and anti-money laundering. Individuals carrying out each of these functions must be pre-approved by the regulator(s), must comply with the Conduct Rules and will be subject to a duty of responsibility as set out below.

The duty of responsibility

**No reverse burden of proof:** The early expectation was that the legislation would create a reverse burden of proof with a presumption of responsibility on senior managers. This led to a considerable amount of commentary and concern and in the event, in October 2015, prior to implementation of the regime, the position was watered down.

**Duty to take reasonable steps:** The position is that senior managers have a statutory duty to take reasonable steps to prevent a regulatory breach. It remains for the regulator to prove they have fallen short of the obligations to take reasonable steps to ensure that the firm is controlled effectively, that the firm (or the part thereof for which they are responsible) complies with the requirements and standards of the regulatory system and that delegation of responsibilities is to an appropriate person whom they oversee — significantly, in the light of the concerns around the role of general counsel on which we comment below.

**Duty to proactively disclose:** Significantly, a senior manager must disclose any information of which the regulator(s) would reasonably expect notice and must be open and cooperative with the regulator.

**Responsibilities map and statement of responsibilities:** To ensure that responsibilities are clear and to create a level of personal accountability (which will facilitate the enforcement process), institutions are required to supply a responsibilities map which sets out the allocation of responsibilities and how the firm is governed. This sits alongside each individual performing a senior management function, “SMF” having a statement of his or her responsibilities. As such, in theory, no key role will fall between the gaps. This concept is bolstered by the obligation on a senior manager, before relinquishing his or her responsibilities, to prepare a handover certificate setting out how the role and responsibilities have been fulfilled and providing information and material that would be relevant to anyone taking over the role. In short, the regime forces firms and individuals to create documentation on which the enforcement teams may later rely.

**Certification:** It is also important to note that individuals who do not fall within the SMF regime will likely nonetheless fall within the certification regime. This requires firms themselves to assess the fitness and propriety of employees in roles which could pose a risk of significant harm to the firm or any of its customers.
In September 2016, the FCA marked the first six months of the regime, giving commentary on implementation to date and proposing further measures to strengthen the regime and reinforce the importance of individual accountability at the most senior levels within organizations. Andrew Bailey, chief executive of the FCA, said,

“Knowing who is responsible for what is critical for firms and regulators and we have seen genuine engagement on this from the Board down”

Responsibility, accountability and governance in financial services firms and their impact on conduct remains a priority for the FCA with a focus on the most significant drivers of good or poor mindsets and behaviors. The FCA therefore launched a consultation on the duty of responsibility and the circumstances in which enforcement actions can be taken against a senior manager, if they are responsible for the management of any activities in relation to which there is a regulatory breach, and they do not take such steps as a person in their position could reasonably be expected to take to avoid the breach occurring or continuing. The response is imminent and will no doubt make interesting reading.

In March 2017, a year into the regime, the FCA noted that changes have been put in place to ensure that individual responsibility is at the heart of how firms conduct themselves and that these responsibilities are being taken “more seriously.” The regulators say that they are continuing to work to ensure that responsibilities are properly allocated and understood in firms. If they are successful in this it will perhaps be good news all round.
FCA v. Macris: A problem for senior managers in the U.K.?

By Francis Kean (Executive Director, FINEX Global)
Originally Posted on FX-MM: 28 March 2017 [here]

There have always been concerns about the risk of collateral damage to reputation for individuals caught up in large scale FCA enforcement proceedings involving their employers. Last week, the U.K. Supreme Court’s decision in the case of the Financial Conduct Authority v. Macris clarified the law, but in a way that will give no comfort to senior managers.

The controversy relates to the extent to which individuals are entitled to make representations as to their innocence in circumstances where their employers (or more likely perhaps) their former employers have reached a settlement with the FCA. This is a battleground ripe for conflicts of interest between employer and employee. Settlements with the regulator invariably include provision for the publication of a Final Notice containing criticism of the conduct which gave rise to the enforcement proceedings in the first place. Where an individual is named, Section 393 of the Financial Services and Markets Act 2000 gives him or her the opportunity to make representations. What happens where the individual is not named but is still arguably “identified” in the Final Notice? That was the issue before The Supreme Court.

A new problem is now facing senior managers

The case stemmed from the FCA’s Final Notice to JP Morgan in the infamous London Whale case, in which the bank was fined £137 million. The Notice referred to the bank’s “CIO London management” but did not name any individuals. Mr. Achilles Macris at the relevant time served as part of the management structure of the bank. He exercised a controlled function and had the job title of international chief investment officer. He complained that, looked at in its proper context, the Notice did, in effect, “identify” him through use of the phrase “CIO London management” and that he had been denied an opportunity to make representations in his defense. The FCA disagreed but had lost on this issue both in the Tribunal and in the Court of Appeal.

By Francis Kean (Executive Director, FINEX Global)
Originally Posted on FX-MM: 28 March 2017 [here]

Previously, the Court of Appeal had found that the test for identification should be similar to that applied in defamation cases; in other words: “Are the words used …. such as would reasonably in the circumstances lead persons acquainted with the claimant/third party, or who operate in his area of the financial services industry, and therefore would have the requisite specialist knowledge of the relevant circumstances, to believe as at the date of the promulgation of the Notice that he is a person prejudicially affected by matters stated in the reasons contained in the notice?” On the facts, the Court of Appeal found for Mr. Macris.

The new test for identification

Delivering the leading majority judgment, Lord Sumption rejected the defamation test laid down by the Court of Appeal in favor of a narrower formulation which he set out as follows: “In my opinion, a person is identified in a notice under section 393 if he is identified by name or by a synonym for him, such as his office or job title. In the case of a synonym, it must be apparent from the notice itself that it could apply to only one person and that person must be identifiable from information which is either in the notice or publicly available elsewhere. However, resort to information publicly available elsewhere is permissible only where it enables one to interpret (as opposed to supplementing) the language of the notice.”

Lord Sumption gave a number of reasons for this narrow approach including the “…practicalities of performing the Authority’s investigatory and disciplinary functions.” As he put it: “The internet is a fertile source of information and gossip for those who are willing to go to some trouble to discover… identity. The Authority will not necessarily know what, if any, further information about the business, the facts or the individuals involved may be available to knowledgeable outsiders or discoverable from publicly available sources. In those circumstances it must be able to ensure, by the way in which it frames its own notices, that a third party is not ‘identified’ in the notice, even if he or she is identifiable from information elsewhere.”
The problem for senior managers

That's all very well from the regulator's point of view. It also has the benefit of clarity but will be of cold comfort to individuals and especially to senior managers who are the focus of the new Senior Managers Regime. Indeed, the implications for individuals of this strict approach were a cause of concern for some of the Supreme Court judges including Lord Wilson who issued a dissenting judgment favouring a broader test. He focused on “the particular sort of damage which a wrong criticism of an individual in a notice given by the Authority is likely to cause to him.” As he put it: “It is the reaction to the criticism of those who operate in the same sector of the market which is likely to cause him most damage; for it may prejudice his ability to remain in his employment, or to find other employment in that sector, or otherwise to continue to earn his livelihood in the industry.”

It strikes me that this is the crux of the problem for senior managers. After all, the interests of employers often keen to do a deal with the regulators and move on are not aligned with those of the individuals caught up in the investigation. As another of the judges, Lord Neuberger, put it in his judgment:

“The interests of the addressee of a notice who is accused of failings, and those of a third party such as an employee of the addressee, who may be identifiable as responsible for, or implicated in, the alleged failings, are by no means necessarily aligned. Thus, it may well be that an employer would want to try and curtail any publicity about the alleged failings by quickly negotiating and paying a penalty, even if there may be grounds for challenging the allegation in whole or in part. But this may often not suit the employee, who might well feel that, in the absence of the Tribunal exonerating him, his reputation, and therefore his future employment prospects, could be severely harmed or even ruined.”

Most senior managers will lead productive and well remunerated professional lives and will never be unfortunate enough to find themselves caught up a major regulatory investigation. I would be willing to bet that the common assumption among this majority is that, provided they have not behaved dishonestly or recklessly, their employers will look after them in the event of trouble. This case and in particular the passage quoted in Lord Neuberger’s judgment quoted above ought to give this majority pause for thought. The lesson here is that senior managers in the (albeit unlikely) case of need should ensure they can always reliably call on (and pay for) independent legal advice.
A conflict over privilege: The U.K. Senior Managers Regime and the legal function
By Claire Nightingale (FINEX Claims, Financial Institutions, London)

In the course of the implementation of the Senior Managers and Certification Regime, a discrete issue as to the roles and responsibilities of in-house lawyers in regulated financial institutions has come to the fore. In September 2016, the Financial Conduct Authority (FCA) published a discussion paper on the overall responsibility and the legal function, particularly in light of feedback received from firms as to whether the in-house counsel function should be subject to the personal accountability regime imposed on those working in and running financial institutions in the U.K.

The FCA accepts that there was some uncertainty at the time of implementation about how to deal with the legal function, as it is not included in the indicative list of business activities and functions that require a senior manager, but states that responsibility for the management of the legal function is currently, and should continue to be, included in the regime. The FCA says that the purpose of having a specific function called “other overall responsibility” (SMF 18) is to allow a firm to allocate responsibility to someone whose job is not otherwise in the list of SMFs. It allows firms to have pre-approved senior managers without constraining their ability to organize their affairs. Concerning the legal function, the FCA states that it wishes to balance the independence of the legal function and its ability to offer legally privileged and impartial advice.

The discussion paper sets out a number of reasons to keep the head of legal or general counsel (HoL) function in the SMR. These include that the legal department is an “activity, business area or management function,” the failings of which can impact the wider business and that there are arguments in favor of the view that the inclusion of the head of legal does not prejudice legal privilege. Given the importance of legal professional privilege, this is a contentious view.

Legal professional privilege is a substantive and important right as a matter of public policy in English law. Indeed it has been described as a fundamental human right that legal advice cannot be effectively obtained unless the client is able to put all the facts before the advisor without fear that they may afterwards be disclosed and used to his prejudice (per Lord Hoffmann in R (Morgan Grenfell & Co Ltd) v Special Commissioner of Income Tax [2003].

This is the purpose of legal advice and litigation privilege: that the client’s advice is maintained in confidence and he is protected from the risk that the advice he received is later used against him. Importantly the privilege belongs to the client and cannot be waived without his consent. This protection should logically extend beyond civil and criminal proceedings to other authorities, such as regulators.

Some bodies and commentators have expressed their views. The British Bankers’ Association (BBA) and the Association for Financial Markets in Europe (AFME) (together BBA-AFME) published a letter to the FCA on May 10, 2016. The letter urged the FCA not to include the legal function within the scope of the SMR. BBA-AFME argued that the legislative and regulatory framework underlying the Senior Managers Regime does not contain any requirement that the role of HoL should be designated as a senior management function. Their view is that the legal function is an advisory one and not one that involves management of a firm’s affairs. They consider that:

- the independence of the legal function may be compromised, leading to firms engaging with their legal function less and/or using external counsel more frequently.
- the Head of Legal would be subject to a complex matrix of conflicting duties arising from their SMR responsibilities and their existing regulatory obligations set by the SRA (the U.K. Solicitors’ Regulatory body).
- the Head of Legal would face a conflict of interest between protecting his/her own personal position under the SMR and the duty to act in the best interests of their client, including protecting legal advice privilege. The BBA-AFME are concerned that a Head of Legal might be required to disclose legally privileged material to comply with their regulatory duties.

It is not entirely coincidental, given the developments we describe above, that during 2016, the Law Society has also been considering the use of privilege in regulatory investigations. This has become a highly difficult area for financial institutions, and it has in the past been suggested by both the FCA and the Serious Fraud Office (SFO) that a firm that has not handed over privileged material has not cooperated with them, and thus cannot obtain the upsides of, for example, potentially reduced fines, etc., or in the case of the SFO, a deferred prosecution agreement for having done so. In November 2015, the FCA’s director of enforcement (Jamie Symington) stated that asserting legal professional privilege.

"Looks... like a ‘gaming’ of the process in order to shroud the output of an investigation in privilege"

This has been particularly the case in relation to the creation of early interview notes and communications at the outset of an internal investigation (a point which has subsequently been litigated; it was held that legal advice privilege is restricted to communications between a lawyer and those individuals authorized to seek and obtain advice on behalf of an organization, not those authorized to provide information [RBS Rights Issue Litigation]). The Law Society’s draft guidance picks up quite clearly on this tension, stating that
“Certain regulatory bodies and enforcement authorities have voiced concerns that they see legal professional privilege sometimes being used to frustrate their efforts.”

and goes on to suggest that adverse inferences should not be drawn from a claim to legal professional privilege. Furthermore, in January 2017 the Law Society issued a practice note stating its guidance that legal professional privilege is “sacrosanct” and the law is clear that adverse inferences cannot be drawn from a client’s refusal to waive privilege, and no regulator or investigator is entitled to pressure a client to waive privilege. The Law Society has also stated that, clearly, legal functions should not be included in the Senior Managers Regime because such inclusion can create conflict and erode legal professional privilege. The guidance is clear that lawyers have a professional duty to advise their clients of the right to privilege and their entitlement to assert it.

As things stand, the guidance to the Conduct Rules (but not the Senior Management Conduct Rules) now recognizes that the right to preserve legal professional privilege may be a good reason not to cooperate with a regulator’s request for information. The paper suggests clarifying that this guidance applies across the board. It is consistent with the fact that the Financial Services and Markets Act provides that no power under the Act can be used to require disclosure of protected items, which are stated to be defined in terms that are materially identical to legal professional privilege in section 10 of the Police and Criminal Evidence Act 1984.

To balance the FCA discussion paper, it does acknowledge reasons to exclude the HoL function from the SMR, recognizing and succinctly setting out the concerns around privilege and setting out that it might be said that the role is advisory and does not involve management of the regulated firm’s affairs of the firms. It further notes that all staff are required to be open and cooperative with the regulator. Whatever the outcome of the debate, it is clear that the personal accountability of lawyers in financial services extends beyond their obligations to their clients.
Individual risks — transactions
Private vs. public D&O coverage in M&A
By Matthew L. Jacobs, Esq. (Jenner & Block LLP, Washington DC)

Matthew is co-chair of Jenner & Block’s Insurance Recovery and Counseling, Reinsurance, and International Arbitration Practice and one of the most experienced insurance coverage litigators in the United States. We are thankful for his contribution to the Observer and to Willis Towers Watson’s clients.

While it is commonly accepted that director and officer (D&O) liability insurance is critical to the directors and officers of both public and private companies, not all D&O policies provide that coverage equally well. Due to the differences in the nature and extent of the exposures facing private and public companies, there are substantive distinctions between private company and public company D&O coverage forms. While both types of companies face similar risks, the nature and extent of their exposures can differ based upon whether they are a privately held portfolio company, for example, or a Fortune 500 public company. This article highlights some of these critical differences by examining some of the common claim scenarios that result from the typical merger and acquisition transaction.

Background
There are many similarities between public and private company D&O policy forms. Both typically contain three insuring agreements, which are normally identified as Side A, Side B and Side C coverage. As one court succinctly put it: “(1) losses resulting from [non-indemnified] claims against directors and officers of [the company] for individual acts, also known as ‘Side-A’ coverage; (2) losses resulting from [the company’s] indemnification of its directors and officers, also known as ‘Side-B’ coverage; and (3) losses sustained by [the company] and its subsidiaries as a result of securities law violations, also known as ‘Side-C’ coverage.”

Entity coverage: A relatively well known difference between public and private D&O forms is the scope of Coverage C, the entity coverage.

- A public company D&O policy insures the company only for securities claims (as defined by the policy) brought against the company.
- A private company D&O policy typically insures the company broadly for claims against it, and those claims usually include employment-related claims, claims brought by government regulatory agencies, antitrust claims and claims brought by customers and vendors.

This is one of the reasons why private company D&O coverage is deemed broader than that afforded to public companies — the breadth of entity claims covered by Side C of private company policies.

Duty to defend: Unlike their public counterparts, private D&O forms may afford defense coverage on a duty to defend basis.

- A public company D&O policy typically affords no duty to defend, but instead requires the insurer to reimburse the policyholder for defense costs (which are typically defined as “loss” in the policy).
- A private company D&O policy typically includes a duty to defend, which permits the insured to tender the claim to the insurer for defense, by the insurer’s selected defense counsel, who will handle the claim through final resolution.

In some circumstances, and where there may exist a conflict between the insurer and the policyholder based upon the insurer’s coverage positions as expressed through a “reservation of rights” letter, the insurer is permitted to fulfill its duty to defend by allowing the policyholder to retain independent counsel of its choice.

Some states do not require that a conflict exist before the policyholder may be entitled to independent counsel, as opposed to “panel counsel.” For directors and officers of smaller companies, the duty to defend coverage may prove to be critically valuable as it may afford a broader defense that can apply to uncovered claims as long as covered claims are being defended.

Key mergers & acquisitions coverage issues
Mergers among companies raise a number of insurance coverage considerations. First, the acquiring company will need to undertake due diligence on the to-be acquired company’s insurance coverage program. Additional factors must be considered as they relate to the merger of the two companies’ D&O programs. This can become particularly complicated when both companies are private companies and have private company D&O insurance policies.

General D&O considerations
Overarching coverage considerations for D&O policies in the mergers and acquisition context are relatively similar for public and private companies.

Importantly, the D&O insurance programs of the two separate entities will need to be combined upon the merger for going-forward conduct, while also preserving coverage for pre-acquisition conduct. This means that the existing coverage program for one entity (likely that of the acquired company), after acquisition, will need to be put into runoff with a tail period, usually of six years, to protect the directors...
and officers of the acquired company from liability for wrongful acts that took place pre-acquisition. This is typically accomplished through a run-off endorsement.

Often the purchase or acquisition agreement will contain some level of requirements as to D&O insurance, which can serve as a guide for structuring the insurance program post-merger. Certainly, it is best to consider these requirements before the merger goes through.

There are certainly additional coverage considerations in the M&A context, including whether cancellation provisions of a policy are triggered by the merger (most public and private D&O policies contain “change in control” provisions), the pricing for additional coverage, whether and how different exclusions and other terms and conditions between the two programs will come into play, and whether additional capacity (limits) will be needed to offer sufficient insurance protection post-merger. These may be particularly important issues for private or smaller publicly owned companies that may not have the same level of expertise or the same degree of risk management and legal support, even though the directors and officers face the same issues as those on the boards of larger companies.

A critical consideration under both public and private D&O is how to address claims based on acts, errors or omissions that actually or allegedly happen before and after the effective time of the transaction. Often referred to as straddle coverage, carriers are sometimes willing to enhance coverage to help address challenges posed by coverage for claims that involve pre- and post-merger acts, errors and omissions.

**IPO considerations**
When a private company is considering an initial public offering (IPO), this implicates a number of D&O insurance issues that are unique to D&O policies. The public company/private company D&O policy distinction means that, if a business transitions from being a privately held company to one that is publicly traded, it will face very different options for D&O insurance coverage. As a result, before making the transition from private to public, a company should ensure that it retains coverage for any potential liabilities arising from conduct taking place prior to and up to the time of the IPO, and securing the broadest possible entity coverage for as long as possible.

**Typical IPO-related claims**
A company’s ability to retain coverage under a private A company’s ability to retain coverage under a private company D&O policy for conduct prior to and leading up to an IPO depends upon the type of IPO being undertaken as well as on the securities exclusion already contained in the private company D&O policy.

One example of a securities exclusion contains relatively restrictive language, with only a limited exception for a certain subset of securities claims:

*Insurer shall not be liable for Loss under this Coverage Section on account of any Claim: ... alleging, based upon, arising out of, attributable to, directly or indirectly resulting from, in consequence of, or in any way involving:*

(i) any public offering of Securities undertaken or consummated by or on behalf of the Company (“Public Offering”), or the solicitation, sale, purchase, distribution, or issuance of any such Securities, whether any such activity occurs or allegedly occurs prior to, during, or after such Public Offering; or

(ii) any Wrongful Act, including without limitation any actual or alleged violation of any Securities Law, relating in any way to a Public Offering or to any Securities issued, sold or distributed pursuant to a Public Offering, whether any such Wrongful Act occurs or allegedly occurs prior to, during, or after such Public Offering

provided that this exclusion shall not apply to Claims arising from an offer, sale or purchase of Securities in a transaction that is exempt from registration under the Securities Act of 1933, or any amendments thereto or any rules and regulations promulgated thereunder.
The range of securities exclusions available in the market highlights the need for companies to evaluate their coverage before they consider an IPO. If a company even potentially considers undertaking an IPO, inadequate coverage or overly broad exclusions could result in a denial of coverage once a claim arises.

**Portfolio companies or spinoffs**
Coverage for IPO-related claims can be even more complicated when a private company spins off a portfolio company (or a company spins off a profitable subsidiary). In this situation, there might be claims that impact both companies, resulting in competition for policy limits. For example, if a private equity fund spins off a portfolio company into a publicly traded company, consideration must be given not only to retaining coverage for the portfolio company until the IPO but also how coverage will function for insured who serve as board members of both the private equity fund and of the former portfolio company/newly public company.

This situation not only raises issues of insufficient coverage, but it also raises capacity issues, i.e., identifying the capacity in which a particular person is acting (as a director of the private equity fund, of the spun off portfolio company, or of both) to determine whether claims are covered.

Often D&O policies include language in the definitions of “insured” or “wrongful acts,” or in exclusions, which condition coverage on the requirement that an individual acts in only one capacity and no other. Much like mergers and acquisitions, straddle coverage is necessary.

Outside the U.S., coverage may be available in a specialized D&O form, the public offerings of securities insurance solution. That product would ring-fence coverage for IPO-related exposures in one single tower of coverage with built runoff.

Regardless of how this situation would play out, it is a stark reminder that policyholders must remain sensitive to the need to craft or revise insurance policies for private equity/portfolio company spin-off situations.

**Conclusion**
As we said at the beginning, not all D&O policies are created equal. Nowhere are the differences between public and private D&O coverage more apparent than in the context of M&A. Although we have examined some of the most common claim and coverage issues that arise in the context of a corporate acquisition or sale, there are also many other transaction-specific issues to be aware of. Before embarking on any M&A transaction, it is essential to not only ascertain the availability an amount of D&O cover but also understand the specific type of insurance involved, take advantage of opportunities to right-size coverage and avoid potential pitfalls. Only with this knowledge can the full value of your risk transfer program be understood.
Emerging risks
D&O risk in the age of cyber insecurity

By Rob Yellen (D&O and Fiduciary Liability Product Leader, New York)

As cyber insecurity advances at breakneck speed, so too do the attendant risks. It’s not just data and firewalls anymore. With cyber threats and privacy breaches making regular headlines, and seemingly everyone — even the CIA — falling victim, we are more cyber-threatened than ever. In this world of ever-increasing risk, the boardroom must take note.

Expectations are changing: As our awareness grows, so do our expectations for the caretakers of our information, investments and cyber-accessible assets. We would all like to believe that someone has this all under control — the government, technology companies, internal IT departments, big corporations, financial institutions, credit card vendors, website hosts, your cell service and phone manufacturer, social media sites, search engines... someone, right? The reality is that business and governmental leaders cannot forego the unprecedented opportunities that technology, data and the evolving social paradigm present to make sure we are perfectly cyber secure.

“Risk management is no longer simply a business and operational responsibility of management. It has also become a governance issue that is squarely within the purview of the board. Accordingly, oversight of risk should be an area of regular board assessment.”


Cyber has become a board of directors-level risk management issue: Even with prudent controls, consistent employee training and exemplary IT staffing and performance, the dark side of digital connectivity will eventually find its way in. Cyber crooks will get things of value and criminals will hold us hostage or cause problems. Meanwhile, the threat landscape expands exponentially.

The good news is that awareness of cyber insecurity is growing and our sophistication is maturing. However, with the torrent of noise around cyber insecurity, we risk becoming desensitized — not blasé, just saturated. How much more noise can we absorb and meaningfully digest? Enough already! We have our businesses to run, too.

With cyber risks inherently incorporeal, we also risk being less offended by cyber-attacks than we might if physically attacked, or less outraged than we might if we knew we were being personally spied on.

On the flip-side, however, the day may come when the perceptions of regulators and investors changes. Although cyber-attacks will undoubtedly continue to plague the business world, stakeholders will take increasingly closer looks at what was done to minimize the harm at the top.

Cyber insecurity is no longer just a technology problem. Siloing, we now know, is incomplete and ineffective. As cyber insecurity matures, best-in-class risk management solutions are evolving into a holistic, enterprise-wide effort driven from the board room down through the entire organization, engaging everyone from executives to brand new employees. It’s about people and culture.

So, how can we live with cyber insecurity? Are we ready? Can we address cyber threats much like we do other unavoidable risks like germs and accidents — as just part of everyday life? We may not have a choice. While we can mitigate cyber risk, we cannot eliminate it. The risk is too dynamic and pervasive. The financial incentives of the dark side of cyber are way too high, and our current legal and enforcement regimes are still relatively ill-equipped to address this incorporeal, ubiquitous risk.

Insurance (cyber-specific) has a role: Much like we insure against our exposure to physical accidents and liabilities, we do have insurance solutions to help transfer difficult-to-manage cyber insecurity risks.

Cyber and D&O insurance: While cyber insurance plays a critical role in managing direct cyber insecurity risk, current cyber insurance does not reach indirect risks traditionally addressed under D&O insurance. This leaves unanswered the question of how well will D&O insurance respond if liability for cyber insecurity reaches the C-suite or the boards of directors. The consensus suggests that for the perils typically covered under D&O liability insurance, such as derivative and securities class action lawsuits, D&O insurance should already respond.
Cyber exposed

For this cyber insecurity discussion, let’s assume:

- Cyber-attacks on your business are commonplace, sophisticated and persistent. Because they almost certainly are.
- Information has leaked, and it is readily available to criminals on the dark web.
- On your system somewhere is dormant, undetected malware that has expanded and become “weaponized.”
- Your internet-capable phones (cell and wired or wireless VOIP) and other networked devices allow competitors and others to eavesdrop on your every word — even when those devices appear off.
- A loss of internet connectivity will materially impact the viability of your business, and a prolonged loss of internet connectivity could ruin you.
- Corruption of, or damage to, your systems by ransomware practitioners (with varied agendas) could materially impact your business. Imagine if your accounts receivables were permanently unreliable.
- Your organization holds, or is responsible for, private and confidential data, if only for your employees.

Now, let’s assess potential directors and officers liability risk.

D&O cyber risks

Fiduciary duties
Risk management clearly falls within directors’ fiduciary duties. Not day-to-day risk management, but oversight of the function. We continuously see more organizations putting more attention into such areas as enterprise risk management (ERM). The appearance of chief risk officers (CRO) within companies is more commonplace today than ever before. In other words, “risk” is on the agenda for board meetings, and many stakeholders in companies entrust boards of directors with the power to manage risk prudently. But while directors clearly have these fiduciary duties, the bar for plaintiffs to establish those duties have been breached is still pretty high.

“Generally where a claim of directorial liability for corporate loss is predicated upon ignorance of liability creating activities . . . only a sustained or systematic failure of the board to exercise oversight — such as an utter failure to attempt to assure reasonable information and reporting system exits — will establish the lack of good faith that is a necessary condition to liability. Such a test of liability — lack of good faith as evidenced by sustained or systematic failure of a director to exercise reasonable oversight — is quite high.”

In re Caremark International Inc. Derivative Litigation, 698 A.2d 959, 971 (Del. Ch. 1996)

With respect to cyber insecurity, plaintiffs have tried to make claims against directors and officers stick. So far, no success. No wonder, with the bar so high.

Federal laws and regulations
While fiduciary duties may not be the driving D&O risk arising from cyber insecurity, regulatory risk may be scary enough. The following highlights are intended to be illustrative rather than exhaustive.

NIST Framework: The National Institute of Standards and Technology (NIST) published The Cybersecurity Framework in February 2014. In January this year, (NIST) issued a draft update to the Framework with new details on managing cyber supply chain risks, clarifying key terms, and introducing measurement methods for cybersecurity, the updated Framework aims to further develop NIST’s voluntary guidance to organizations on reducing cybersecurity risks.

The SEC has recently voiced its support of the Framework for Improving Critical Infrastructure Cybersecurity released by NIST and has indicated that as part of fulfilling their risk oversight function, boards should at a minimum work with management to ensure that corporate policies are in line with the Framework’s guidelines.

Dodd-Frank Act: The Dodd–Frank Wall Street Reform and Consumer Protection Act was signed into federal law on July 21, 2010. Among other things, Dodd-Frank requires bank holding companies with total assets of $10 billion or more, and certain other non-bank financial companies as well, to have a separate risk committee. That committee must include at least one risk management expert with experience managing risk of large companies.

Federal Trade Commission: The Federal Trade Commission Act prohibits “unfair or deceptive acts or practices in or affecting commerce.” 15 U.S.C. § 45(a). Since 2005, the Federal Trade Commission used this provision to bring actions against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers. An August 24, 2015 decision in Federal Trade Commission v. Wyndham Worldwide et al., 799 F.3d 236 (3d Cir. 2015), confirmed that certain data security practices could be considered “unfair” under § 45(a) and that the FTC’s “unfairness” authority my encompass cyber insecurity.
Financial Services Regulators: On Wednesday, October 19, 2016, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC) and the Federal Reserve Board (FRB) (collectively, the “Bank Regulators”) jointly announced proposed rules to enhanced cyber risk management standards for financial institutions that would apply to large and interconnected entities under the agencies’ supervision. These standards may impact business well beyond financial institutions since the proposals may apply, to some extent, to their vendors, too. Among the prescriptive elements of the proposed rules:

- The board must have deep knowledge in cybersecurity or direct access to external expertise.
- Certain risk functions, including cyber risk professionals, must have direct and independent reporting lines to the board.
- A detailed, board-approved cyber risk management strategy. Board-approved cyber risk appetite and tolerances, which cover external and internal risks, which explicitly aim, over time, to reduce aggregate institutional and sector-wide cyber risk.


“(1.) Disclosure requirements may impose an obligation on registrants to disclose [cybersecurity] risks and incidents.

(2.) Material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.”

The guidance also advised that appropriate disclosures may include:

- Business and Operations Risk: Discussion of aspects of the registrant’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- Outsource Risk: To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Historic, Material Cyber Incidents: Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Undetected Incident Risk: Risks related to cyber incidents that may remain undetected for an extended period; and
- Insurance: Description of relevant insurance coverage.

Test Case — SEC Disclosure Requirements
SEC disclosure requirements are at the heart of a reported SEC investigation of a global internet information company that suffered two massive data breaches, and the timing of its disclosures of those breaches. The results could become a watershed event.

Background: Since the SEC’s guidance in 2011, D&O risk experts watched for signs that the SEC or plaintiffs’ bar would use it as a springboard for a new wave of class action litigation. However, those concerns fizzled as securities lawyers worked their wording magic and effectively took the wind out of the class action sails. An SEC investigation into cybersecurity disclosures is also not new. The SEC has investigated multiple companies over whether they properly disclosed breach events. Those investigations include headline-making security breaches like those of a large retailer that suffered multiple breaches that compromised hundreds of millions of credit and debit card accounts.

Why this one is different: A two-year delay between the breach and its disclosure seems on its face very concerning. That the issuer’s core business was being acquired for $4.83 billion during that delay, and that the disclosure of the cybersecurity events led to a $350 million decrease in the purchase price gives us ample reason to be concerned that the SEC could take game-changing action.

But what will the SEC do? Too soon to tell, but any SEC action could provide a basis for the plaintiffs’ bar to successfully pursue cybersecurity-based securities class actions.

Cyber disclosure-based class action: At least one law firm has not waited. A securities class action has been filed against the company, together with its CEO and CFO, alleging that during the class period, the company made false and misleading statements over multiple quarters. The defendants are alleged to have failed to disclose that hackers had stolen information in two distinct incidents, over two years, involving more than 500 million and one billion accounts, respectively. Plaintiffs are seeking recovery based upon Securities Exchange Act Section 10(b), 15 U.S.C. § 78j(b), and SEC Rule 10b-5, and for control person liability under Exchange Act Section 20(a).

SEC Proxy Rule: Effective February 28, 2010, the SEC’s Proxy Disclosure Enhancements final rule went into effect. The rule addressed, among other things, the board’s role in risk oversight. Intended to promote greater accountability and enhance information available to shareholders, with respect to risk, the rule provides,

“Risk: by requiring disclosure about the board’s role in risk oversight and, to the extent that risks arising from a company’s compensation policies and practices are reasonably likely to have a material adverse effect on the company, disclosure about such policies and practices as they relate to risk management;”
State laws and regulations

NY-DFS, Cybersecurity Requirements For Financial Services Companies: Effective March 1, 2017, DFS now requires banks, insurance companies, and other financial services institutions regulated by DFS to establish and maintain a cybersecurity program. This new regulation sets minimum standards, requires, among other things, a risk assessment, disclosures, training and monitoring, and the encryption of nonpublic information.

Beginning February 15, 2018, covered entities must annually prepare and submit a Certification of Compliance to the superintendent. Essentially, that certificate requires the chairperson of the board or a senior officer to certify:

(1) The relevant directors or officers have reviewed the required documents, reports, certifications and opinions; and

(2) To the best of the directors’ or officers’ knowledge, the company’s cybersecurity program complies with the regulation.

Signed by the Chairperson of the Board of Directors or Senior Officer(s).

In the event of a data breach, the DFS or plaintiffs may argue that the certifying officer made deliberate or inadvertent misrepresentations in the certification.

International Organization for Standardization (ISO)

The International Organization for Standardization (ISO), an independent, non-governmental international organization, published its own information security standard known as the ISO/IEC 27001, which provides another framework for cybersecurity implementation.

D&O insurance coverage

With the exception of D&O policies that have an explicit cyber exclusion, public company forms generally handle cyber-related D&O claims as well as they handle other D&O claims. Claims for breaches of fiduciary duty, whether direct or derivative, would generally fall within the scope of typical D&O coverage. Likewise, private company D&O forms largely handle claims for breach of fiduciary duty well absent a specific exclusion. To the extent a D&O claim is based upon public company disclosure claims (including securities class actions) and/or merger objection claims (somehow tied to cyber insecurity), today’s D&O policies would generally work as expected for claims of this type. Nevertheless, there are a few things to consider about cyber insecurity that differentiates that risk from others.

First-party loss: Except for certain costs of responding to an investigation, the cost of defense, and any covered crisis management costs, the typical D&O policy provides coverage for liability for third-party loss. It is not designed to cover first-party loss resulting from a cyber event — no coverage for forensics work, loss of data, damaged hardware or other property, or business interruption. That coverage may be available under a typical cyber insurance policy.

Terrorism exclusion: Cyber claims may be the result of hacktivists, government and/or quasi-government actors. If so, a war or terrorism exclusion that fails to explicitly carve out cyber-based events could be triggered and restrict coverage.

Privacy exclusion: Some carriers may assert that any invasion of privacy exclusionary wording in their policies (if they have that exclusion) excludes certain cyber claims — direct or indirect. Even if the carrier has added a limited cyber carve-back, there may be limited coverage. If not sufficiently broad, the carve-back may actually strengthen the exclusion. Simply by adding the carve-back, the carrier has a stronger argument that the privacy exclusion was intended to exclude some cyber loss. The take away: Make sure any carve-back is broad enough to not limit coverage you would expect under a D&O form, particularly for the individual D&Os.

Cyber exclusions: Although not yet commonplace, some carriers require a cyber exclusion for private companies. They do so because of the open-ended, broad form entity coverage that is typically part of a private company’s D&O coverage. If your policy has such an exclusion, make sure it does not interfere with the traditional role of your D&O insurance.

Conclusion

With cyber insecurity risk and cybersecurity regulation so dynamic, directors and officers should keep a close eye on their increased risks. Regulations like the Enhanced Cyber Risk Management Standards and the DFS Cybersecurity Requirements For Financial Services Companies are prescriptive and could result in heightened risks for directors and officers, whether from enforcement or any civil liability for not preventing a serious breach. A professionally placed D&O policy should respond well in case you are faced with cyber-related claims or investigations, but, until our collective cyber insecurity subsides dramatically, we recommend a copious review of your policy to make sure it is optimized to avoid unforeseen gaps in coverage.
Fee litigation plague spreads to universities and mid-market companies

By Alison Miller (Atlantic Regional Leader, FINEX Claims, Radnor)

ERISA fee litigation shows no sign of slowing down. First brought over a decade ago, more than 75 fee cases have been filed, and more than 30 are pending today. In recent years, exponential expansion reflects the revolution from a one-firm cottage industry to, through its success, a multi-plaintiffs firm industry.

Until recently, targets were typically fiduciaries of large company-sponsored 401(k) retirement plans over $1B. Today, plaintiffs’ firms are casting a wider net. They are going smaller and broader.

- Smaller 401(k) plans, in at least one case as small as $9M in assets, are being targeted, too. That makes this threat real to a much broader set of sponsors, plans and fiduciaries.
- A wave of university-sponsored 403(b) plan fee suits almost instantly changed the risk profiles of large not-for-profit organizations.

Types of excessive fee cases

Fee cases fall into three categories.

1. Nonproprietary fund claims: Corporate plan sponsors and third-party plan service providers (including fund advisors).
2. Proprietary fund claims: Arise from fees or other compensation paid by financial institution-sponsored plans to their proprietary funds.
3. University-sponsored 403(b) plan claims: Pursue recovery from universities based on the same types of arguments that are made against private companies (such as an unreasonable structure or fee, unreasonable investment options, failure to monitor co-fiduciaries).

Among the newer “creative” allegations are that plan fiduciaries:

- Should have offered a stable value fund (while other cases allege that a stable value fund should not have been offered!)
- Should not have included unusual asset classes, either in core line-up or as a component in the target date retirement funds
- Failed to follow the plan document rules or to implement participants’ transactions correctly

Recent excessive fee case settlements

Excessive fee cases have been the subject of some very large settlements. As outlined below, the settlements in the last three years have varied greatly:

<table>
<thead>
<tr>
<th>Industry</th>
<th>Settlement</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aerospace</td>
<td>$62 million</td>
<td>July 2015</td>
</tr>
<tr>
<td>Aerospace</td>
<td>$57 million</td>
<td>August 2015</td>
</tr>
<tr>
<td>Health care</td>
<td>$32 million</td>
<td>November 2015</td>
</tr>
<tr>
<td>Insurance</td>
<td>$30.9 million</td>
<td>June 2016</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>$30 million</td>
<td>January 2014</td>
</tr>
<tr>
<td>Financial services</td>
<td>$27 million</td>
<td>July 2015</td>
</tr>
<tr>
<td>Financial services</td>
<td>$12 million</td>
<td>October 2014</td>
</tr>
<tr>
<td>Financial services</td>
<td>$3.8 million</td>
<td>June 2016</td>
</tr>
</tbody>
</table>

In addition to the millions listed above, settling defendants also agreed to non-monetary consideration — including prohibited investments and requiring marketing services to the plan.
Availability of insurance coverage

Plans and fiduciaries that purchase fiduciary liability insurance coverage with language vetted by trusted professionals should find that the claims asserted largely fall into the coverage afforded by today’s offerings. Limits adequacy has become a greater concern as the fee cases have settled for in excess of $60M, and defense expenses could exceed another $10M. For universities, it has been harder to find coverage on renewal. Large 403(b) plans and their sponsors should expect more scrutiny and potentially higher premiums at renewal this year.

Naturally, there remain traps and gaps for the unwary fiduciary insurance buyer. Coverage defenses frequently raised by carriers include:

- Covered “loss” does not include fines, taxes, penalties, fees and uninsurable matters (including disgorgement).
- Criminal/ fraudulent acts, illegal profit or advantage may be excluded upon a final adjudication of the underlying action.
- Contractual liability and benefits due exclusions. This risk may be heightened due to the Department of Labor’s new Fiduciary rule and its Best-Interest-Contract exemption, but it can be mitigated at placement with an endorsement.
- Third-party indemnification obligations, like those owed to a co-fiduciary, may mean that the sponsor or plan has a duty to indemnify defense costs and/or settlement contributions of others that will not fall within insurance coverage. Ironically, insurance may respond better with no co-fiduciary even if having the co-fiduciary improves the overall risk profile of the plan and its fiduciaries.

Given the threat, now is a good time for businesses of all sizes to discuss their fiduciary coverage with a trusted broker and their lawyer to make sure the policy will perform as intended and to confirm that limits purchased are adequate for the heightened risks.

Managing the risk of excessive fee litigation

In addition to risk transfer, sponsors, plans and fiduciaries can mitigate the risk of excessive fee litigation through process diligence, internal testing, external compliance audits and the following:

- Closely monitoring third-party plan service providers by preparing and putting out to the marketplace a comprehensive request for proposals no less frequently than every two years. Many of our clients review investment options quarterly.
- Develop and monitor written procedures for evaluating third-party plan service providers.
- Form a competent and qualified 401(k) committee (or other fiduciary) to be entrusted with the decision-making authority as it relates to the plan. Consider co-fiduciary services.
- In the case of proprietary funds offered to employees, close attention should be paid to the selection of the investment options. Could engaging a third-party plan service provider help mitigate risk?

While these suggestions cannot protect against the filing of a suit or the consequences of an IRS or DOL audit, they likely help reduce the likelihood of getting sued, bolster defenses and potentially mitigate severity.
Will emissions disclosures remain a hot D&O risk?

By Kristin M. Zieser (FINEX Claims, New York)

While it might seem, with the new administration in Washington, that last year’s alarming emissions disclosure-related enforcement and litigation activity may no longer be an emerging concern for directors and officers, it may be a bit too early to relax.

2016 developments in emissions regulation, enforcement and litigation may nevertheless suggest the potential for a new sector of liability for businesses and their leaders. What remains unclear is not just to what extent the new administration’s environmental policies will alleviate corporate concerns, but also, which regulators (state, foreign) may fill any regulatory gap, and whether civil plaintiffs may pick up any regulatory slack or whether, without federal pre-emption, emissions becomes free-for-all. Last year’s developments have effectively provided a road map for the emissions focused. It may not matter if the new administration drives – someone likely will. The genie is out of the bottle.

Oil firm (SEC and NYS attorney general)

The Securities and Exchange Commission (SEC) recognized the potential financial impact of climate change when it issued their Interpretive Guidance of Climate Disclosure in February of 2010. The February 2010 Guidance cautioned public companies to be aware that the legal, technological, political and scientific developments concerning climate change may create new risks, and to take into account, for disclosure purposes, any direct or indirect consequences climate change may have on their businesses. An example of an emissions-related disclosure by a well-known car manufacturer:

“We are subject to extensive laws, governmental regulations and policies, including those regarding . . . emissions controls, which can significantly increase our costs and affect how we do business. . . . Meeting or exceeding many of these regulations is costly and often technologically challenging, especially where standards may not be harmonized across jurisdictions, a significant challenge with respect to mandated emissions and fuel economy standards. We anticipate that the number and extent of these regulations, and the related costs and changes to our product portfolio, may increase significantly in the future. These government regulatory requirements could significantly affect our plans for global product development and given the uncertainty surrounding enforcement and regulatory definitions, may result in substantial costs, including civil or criminal penalties.

In addition, an evolving but un-harmonized regulatory framework may limit or dictate the types of vehicles we sell and where we sell them, which can affect revenue.”

While the potential for regulatory action relating to climate change reporting liability has been a possibility for years, it seemed not to have been an SEC priority until 2016.

On September 20, 2016, The Wall Street Journal reported, in [here, subscription required] that a large oil firm was being investigated for its accounting around write-down values and future costs of complying with regulations to curb greenhouse gases. Nearly a year earlier, the New York Times reported that the same oil firm was being investigated for “possible climate change lies” by New York’s Attorney General, Eric T. Schneiderman. On September 16, The Wall Street Journal reported that [here, subscription required] the New York AG expanded its investigation to include the oil firm’s practice of not writing down the value of its oil and gas reserves when prices decline.

Truck engine manufacturer (SEC and securities litigation)

A truck manufacturer paid $9.1M to settle a securities class action alleging the manufacturer made false and misleading claims about the development of a reduced emissions engine. The SEC’s enforcement action against the manufacturer’s former chief executive officer is pending in federal court in Illinois. The manufacturer itself settled with the SEC in 2016 – agreeing to pay $7.5M to settle charges.

Automobile manufacturer (EPA, SEC, FBI, DOJ and foreign regulators, U.S. securities class action, Dutch collective action)

The automotive industry has also been in the spotlight lately for scandals dealing with emissions reporting on their vehicles. In September 2015, the EPA hit a major automotive manufacturer with a notice of violations of the Clean Air Act. The EPA claimed the auto manufacturer intentionally programmed turbocharge direct injection to activate certain emissions controls only during laboratory testing. The company recently pleaded guilty to these charges and agreed to pay $4.8B in criminal and civil fines. U.S. authorities indicted six of the company’s executives on a variety or charges. The FBI even arrested one of the company’s compliance officers in early 2017 for allegedly lying to investigators. A U.S. securities class action, a Dutch collective action and a German template case has been approved under the German Markets Model Case Act. An environmental mess!

Similar troubles: An all-American motorcycle producer faced a similar fate, paying $12M to resolve claims by the EPA of emissions cheating. On the other side of the Atlantic, French regulators looked into whether or not one of that country’s largest automobile manufacturers attempted to
game emissions standards, while another auto manufacturer is currently facing claims that they took advantage of a consumer’s desire to make environmentally friendly choices, and saw this as an opportunity to charge premium prices.

**Broader regulatory views**

*NAIC:* The SEC, NYAG, and environmental activists are not the only ones concerned with climate change disclosures. The NAIC (National Association of Insurance Commissioners) also views climate change disclosures a main concern. According to a study by Munich Re, extreme weather events resulted in $560B in insured losses from 1980 to 2015. With this uptick, it is imperative insurers and risk managers identify these factors and weigh how they will impact their businesses.

Companies in the energy, manufacturing and insurance sectors are not the only ones facing regulatory scrutiny. Of course, in this new age of individual accountability, companies are not the only targets of regulators’ wrath.

**Activists**

What’s more, shareholders — activist investors, to be exact — are getting in on the actions as well. Another oil firm, for example, is facing pressure from an activist shareholder group looking to protect the company’s business from climate change regulations worldwide. Essentially, the activists seek to force diversification of the company’s business to protect its bottom line from changing regulations. Perhaps in response, last fall the company’s CEO responded that 10% of executive bonus payments will be linked to greenhouse gas management starting this year.

**The new administration**

So, how might the new administration affect emissions disclosure risk?

Seems our current president questions whether global warming was even real. This month, the President announced the U.S.’s intention to pull out of the Paris climate agreement which he asserts is unfair to the United States. The Paris Agreement, adopted by 190 countries in December 2015, came into effect on November 4, 2016. The agreement aims to limit global warming to well under two degrees Celsius. The President has indicated a willingness to renegotiate the accord in a way that does not put the U.S. at an economic disadvantage.

**Conclusion**

Despite this political uncertainty, it may be too late. Public opinion, investor preferences and regulatory oversight may already be far enough down the road to seriously — or permanently — reverse course. There are too many stakeholders and regulators. Foreign governments, such as China, have set ambitious renewable and climate change goals. These stakeholders will likely continue to push climate change and environmental concerns.

The main takeaway here is that uncertainty breeds risk. Under these conditions, our advice is to be proactive and seek professional guidance to weather the storm. Use your resources. Use your attorneys. Use your peers. And use your trusted brokers.

- **Use your attorneys for guidance.** Your attorneys should be well versed in the 2010 Interpretive Release. Have them guide you through the SEC’s disclosure requirements to ensure you are following them.
- **Use your peers for a gauge.** Companies were targeted mainly because they were not doing something that everyone else in their industry was doing.
- **Use your brokers for coverage.** Let your broker check up on your directors & officers insurance to ensure you are properly prepared for such an exposure.

As to coverage, directors and officers should continue to make sure that their D&O insurance — especially their Side-A insurance — does not have a pollution exclusion that can result in coverage gaps or traps when they need their coverage most.
This document is a general guide to the issues presented. It doesn't provide any legal advice, and no attorney-client relationship is created through this document. Consult with a licensed attorney to obtain legal advice regarding any specific issues.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.