Insurance for Cyber, Social Engineering, and Professional Liability Risks

Dale L. Kingman
Gordon Tilden Thomas & Cordell LLP
600 University Street, Suite 2915
Seattle, WA 98101
(206) 467-6477
dkingman@gordontilden.com

Haley K. Krug
Andersen Schwartzman Woodard Brailsford PLLC
101 S. Capitol Boulevard, Suite 1600
Boise, ID 83702
(208) 342-4411
HKK@aswblaw.com

The Seminar Group
Portland, Oregon
October 25-26, 2018
DATA BREACH, CYBER LIABILITY AND SOCIAL ENGINEERING FRAUD

I. INTRODUCTION

The purpose of this section of the paper and presentation is to provide a broad overview of insurance coverage for cyber risks/liability and social engineering fraud. It is intended to acquaint the reader with the current state of the insurance marketplace and the response of insurers and courts to claims for coverage under both liability and property insurance policies. Cyber risks have been around for 10 to 15 years and seem to be on a geometric pace of expansion as economies become more dependent on electronically created and stored data.

More recently, businesses have been the subject of what has been characterized as “social engineering fraud.” This is a species of fraud that occurs when a criminal impersonates a legitimate customer, client, vendor, or other business, and deceives an employee, usually an accounts receivable or payable employee, into transferring to the imposter’s account legitimately owed funds due a legitimate business. The artifice is accomplished usually through use of a computer, by email, sometimes by hacking into an insured’s computer system, and through which payment instructions are changed either by an employee or through hacking. Monies otherwise due legitimate businesses or customers are then sent to bank accounts which almost immediately are emptied, with the stolen funds transferred, generally overseas. These particular activities are often characterized as “phishing,” spear-phishing, social engineering, pre-texting, or diversion. They are all accomplished via email, text, instant message, social media related communication, or any other electronic, telegraphic, telephone, or written instruction, all of which is designed to fool an employee into sending funds to criminals.

A. What Are Cyber Risks?

1. Definitions and Examples

Cyber risk, cyber-attack, data breach, data leak, data spill: All of these terms describe a fluid, somewhat amorphous and ever evolving area of “cyber risk.” A cyber-attack, for example, is any affirmative or offensive attack deployed by individuals or organizations, and targeting computer information systems, computer networks and/or personal computer devices through the employment of malicious attacks, designed to steal, alter or destroy data and information. A data breach, on the other hand, is an intentional or accidental release of otherwise sensitive or confidential data into a broader unsecured environment. A data breach may involve sensitive or confidential information such as client records, intellectual property, financial records; for individuals, the most common breach involves stolen “Personally Identifiable Information” (PII) or “Personal Health Information” (PHI) such as medical records.

A recent study by the Ponemon Institute, found the leading causes of cyber-attacks in the healthcare industry are criminal in nature and are the leading cause of data breaches. According to the Ponemon Institute, data breaches cost the healthcare industry $6 billion annually. In 2018,
the Ponemon Institute provided updated causes and figures. The causes of cyber breaches were malicious or criminal attack (48%), human error (27%), and system “glitch” (25%).

Ponemon estimates, as of 2018, a breach of one million records yields an average total cost of $40 million, and a breach of 50 million records yields an average total cost of $350 million. By way of example, the cyber-attack against Anthem, Inc. in 2015 resulted in 80 million records being hacked; of myHeritage in 2018 yielded 92 million hacked records; Ebay, in 2014, 145 million records were hacked; Equifax in 2017, 143 million records were lost through poor security; and astonishingly, three billion records were hacked at Yahoo in 2013, and another 500 million in 2014.

Other sectors that have experienced data breaches and cyber-attacks include the retail sector and industries relating to entertainment, finance, and insurance. The legal sector has not been immune and, of course, all levels of government have been subjected to both breaches and attacks. The list of businesses, institutions, and governments that have suffered data breaches through criminal conduct, system failures, or human error is impressive and growing.

2. Information at Risk

As the foregoing targets demonstrate, there is no “safe information.” The type of information at risk includes consumer information consisting of credit cards, payment information, social security numbers, tax payer records, customer transaction information, personally identifiable information such as driver’s licenses or passports, financial information, account balances and bank numbers, email addresses, phone lists, and telephone numbers.

Employers have a vast store of information about their employees, and the larger the employer, the more information is at risk. In connection with businesses, not only is the business itself at risk, but its business partners.

---

3 2018 Cost of a Data Breach Study: Global Overview (Ponemon Institute LLC and IBM, July 2018).
4 Listed Data Breaches (Wikipedia, Sept. 11, 2018).
5 Home Depot (2014), 56 million customer records stolen; Target (2013), approximately 40 million credit and debit card accounts stolen; Subway, 146,000 accounts.
6 Sony Pictures (2014), thousands of employee personnel records, emails, etc., leaked online; PlayStation Network (2011), thousands of stolen credentials; Ashley Madison (2015), 37 million user files stolen.
7 J.P. Morgan Chase (2014), 76 million records, PII, stolen; VISA/Mastercard (2012), over 10 million credit cards stolen; Heartland Payment Systems (2009), up to 100 million credit card information from more than 650 financial companies compromised.
8 AIG (2014), almost 800,000 customers’ financial information stolen by former financial advisor.
9 “Panama Papers” scandal involving Mossick Fonseca. Other financial firms which have been hacked include Wiley Rein, LLP, McKenna Long & Aldridge, merged with Dentons in 2015, and more recently Cravath, Swaine & Moore and Weil, Gotshal & Manges. Law.com, March 30, 2016 article, “Cravath Admits Breach as Law Firm Hacks to Public.”
10 IRS (2014), Office of Personnel Management, 4 million current and former federal employee records stolen (June 2015); Office of Homeland Security, 30,000 records in 2016; various Departments of the U.S. government (Army, Defense, Veterans Affairs) and several state governments (Texas, Ohio, Massachusetts, Washington State, to name but a few).
Intellectual property, trade secrets, and confidential business information are all targets of hackers and data breaches. More recently, law firms servicing Wall Street have been seen as also lucrative targets for hackers playing the IPO game. It is enough to say that any PII or PHI is at risk given the pervasive nature of the internet and electronic storage of information.

3. **Threat Environment**

The threat environment encompasses accidental and intentional hacks and breaches as well as internal and external causes.

The intentional threats come from criminal activity which, as noted above, is pervasive in the healthcare industry. Criminal attacks usually involve PII seeking credit or debit card information and intellectual property, items that can be sold. Other intentional activities are either terrorist or state-sponsored, and designed to create uncertainty, and impose economic hardship, property damage, and loss of life. Ideological activism also provides a source of intentional and often criminal activity.

Accidental data breaches, however, can occur with great frequency and include lost or misplaced devices, inadvertent publication of data, carelessness by vendors, or independent contractors over whom a party may have no control.

In practical terms, while there may be a difference in motive, there is very little difference in outcome: the publication and dispersal of information a party does not want released.

**B. Costs and Loss Items**

The costs of a data breach or cyber-attack are significant. These costs may include legal liability such as defense and settlement costs, regulatory investigations resulting in additional defense costs and imposition of financial penalties, the cost to repair or replace data that has been stolen, corrupted or destroyed as well as software that is corrupted, destroyed, or in need of a complete remediation.

Response costs incurred in connection with investigation of both the breach and remediation, legal costs, notices to customers, credit card and credit monitoring, and public relations are all costs imposed on the party that has suffered the breach or attack.

Bottom line: everybody is a target, nothing is safe, and any assumption to the contrary is a fool’s errand.

**II. CYBER LIABILITY COVERAGE UNDER COMMON INSURANCE PRODUCTS**

**A. Introduction**

There are a variety of insurance products commonly obtained by businesses that may respond to cyber liability. Whether any of these insurance products will respond to cyber liability depends on both the threat environment and information at risk. For example, whether the threat
environment is accidental or intentional, is the information at risk PII or PHI that is either leaked or disseminated to third parties? Is the threat environment a cyber-attack in which the intention is to disable operating systems or corrupt information?\textsuperscript{11}

In today’s environment, businesses have a responsibility to their customers and clients to ensure the safety and confidentiality of information they receive and store. A failure to do so, with the attendant economic costs and liability imposed on the company, may result in the officers and directors of the company being exposed to secondary liability. Will directors and officers insurance respond?

Law firms and other professional service organizations who possess confidential and proprietary information, or who are involved in IPOs or security placements, also risk exposure to hackers who, in turn, either sell or use the information to “game” the market or a competitor. Will these professional service organization’s errors and omissions coverage provide liability cover?

Computer software and processing systems can be corrupted and, as has been seen, the corruption or manipulation of operating systems can result in property damage. Is it possible that an “all risk” policy will provide property insurance coverage?

In this section, we will explore, generally, the applicability of the most common insurance products to cyber liability and cyber risks. The section that follows will outline current insurance products that are or may be available in the marketplace, and specifically, developed for cyber risks.

B. Standing Necessary to Trigger Liability Exposure

Before a liability policy is exposed to any risk of indemnity, the claims brought against a company subject to a cyber-attack or data breach may be required to be filtered through the principle of “standing.”

In the federal system where many cyber risk cases are either filed or end up (because of diversity or federal question), standing takes on increased importance because of the limitation of federal court jurisdiction to actual “cases or controversies.”\textsuperscript{12}

“Standing” is the concept employed to ensure the requirements of “case or controversy” is met. To establishing standing, an injury must be “concrete, particularized, and actual or imminent;

\textsuperscript{11} For example, Stuxnet, a computer worm employed as a cyber weapon; a 2014 cyber-attack on a Thyssen Krupp steel mill that prevented a blast furnace from shutting down resulting in significant physical damage. Emerging Cyber Risk: Cyber-Attacks and Property Damage—Will Insurance Respond? \textit{JLT Specialty Ins. Services, Inc.} monograph.

\textsuperscript{12} U.S.C.A. Constitutional Article 3, § 2, Cl. 1; \textit{Clapper v. Amnesty Int’l USA}, 133 S. Ct. 1138, 185 L.Ed.2d. 264 (2013) (dismissing claim against United States alleging unconstitutionality of Foreign Intelligence Surveillance Act because plaintiffs failed to demonstrate sufficient injury).
fairly traceable to the challenged action, and re-dressable by a favorable ruling.”

Allegation of possible future injury is not sufficient to confer standing on a claimant.

Cyber-attacks and the potential dissemination or exposure of information coalescing in a class action lawsuits present difficult issues of standing. Claimants must allege more than increased risk of identity theft or a mere loss of data without any evidence of actual injury.

The seminal case on liability for a data breach is the Supreme Court case of *Clapper v. Amnesty International U.S.A.* supra, n.12. In the post-*Clapper* world, allegations of future harm are not sufficient to confer standing; allegations of actual harm are required.

To the extent a claimant passes the standing test, what policy coverages are available?

C. Coverage Under Commercial General Liability Insurance

The potential coverage under a Commercial General Liability (“CGL”) policy is twofold depending on the threat environment. A CGL policy will be triggered if a claimant suffers “property damage” or an “offense” listed in the “Personal and Advertising Injury Liability Coverage,” as those terms are defined in the policy.

Under Coverage A, “property damage” is defined as “physical injury to tangible property, including all resulting loss of use of that property or loss of use of tangible property that is not

---

14 *Clapper*, 133 S. Ct. at 1147 (citing, inter alia, *Whitmore v. Arkansas*, 495 U.S. 158, 110 S. Ct. 1717 (1990) (death row inmate did not have standing to challenge validity of other death row inmate’s death sentence)).  
15 See, e.g., *In Re Barnes & Noble Pinpad Litig.*, 2013 WL 4759588 (N.D. Ill. 2013) (claim against Barnes and Noble for failing to prevent “skimming” of customer financial information insufficient to establish standing due to lack of cognizable injury).  
17 *Krottner v. Starbucks Corp.*, 628 F. 3d 1139 (9th Cir. 2010) (employees’ allegation that theft of laptop subjected them to increased risk of future identity theft was sufficient to establish injury in fact); *Remijas v. Neiman Marcus Group*, 794 F. 3d 688 (7th Cir. 2015) (department store credit card owners showed actual fraudulent activity as a result of data theft able to establish injury in fact); *In Re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014) (software licensees whose personal information was actually compromised as result of online data breach showed sufficient injury in fact to establish Article III standing); *Enslin v. The Coca-Cola Co.*, 2015 WL 5729241 (E.D. Pa. 2015) (theft of money from employee’s bank account and fraudulent credit cards opened sufficient to establish injury in fact for Article III standing); *Lewert v. P.F. Chang’s China Bistro, Inc.*, 14-CV-4787, 2014 WL 7005097 (N.D. Ill. Dec. 10, 2014) rev’d and remanded, 14-3700, 2016 WL 1459226 (7th Cir. Apr. 14, 2016) (time and expense incurred by representative to prevent fraudulent charges was sufficiently concrete to establish injury in fact); *Corona v. Sony Pictures Entm’t*, 2015 WL 3916744 (C.D. Cal. 2015) (allegations that private data has been traded on black market website sufficient to establish injury in fact); *In Re Anthem, Inc. Data Breach Litig.*, 2016 WL 589760 (N.D. Cal., Feb. 14, 2016) (a mixed ruling) (breach of data insufficient to establish injury for purposes of Indiana state law).
physically injured . . . .” Current CGL policies also add that “for purposes of this insurance, electronic data is not tangible property.”

Earlier versions of the CGL policy, some of which may be in circulation today or used or not updated by certain insurers do not include the definition of “electronic data” excerpted in n.18, nor state that “electronic data” is not “tangible property.”

Within Coverage B of the CGL policy, “Personal and Advertising Injury,” certain offenses are covered; for our purposes, the most important being “oral or written publication, in any manner, of material that violates a person’s right of privacy.”

1. **Property Damage**

Absent the electronic data provision noted above, damage to software or loss of data can and has been treated as “property damage.” The cases are rare however, as the majority of courts have held data to be “intangible property,” and not “tangible property” within the meaning of the term “property damage.” There appears to be a better likelihood of success under the second prong of the “property damage” definition: “loss of use of tangible property.”

Although cases are few, coverage for “loss of use of tangible property” has resulted in rulings favorable to insureds. *Eyeblaster, Inc. v. Federal Ins. Co., infra, n.19*, is an example. In *Eyeblaster*, a computer user sued Eyeblaster claiming his computer, software, and data were injured or destroyed after accessing Eyeblaster’s website. The court held the computer, alleged to have been rendered useless, was tangible property and therefore triggered the “loss of use” part of the definition of property damage.

Coverage will be limited under a CGL policy. With the definition of “tangible property” narrowed to exclude any type of electronic information, data, etc., triggering a CGL policy for a cyber loss will be difficult in the future. In addition, many insurers are including specific exclusionary language in endorsements to make clear that the CGL policy will not cover any of the myriad potential claims arising out of a cyber risk.

2. **Personal and Advertising Injury Liability**

The current litigation regarding the offense of “oral or written publication of material that violates a person’s right of privacy” is over the meaning of the term “publication.” The most recent discussion of “publication” in the context of a CGL policy is the Fourth Circuit case, *Travelers*

---

18 Electronic data is defined to mean “information, facts or programs stored as or on, created or used on, or transmitted to or from computer hardware, including systems and applications software, hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices, or any other media which are used with electronically controlled equipment.” ISO Form CG 00 01 04 13, § V.17.
20 The definition of “tangible property” excluded any “software, data, or other information that is in electronic form.” In *Eyeblaster*, the court held that tangible property included computers, and the claimant alleged “loss of use” of his computer as distinguished from software, data or other information.
**Indemnity Co. of America v. Portal Healthcare Solutions, LLC**, 2016 WL 1399517 (4th Cir. Apr. 11, 2016). *Portal* involved a class action filed by two individuals alleging that Portal and others engaged in conduct resulting in the plaintiff’s medical records being on the internet. Travelers sued for a declaratory judgment it had no duty to defend Portal, maintaining the Complaint failed to allege a “covered publication by Portal.” *Id.* at *1.

The Circuit Court, affirming the District Court, held the class action complaint potentially or arguably alleged a publication of private medical information in that the patient’s privacy could be viewed by any member of the public with an internet connection, satisfying the predicate for triggering at least the duty to defend. The District Court held that “publication occurs when information is ‘placed before the public,’ not when a member of the public reads the information placed before it.” 35 F. Supp. 3d 765, 771. Thus, the data breach and dissemination of the information is sufficient to trigger the personal advertising injury liability coverage and at least provide a defense.

On the other hand, a mere loss or theft of data with no indication anyone could access it, does not constitute “publication.”

If the CGL policy is to have any currency, absent a specific exclusion by endorsement of any cyber risk liability, the personal and advertising injury liability coverage B appears to be the most likely source of coverage.

**D. Directors & Officers Liability Coverage**

It takes no great leap of logic to deduce that corporate data breaches would spawn litigation against not just the corporation, but its officers and directors.

Claims against officers and directors arising out of data breaches or cyber liability target managerial conduct and thus potential “wrongful acts.” D&O policies are frequently tailored to a specific industry such as financial, securities, retail, manufacturing or commercial sectors. Nonetheless, the basic concept of a “wrongful act” is almost always included in the grant of coverage.

For example, in *First Bank of Delaware, Inc. v. Fidelity & Deposit Co. of Maryland*, Fidelity’s “D&O Select Plus Insurance Policy” was held to provide coverage under its Electronic

---


22 Indeed, in a number of cases cited earlier involving Target, Home Depot, and Sony Pictures, officers and directors were named as defendants in both derivative and class action litigation. *Kulla v. Steinhafel*, D. Minn. Civ. No. 14–203; *In Re Heartland Payment Sys., Inc. Securities Litig.*, 2009 WL 4798148 (D.N.J. 2009), in which the officers and directors were claimed to have made fraudulent statements in connection with investor calls.

Risk Liability section as a result of a credit card transaction company’s computer being hacked, resulting in losses of approximately $1.5 million.\textsuperscript{24}

E. Professional Liability Coverage

Errors & Omissions coverage is normally triggered for claims arising from “negligence, omissions, mistakes, and errors made by the insured in the course of providing professional services.” It is not too difficult to envision claims by clients, customers or customers’ competitors against legal professionals for a data breach resulting in the dissemination of confidential information or intellectual property. The question to be answered is often whether the law firm was negligent in how it maintained its computer’s security systems. The \textit{Panama Papers} case is a good example of an obvious failure on the part of a law firm resulting in the dissemination of millions of documents and the breach of confidentiality and privacy of thousands of individuals. In that case, Panama law firm Mossack Fonseca was hacked and 11.5 million internal legal and financial documents were leaked. The documents exposed the offshore tax shelters employed by a number of high-asset and high-influence individuals. Investigation revealed the hack was made possible by numerous unpatched vulnerabilities in Mossack’s website and e-mail server. Criminal and regulatory investigations followed, insurance disputes ensued, and ultimately, Mossack Fonseca closed its doors citing irremediable “reputational harm.”

While the \textit{Panama Papers} was large in scale and potential repercussions given the nature of the firm’s practice and the materials accessed, the basic patch failure that caused the breach could occur at most any firm. The vulnerability of client data in law firms presents both liability risks and ethical concerns. Many states are now addressing the vulnerability of client data via their rules of professional conduct. Under Rule 1.1 of the ABA Model Rule relating to lawyer competence, some states have added a new comment to make clear that an understanding of technology is an expected duty of every lawyer, “including the benefits and risks associated with relevant technology.” \textit{See} Utah Rule 1.1, comment 8.

In Washington, RPC 1.6 regarding confidentiality, comments 16 and 17, explicitly refer to inadvertent or unauthorized disclosure, including when transmitting information. Oregon Rule of Professional Conduct 1.6(c) similarly requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of or access to client information.

Cyber liability endorsements to professional liability policies are offered to law firms as well as to other professionals. The language of such endorsements must be examined closely to determine whether the coverage is adequately tailored to the risks the individual firm faces. Cyber liability coverages will be interpreted according to their terms and not always in a predictable manner given their relatively recent introduction.

In a recent case involving a medical liability policy that included a “cyber claims” endorsement, the court determined the endorsement’s coverage for “privacy wrongful act[s]” did not cover a cosmetic surgeon’s conduct in accessing customer information from a spa and texting

\textsuperscript{24} \textit{See also Bank of Rhode Island v. Progressive Cas. Ins. Co.}, 19 F. Supp. 3d 378 (D.R.I. 2014) (bank’s Directors & Officers policy responsible to cover claims for data breach and manipulation of electronic data by employee for that part of jury award not subject to “Internet Services Exclusion.”).
those people to advertise his services. The court reasoned the text messages did not involve “financial, credit, or medical information” as defined by the endorsement.\textsuperscript{25} Many common professional liability policy exclusions may also affect coverage for cyber losses, including exclusions for bodily injury and property damage that also reference “invasion of privacy” and exclusions for breach of contract.

\textbf{F. First Party Property Insurance}

1. \textit{“All Risk” Coverage}

An All Risk policy provides coverage for “physical loss or damage” caused by a “covered peril.” The predicate for coverage under an all risk policy is “physical loss or damage,” a concept not too far removed from “physical injury to tangible property” under CGL policies.

Many cases have held that a loss of data, regardless of how occasioned, did not trigger the insuring clause of an all risk policy.\textsuperscript{26}

On the other hand, a software company whose computers were hacked, and sustained data loss was an insured for the consequential income losses under a Business Interruption endorsement. The court held that “there was no question NMS suffered damage to its property, specifically, damage to the computers it owned.”\textsuperscript{27}

2. \textit{Commercial Crime Policies}

A species of first party coverage is the Commercial Crime policy. These policies are designed to protect against employee misconduct such as employment dishonesty, forgery, alteration or embezzlement. Inasmuch as a significant portion of data breaches occur as a result of employee misconduct, a review of Commercial Crime policies is warranted. However, because of numerous exclusions, it is doubtful that most traditional Commercial Crime policies issued in today’s marketplace will provide coverage.\textsuperscript{28}

However, insurers have, within the last few years, begun to provide an insurance product designed to insure against social engineering fraud. Usually this product is provided either as an add-on to a Crime policy or as an endorsement to the Crime policy.

3. \textit{Social Engineering Coverages}

Although policy wordings may differ in certain aspects, most insurers in today’s marketplace are offering coverage for “social engineering” risks as part of the Commercial Crime

\textsuperscript{25} \textit{Doctors Direct Ins., Inc. v. Bochenek}, 38 N.E.3d 116 (Ill. App. 2015).
\textsuperscript{27} \textit{NMS Services, Inc. v. The Hartford Ins. Co.}, 62 F. Appen. 511 (4th Cir. 2003); \textit{Lambrecht & Assoc. Inc. v. State Farm Lloyds}, 119 S.W.3d 16 (Tex. 2003) (in which coverage under a property policy was triggered specifically because the insured had an endorsement covering “electronic media and records,” a common All Risk coverage).
package. Usually, the coverages are added by endorsement and can be viewed as stand-alone coverage. These coverages are designed to cover “computer fraud,” “funds transfer fraud,” or “fraudulently induced transfers.” A typical coverage may be found in a policy issued by Chubb designed to coverage employee theft, forgery or alteration, theft of money and securities, both inside and outside the premises, and certain types of cyber fraud. For example, two particular coverages in a typical Chubb policy are for both “computer fraud” and “funds transfer fraud.”

The coverage for “Computer Fraud” is:

The Insurer will pay for loss of or damage to money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises: (a) to a person outside those premises; or (b) to a place outside those premises. (Emphasis supplied.)

Computer fraud coverage has traditionally been considered by the industry to be the result of “hacking” into a business’s computer and extracting information necessary to steal money or securities through the use of a computer. Recent case law has, however, failed to agree with the industry claim.

“Funds Transfer Fraud” is defined:

The Insurer will pay for loss of funds resulting directly from a fraudulent instruction directing a financial institution to transfer, pay, or deliver funds from the Company’s transfer account. (Emphasis supplied.)

In plain English, this means that an imposter, through a phishing expedition, creates a fraudulent instruction which, in turn, will lead an employee to direct a financial institution, i.e., bank, to transfer funds from the defrauded company’s account to that of a criminal third party.

Another formulation of coverage for “Computer Fraud” provides:

We will pay for loss resulting directly from the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of money, securities or other property from your premises or banking premises to a person, entity, place or account outside of your control.29 (Emphasis supplied.)

You will note the immediately preceding Great American formulation of computer fraud is different than that contained in the Chubb policy. Similarly, a Great American policy also provides, by endorsement, coverage for “Fraudulently Induced Transfers,” which are characterized

29 Great American Insurance Co., Crime Protection Policy (SP 00 01 (04/12)).
as transfers resulting from payment orders transmitted from the Insured to a financial institution made in good faith reliance on an electronic, etc., instruction from a person purporting to be an employee, customer, vendor, or owner, establishing or changing the method of such payment, and is transmitted by someone impersonating an employee, customer, vendor, or owner without the Insured’s knowledge or consent.

While the formulation in the Great American policy of a funds transfer fraud is somewhat different than that in the Chubb policy, both policies are designed to insure against fraudulent conduct in which a computer is employed to directly cause the fraudulent transfer of money from the Insured’s business to a criminal third party.

It is worth noting that because policy language employed by insurers often differs, the facts of a particular loss must be correlated with the policy language to determine whether there is coverage. This is not necessarily an easy task as the case law, which has developed over the last two to three years, has revealed.

4. **Case Law Under Social Engineering Coverages**

   a. **Recent Trends**

   Cyberattacks and data breaches which result in hacking of customer and client lists, personal information or PII, are usually designed to accumulate data which is then sold to criminal third parties who, in turn, hack into bank accounts, or engage in methods of identity theft to impersonate individuals with the goal of stealing money. Social engineering fraud is slightly different and results in a more direct access to money and securities. While imposters, deception, etc., is not new in the business world, the use of computers to conduct fraudulent activities on unsuspecting or ignorant employees is relatively recent. Hence, the creation of insurance products designed to provide some indemnity for these direct fraudulent thefts.

   The courts’ treatment of social engineering losses has been somewhat mixed over the last few years. As of September 2018, however, the trend appears to be a more nuanced look at the coverages available in conjunction with the particular fact patterns.


   Both cases involved the courts’ interpretations of “Computer Fraud” coverages under Federal’s and Travelers’ policies, respectively. The *Medidata* opinion affirmed the district court, finding coverage for Medidata under Federal’s Computer Fraud coverage provision, while the 6th Circuit in *American Tooling* reversed the Insurer victory in the district court which found no coverage under the Computer Fraud coverage provision.

   Both *Medidata* and *American Tooling* involved “spoofing” or “phishing” in which an imposter pretended to be, in one case an executive, and in the other, a vendor. In each case, funds, otherwise owed for legitimate purposes, were redirected to the imposter’s bank accounts. And, in
each case, the appellate courts had little trouble finding coverage under the respective policy’s Computer Fraud provisions.

One of the principle issues upon which Insurers have defended against coverage with their Computer Fraud coverage provisions has been whether the loss was “directly caused” by or a “direct result” of the use of a computer to effectuate the fraud. In earlier cases, the Insurers were more successful in arguing there were too many intermediate steps that needed to take place in order for funds to be fraudulently transferred, and hence the “direct” requirement was not met.

In earlier cases, some fact patterns of which were not unlike Medidata and American Tooling, the transfer was initiated with the receipt of a spoofed email or telephone call requesting changes in payment instructions. A clerk or an employee would then necessarily have to go into the Insured’s computer and change payment instructions, or contact a bank to change payment or wiring instructions. Courts held that as a result of these intermediate steps, there was no direct connection between the criminal’s use of a computer and the transfer of funds.

Both Medidata and American Tooling, however, rejected the analysis of the earlier cases, particularly a couple of cases in the Ninth Circuit. The Medidata and American Tooling courts had no trouble finding a direct nexus between the spoofed email or instruction and funds transfer. The fact human agency was required as an intermediate step between receipt of the email and transfer of the funds was sufficiently “direct” since no other step was necessary. Even in American Tooling where the employee sought the assistance and authority of her supervisors to send the funds, the transfer was not deemed to be anything less than direct.

b. Summary of Representative Social Engineering Cases


Imposter fraud in which imposter posed as vendor requesting change in bank information for vendor. Payment sent to criminal imposter. The District Court ruled for Apache, holding that, “Intervening steps of the [post-email] confirmation phone call and supervisory approval do not rise to the level of negating the e-mail as being a ‘substantial factor’.” Fifth Circuit reversed, holding that the email was “merely incidental” to the crime, and was not directly related to coverage under the policy.


Principle involved imposter changing payment instructions to Chinese bank via fraudulent e-mail. The District Court found “Computer and Funds Transfer Fraud” coverage to be ambiguous, finding for the policyholder. Even though there were intervening events between receipt of the email and payment of the funds, the District Court found these events were not sufficient to interrupt the “direct” relationship between the computer fraud and false payment.

The Ninth Circuit found for the Insurer under circumstances in which an accounting firm complied with an imposter’s fraudulent email instructions, upholding the District Court’s denial of coverage. In *Lieberman*, the Court interpreted the funds transfer/computer fraud coverages to be inapplicable, as was the coverage for “forgery or alteration of a financial instrument by a third party.” Essentially, the Court held the computer system had to be “hacked,” and that a fraudulent email was insufficient to trigger coverage.


The District Court held that the use of a computer was “incidental” to, and not directly related to financial loss of another social engineering fraud. Pestmaster employed a third party to collect and pay payroll taxes. The third party, rather than paying the IRS, paid itself through a fraudulent scheme. No coverage as no direct relationship. The Ninth Circuit affirmed this part of the holding.


Another social engineering case in which payment instructions were changed by employees in response to emails. Both courts held there was no direct relationship between the fraudulent email and ultimate payment in which an employee actually had to change wiring instructions in Aquastar’s computer. You will note this case is contrary to that of *Medidata* and *American Tooling*.

The foregoing is but a representative sample of some of the social engineering fraud cases that have recently been before the courts. While the issue remains hotly contested, there are divisions amongst various circuits, and the insurance industry will aggressively defend against social engineering fraud based on the types of coverages provided in each policy. Hence, a close reading of the policy language in conjunction with the particular facts is imperative.

### III. Current Cyber Liability Products

With the expectation that cyber liability and data breaches will become the norm rather than the exception, insurers are responding to those cases in which courts have found liability under the current insurance products on offer.\(^{30}\)

For example, the Insurance Services Office (“ISO”) has introduced new exclusions for CGL policies designed to exclude all coverage for cyber-attack related liabilities. Think analogously of the Absolute Pollution Exclusion. Similar exclusions can be anticipated, if not already included, in Directors & Officers, Errors & Omissions, and Commercial Crime policies.

And no doubt “All Risk” policies will follow in turn by including specific exclusions to “covered property” or adding an endorsement precluding all coverage for cyber breaches/attacks. Again, the analogies are the Absolute Pollution Exclusion, Terrorism exclusions, Asbestos, Silica, etc.

With the foregoing in mind, insurers are working to produce cyber policies tailored to specific industries. The process is an ongoing work in progress.

While this paper is not designed to provide detailed information on cyber products currently available, a few comments are helpful. First, the cyber insurance market is in its infancy, and while growing, insurers are in the process of developing both stand-alone and by endorsement policies and coverages.

Second, one of the biggest issues facing insurers is the inability to measure the “risk.” Cyberattacks and social engineering fraud incidents are random, and there is insufficient historical data to be able to predictably measure, and therefore assign risk, to a product and coverages. Insurers can predict with a relative degree of certainty what the incidents of fire or certain other casualties might be as they have sufficient historical data. Not so with cyber risk.

Third, limits will always be an issue, regardless of predictability. Cyber risks, by their very nature, can impact one company and one event, or one company and thousands of customers. The costs can be exponential depending upon the type of attack and potential exposure. Thus, insurers must protect against the single event with a catastrophic loss profile. Thus, current products will have outer limits in the $10-$20 million range.

Fourth, coverage for cyber risks can be either a stand-alone policy or through an endorsement. Most of the cases outlined in this paper have interpreted coverages which were provided by endorsement or as a part of an overall Commercial Crime Policy. Increasingly, stand-alone cyber products are being introduced to the market. A policy being marketed by a unit of Munich Re provides coverage for information privacy, network security, business interruption, extortion, financial/social engineering fraud and computer fraud, and media liability. It is provided on a claims made basis. The policy itself is too detailed for purposes of this paper, but it represents a stand-alone system of coverages which appears to be the trend amongst certain insurers. Other insurers’ products the authors of this paper have reviewed include Chubb, Great American, Underwriters at Lloyd’s, XL (now part of AXA Group), and American International Group.

What costs should an insured anticipate the need to be covered in the event of a cyber loss? In addition to the coverages that may be available in a cyber policy, whether stand-alone or through endorsement, a policyholder has to be concerned with the types of expenses and costs it will incur in the event of a cyber loss. These include forensic investigation costs, remediation costs to rectify any hardware or software problems, customer notification, restoration of data, business interruption, and legal and public relations expenses. The costs attributable to a cyber loss, as pointed out above, are significant. Regardless of the business, risk management must take into account the ultimate objective of insurance, which is to pay claims. This necessarily requires risk management assess what types of claims might be forthcoming in the event of a cyber loss, and what the cost may be.
PROFESSIONAL LIABILITY

I. INTRODUCTION

Errors & Omissions (“E&O”) insurance is also known as professional liability or malpractice insurance. Unlike a Commercial General Liability (“CGL”) policy’s coverage for bodily injury and property damage, E&O insurance is designed to protect the professional against economic losses of customers, clients, or third parties arising out of negligence, acts, errors, omissions, or wrongful acts occurring in connection with the provision of professional services by the insured party. Inasmuch as CGL policies almost always contain an exclusion for “professional services,” a party providing “professional services” will require E&O coverage.

E&O coverage is generally tailored to the profession to which it is offered. Thus, while the insuring provision of an E&O policy is semantically static regardless of the profession, the exclusions are tailored to the specific profession to which the policy is marketed. E&O insurance is usually part of a program directed at a specific segment of insureds engaged in a “profession.”

The structure of an E&O policy is similar to that of a D&O policy. They both tend to be “claims made” and employ similar risk exclusions. In the discussion below, many of the exclusions as well as conditions and other limitations are discussed generically, regardless of policy type.

II. ERRORS & OMISSIONS / PROFESSIONAL LIABILITY INSURANCE

A. Insuring Provision

While E&O insurance is developed for a specific profession, the insuring provisions from policy to policy are generally the same. Here are three examples:

(a) Architects and Engineers

The Company will pay on behalf of the Insured those sums in excess of the deductible that the Insured shall become legally obligated to pay as Damages because of Claims for a breach of Professional Duty in the performance of Professional Services rendered to others by the Insured or any entity for whom the Insured is legally liable.

31 See, e.g., Keating v. Nat’l Union Fire Ins. Co. of Pittsburgh, Pa., 995 F.2d 154 (9th Cir. 1993).
32 APPLEMAN § 38.04; Grieb v. Citizens Cas. Co., 148 N.W.2d 103 (Wis. 1967).
33 A good example of the variety of professions for which E&O insurance is appropriate is found in RCW 18.01, et seq., ranging from accountancy at RCW 18.04 to recreation therapists at RCW 18.230.
34 Architects and Engineers Professional Liability policy issued by Lexington Insurance Company, form CM-PL1.
(b) Investment Advisor

The Insured will pay on behalf of an Insured Service Provider and its Insured Persons the Loss which they shall become legally obligated to pay as the result of a Claim first made and reported during the policy period or discovery, if applicable, against the Insured Service Provider or its Insured Persons for a Wrongful Act involving the rendering of or failure to render Professional Services which takes place during or prior to the policy period.35

(c) Attorney

This policy shall pay on behalf of each Insured all sums in excess of the deductible amount and up to the limits of liability stated in the Declarations which the Insured shall become legally obligated to pay as damages as a result of CLAIMS first made against the Insured during the Policy Period and reported to the Company during the Policy Period: (1) caused by any act, error or omission for which the Insured is legally responsible; or (2) because of personal injury, and in each case arising out of a rendering or failure to render professional legal services . . . .36

(d) IT Consultant

We will pay on your behalf money in excess of the retention that you become legally required to pay as damages and claim expenses because of a claim caused by a glitch in your performance of technology services.37

B. Professional Service Requirement

The predicate for coverage under an E&O policy is that the negligent or wrongful act, error, or omission must occur during or arise out of or in connection with the rendering of “professional services.”38 The term “professional services” in most E&O policies is defined to include those types of services that are customarily and uniformly provided by the profession to whom the policy is directed. For example, “professional legal services” can mean “legal services and activities performed for others as a lawyer, notary public, arbitrator, mediator, title insurance agent, court appointed fiduciary, services rendered as a member of a bar association, ethics, peer review, formal accreditation board or similar professional board . . . .”39

---

35 Investment Advisor policy issued by Arch Specialty Insurance Company.
36 Lawyers Professional Liability policy issued by Liberty Insurance Underwriters, Inc.
37 Hartford Fire Insurance Co. Technology Liability policy.
38 APPLEMAN § 38.04.
39 This is a typical definition of “professional legal services” and is taken from a lawyer’s professional liability policy issued by Liberty Insurance Underwriters Inc., Form No. LIU 1601 ED 07 02.
Similarly, in the context of an investment advisor, “professional services” can mean the “professional services rendered by an Insured Service Provider in the regular course of its business and for an insured fund for compensation.”

Regardless of whether a policy contains a definition of “professional services” and circumscribes the range of activities that may be included within the insured’s “professional services,” case law may be used to supplement the term when issues relating to whether an insured is performing “professional services” or whether the act, error, or omission occurred during the course of performing “professional services.” The classic judicial definition of professional services is contained in Bank of California, N.A. v. W.H. Opie, et al., quoting from Marx v. Hartford Accident & Indemnity Co., as follows:

[S]omething more than an act flowing from mere employment or vocation is essential. The act or service must be such as exacts the use or application of special learning or attainments of some kind. The term “professional” in the context used in the policy provision means something more than mere proficiency in the performance of a task and implies intellectual skill as contrasted with that used in an occupation for production or sale of commodities. A “professional” act or services when arising out of a vocation, calling, occupation, or employment involving specialized knowledge, labor, or skill, and the labor or skill involved is predominantly mental or intellectual, rather than physical or manual. . . . in determining whether a particular act is of a professional nature or a “professional service” we must look not to the title or character of the party performing the act, but to the act itself.

Not every act by a professional is the rendition of “professional services.” Rather, to be considered a professional service the liability “must arise out of the special risks inherent in the practice of the profession.” Similarly, professional liability policies do not cover general administrative activities that occur in all types of businesses such as employment decisions, billing practices, or contract disputes in which the capacity of the parties is as business people and not professionals.

---

40 A typical definition of professional services rendered by financial advisors, in this case, an extract from an Arch Specialty Insurance Company policy Form IAP 0002 00 12 03.
41 663 F.2d 977 (9th Cir. 1981). (One of the authors of this paper represented W.H. Opie.)
42 157 N.W.2d 870, 871-72 (Neb. 1968).
43 Id. at 981.
44 MSO Wash., Inc. v. RSUI Group, Inc., 2013 WL 1914482 (W.D. Wash. May 8, 2013) (“The courts in this district and elsewhere have unanimously concluded that the submission of billing claims under the FCA (False Claims Act) does not qualify as a “professional service.”). But see Bayley Constr. v. Great Am. E & S Ins. Co., 980 F. Supp. 2d 1281 (2013) (declining to apply both MSO Wash. and Opie and holding tracking subcontractors’ wage payments could constitute “professional service” under policy definition that included “construction management, pre-construction consulting services, and design services).
C. Coverage for Wrongful Acts

The liability of the insured in the course of rendering professional services must arise out of a “wrongful act.” A “wrongful act,” or similarly denominated delict is generally defined as any actual or alleged act, error or omission, misstatement, misleading statement, or neglect or breach of duty by the insured. Absent an “intentional act” exclusion, it is not unusual for a “wrongful act” to embrace intentional misconduct falling short of criminal misconduct.46

D. Claims by Clients or Third Parties

E&O insurance is designed to protect the professional from claims originating from the professional’s relationship with its clients. In this relationship, there is seldom provoked a dispute with the insurer. A more interesting issue, however, is if during the course of providing professional services to a client, the professional commits a tort or engages in conduct that results in a third party bringing an action against the professional: is the professional covered? The answer is yes.

Again, the case of Bank of California, N.A. v. W.H. Opie, et al., is instructive.47 Opie was a mortgage banking business in Tacoma and had entered into loan agreements with the Bank of California to fund its operating expenses in financing construction projects, assigning the trust deeds and mortgages covering the projects to the bank as security. Employees of Opie misapplied the mortgage funds received from lenders with the result that the construction lenders first lien position was paramount to the Bank of California. The construction lenders were entitled to foreclose on the properties and the trust deeds and mortgages pledged to the bank were essentially rendered worthless. The bank sued Opie and recovered a judgment and then sought to collect the judgment from Opie’s E&O carrier, California Union Insurance Company.

While the principal dispute in the insurance case revolved around whether Opie’s conduct constituted the rendition of a “professional service” within the meaning of Cal. Union’s policy, a secondary and equally important issue was whether the policy required “as a condition of coverage, a professional-service relationship to exist between the insured and the party harmed by the insured’s act or omission.” The Court held: “the policy plainly makes coverage dependent upon the nature of the insured’s conduct, not the status of the party harmed.”48

Thus to the extent the third party’s harm was predicated on an act, error, or omission in the provision of professional services, liability would attach even though there was no professional service relationship between the party harmed—Bank of California—and the Insured, W.H. Opie.

46 The issue generally is whether the definition of “wrongful act” contains the word “negligent” as a modifier to “act, error or omission.” E.g., In re Payroll Am., Inc., 459 B.R. 94 (Bankr. D. Idaho 2011) (professional liability insurer with policy covering “negligent act, error or omission” owed duty to defend complaints alleging negligence or elements of negligence claim, but not complaints alleging only breach of contract, conversion, and fraud); see also; Comm. Indemn. Ins. Co. v. Der Travel Serv. Inc., 328 F.3d 347 (7th Cir. 2003); City of Fort Pierre v. United Fire & Cas. Co., 463 N.W.2d 485 (S. Dak. 1990). If on the other hand negligence is not a modifier then some intentional conduct such as breach of contract will be covered. Gateway Grp. Advantage Inc. v. McCarthy, 300 F. Supp. 2d 236 (D. Mass. 2003); Cont'l Cas. Ins. Co. v. Cole, 809 F.2d 891 (D.C. 1987).
47 W.H. Opie, 663 F.2d 977.
48 Id. at 982.
E.  Exclusions and Other Barriers to Coverage

1.  Prior Acts/Notice/Retroactive Date

There are two aspects involved in exclusions relating to prior acts. The first relates to a “retroactive date.” This is a date generally coinciding with the first issuance of a professional liability or D&O policy to an insured. It is not an arbitrary date, but one underwriters believe provides a sense of security in that claims that may have arisen prior to the “retroactive date” will not be covered under prior policies or under the one being issued. Claims arising out of acts occurring prior to the retroactive date, regardless whether the claim is made during the policy period, are not covered.

Many current policies provide a broader “prior acts” exclusion called a “Specific Incidence Exclusion.” This exclusion is designed to apply to any claim against an insured arising out of a wrongful act or any fact, circumstance, incident, claim or suit referred to in an answer to any question on an application or renewal application. This exclusion works in conjunction with notices in the application itself indicating any misstatement will result in voiding of the policy. (See “Insurer Claims for Rescission” below.)

The second aspect relates to notice. In this context, if an insured has notice of a potential claim in which a demand has been initiated and fails to notify the incumbent insurer or in some cases a predecessor insurer, there will be no coverage.

Exclusions relating to “notice” are not governed by the “notice/prejudice” rule in Washington. If timely notice is not given under a claims-made policy, an insurer’s prejudice is irrelevant. Similarly, if an insured has “prior notice” of a potential claim, or notice of circumstances of a potential claim, prejudice to the insurer is irrelevant if a claim is made during the incumbent insurer’s policy period.

Finally, notice issues often involve exclusions for “interrelated wrongful acts” or “related wrongful acts” which is the subject of discussion below. It is therefore important that in the event of doubt, give notice.

2.  Bodily Injury/Emotional Distress

“Bodily injury,” and to the extent “bodily injury” includes emotional distress, is generally covered under commercial general liability policies. Since D&O and E&O polices are designed

49 See generally APPLEMAN § 38.24[6].
50 A good example is the exclusion contained in Evanston Ins. Co. v. Workland & Witherspoon, PLLC, 2015 WL 1927683 (E.D. Wash. Apr. 28, 2015) (While the court considered the Specific Incidence Exclusion, the insurer’s failure to properly support the exclusion with admissible evidence on a motion for summary judgment precluded the Court from reaching a decision on its application.).
51 This rule, applicable under CGL and other non-claims made coverages, provides that an insured’s late notice does not affect its ability to recover under the policy unless the insurer can demonstrate it has been suffered actual and substantial prejudice. Safeco Title Ins. Co. v. Gannom, 54 Wn. App. 330, 774 P.2d 30 (1989), rev. denied, 113 Wn.2d 1026, 782 P.2d 1069 (1989); Moody v. Am. Guarantee & Liability Ins. Co., 804 F. Supp. 2d 1123 (W.D. Wash. 2011).
principally to protect against economic injuries, the bodily injury exclusion is almost universal.
D&O and E&O insurers do not want to replicate the CGL coverage.

3. **Breach of Contract**

Some E&O policies exclude claims arising out of breach of written contracts. The key element is whether the court in a particular jurisdiction will read the exclusion broadly or narrowly. For example, in *Stanford Ranch, Inc. v. Maryland Casualty Co.*, the court held a complaint alleging breach of contract was excluded because the claim was dependent on the existence of an underlying contract.52 On the other hand, if the insured’s liability does not depend solely on violation of a contract, for example, violation of a statute may also be involved, the exclusion is generally inapplicable.53

4. **Intentional Conduct/Fraudulent Conduct**

The “dishonesty” exclusion is contained in some fashion in almost every E&O policy. Underwriters are simply not going to encourage the moral hazard of dishonest, fraudulent, or criminal misconduct. The policies, however, generally require a “final adjudication” or a determination “in fact” that the insured has engaged in prohibited conduct before the exclusion can be triggered.54 Where the policy requires a “final adjudication,” the adjudication must be made in the underlying case, rather than in contemporaneous or subsequent coverage litigation.55 Where the “in fact” language is used, the factual finding may be made either in the underlying case or parallel coverage litigation.56

In order for the exclusion to apply, the finding of dishonesty, fraud, or criminal conduct must be conclusive of the insured’s liability. If the insured could be liable without a finding of dishonesty, then the exclusion is inapplicable.57

An issue in many cases is interpretation of the term “dishonesty” in conjunction with facts surrounding the conduct. Most courts will generally require some intentional conduct in contrast to conduct not amounting to “actual dishonest purpose and intent.”58

Increasingly, claims are being brought under the Federal False Claims Act (“FCA”), 31 USC § 3729, et seq. Generally, a party cannot be held liable under the FCA for ordinary negligence. Rather, liability under the FCA involves scienter and dishonest conduct. Most courts have held FCA claims fall within a “dishonest act” exclusion.59

---

52 89 F.3d 618 (9th Cir. 1996).
53 *Andover Newton Theological Sch., Inc. v. Cont’l Cas. Co.*, 930 F.2d 89 (1st Cir. 1991); *Sch. Dist. for City of Royal Oak v. Cont’l Cas. Co.*, 912 F.2d 844 (6th Cir. 1990).
55 *Pendergast-Holt v. Certain Underwriters at Lloyd’s, London*, 600 F.3d 562, 572-73 (5th Cir. 2010).
56 Id.
59 *MSO Wash.*, 2013 WL 1914482.
5. **Illegal Profit or Advantage**

Almost every E&O policy excludes “Loss” on account of any “Claim” “alleging, based upon, or arising out of the gaining in fact of any profit, remuneration, or financial advantage to which any Insured was not legally entitled.” Exclusion of illegal profits may also (or alternatively) be found in the definition of “Loss” of some policies, in the form of an exception from the definition of “Loss” for restitutionary damages.60

Because the illegal profit exclusion typically contains the qualification that the profit must be gained “in fact,” a judicial finding that the insured is required to disgorge illegal profits is required to trigger the exclusion.

6. **Insured Versus Insured**

In the broadest sense, almost all D&O and E&O policies exclude actions involving one insured suing another insured. In the D&O world, this exclusion is one of the most often litigated as officers often bring claims against the companies for which they formerly served. Similarly, actions by a company against its officers and directors for misfeasance in office will also trigger the insured versus insured or “IvI” exclusion.

The IvI exclusion has its origin in underwriters’ intent to prevent collusive lawsuits between officers and directors and the corporation and providing funding for corporate misconduct.61

Over the years, as case law has provided substance to the exclusion, insurers have marked out certain exceptions to its application where the indicia of collusive action is not present. For example, shareholder derivative suits are commonly excepted. Other exceptions may include regulatory claims prosecuted on behalf of the FDIC or Resolution Trust Corporation.62 The case law is, however, not uniform, and many courts have over the years upheld the IvI exclusion even though brought by a regulatory agency.63

7. **Employment Practices Liability**

Unless added by endorsement or included within the E&O policy, employment practice claims are almost universally excluded from E&O insurance. The reason for the exclusion is self-evident: with a dramatic increase in employment related claims over the last 20 years, insurers have attempted to restrict the number of policies available for payment of these claims while at the

---


61 *Seafirst*, 1986 WL 1174695.


same time channeling policyholders into products that are specifically underwritten to manage employment related claims such as employment practices liability insurance.\(^{64}\)

The employment related activities exclusion often operates in conjunction with the insured versus insured exclusion to the extent an officer or director is prosecuting a claim against his or her own corporation for employment related conduct or liability.

8. **Outside Entity Liability**

Insurers recognize officers and directors as well as other professionals often serve on both for profit and non-profit boards unassociated with their employment. In the absence of a complete exclusion for liability arising from service to an outside entity, many insurers will either make an exception to the exclusion for certain types of boards, such as non-profit, or provide, for a premium, coverage for outside entity liability.

F. **Additional Considerations**

1. **Policy Limits: Defense Inside/Outside Limits; Self-Insured Retention**

Most professional liability policies are sold with a single limit of liability both per-occurrence and in the aggregate. The limit of liability also incorporates defense costs such that the limit of liability is decreased by the amount of defense costs. In common parlance, these are known as “wasting” policies.

For an additional premium it is possible in most circumstances to purchase additional “defense cost coverage.” This means the insurer will provide a certain limit of defense costs in addition to the limit of liability. For example, if an architect, engineer or attorney purchased a $2 million professional liability policy, it could also purchase defense costs coverage for anywhere from $500,000 to $1 million. Once the defense limit is reached, the indemnity limit of liability will be tapped and thereby decrease with the level of defense costs reimbursement.

Whether the defense costs are included within the limit of liability or not presents different strategic choices for the professional and the plaintiff. Defense within limits also presents strategic issues for the insurer, particularly if the consequences of the alleged wrongful act exceed the policy limits. How long does the insurer allow the defense to waste the limits of liability in the face of a policy limits demand? From the plaintiff’s perspective, aggressive litigation reduces the limits of liability for indemnity; a more judicious approach to litigation might therefore be warranted. From the perspective of the professional, the issue is whether an excess judgment will affect personal or corporate assets.

Most professional liability policies require the professional to pay a self-insured retention (“SIR”) or deductible. There are a couple of considerations that are important when the SIR involves a significant outlay by the professional. First, who gets to select counsel? Most E&O insurers have panel lawyers experienced in defending E&O claims related to the policyholder’s

\(^{64}\) MATHIAS, BURNS, NEUMEIER & BURGDOERFER, DIRECTORS AND OFFICERS LIABILITY: PREVENTION, INSURANCE AND INDEMNIFICATION (2006).
particular profession. On the other hand, many larger professionals have counsel they would prefer. Who gets to choose?

Second, after the SIR is paid, does the insurer now get to pick counsel of its own choice since its funds are at issue? Generally, the insurer will not change counsel but will restrict the rates it will pay counsel selected by the policyholder. This results in an additional issue relating to whether the retained private counsel will accept the insurer’s rate schedule or insist on the policyholder paying the difference between the insurer’s reimbursement rate and the lawyer’s normal rate. This can often involve a process of negotiation between the policyholder, its private counsel, and the insurer.

Analysis of the limits of liability, consideration of defense costs, SIR, and appointed or private counsel are considerations that are often overlooked at the beginning of an E&O matter. They need to be considered upfront to avoid later problems.

2. Related Claims

E&O policies contain “batching” provisions that attempt to collapse together claims arising from the same set of facts. Often falling under the policy’s Limits of Liability section, these “related claims” clauses provide that all “related” claims, or those based on “interrelated wrongful acts,” are “deemed made” at the time of the first such claim. This serves at least two purposes. From the insurer’s perspective, related claims clauses ensure that multiple claims arising from one set of facts or a similar type of conduct will trigger coverage under only the policy on the risk at the time the first claim was made, protecting insurers from liability under multiple, successive policies issued to the same insured. From the insured’s perspective, related claims clauses can be useful in arguing only one deductible or SIR should be applied to multiple claims.

Coverage disputes involving the related claims clause generally boil down to the parties’ competing conceptualizations of what “related” or “interrelated” means. Many policies define the term, but these definitions can often be characterized as ambiguous because they use terms like “similar,” “same,” and “connected.” In the absence of a policy definition, “related” or “interrelated” claims are generally those that have a “logical connection,” interpreted as a “substantial factual overlap.”

3. Consent to Settle or “Hammer” Clauses

Certain professions have “earned” the right to consent to any settlement proposed by their insurer. While consent to settle clauses were initiated in medical malpractice liability policies they have been incorporated into policies marketed to almost all professions. The purpose of the consent to settle or “hammer” clause is to allow the professional a certain leeway in determining whether to accept a proposed settlement for which the insurer is agreeable, while at the same time penalizing the professional if his or her decision is wrong. Thus policies will include provisions that require the professional to consent but in the event the professional rejects the settlement, any

---

later settlement or judgment for an amount greater than what could have been agreed upon in the first instance, will be paid solely by the professional or split 50/50. In other words, the downside risk of rejecting a settlement is placed on the professional, not the insurer.66

4. **Insurer Claims for Rescission**

a. **The Application: Truth or Consequences**

An insurer may seek to have its policy declared void ab initio by raising a claim for rescission of the policy against its insured. Rescission claims often arise as counterclaims to coverage litigation. They are based on the premise that the insured failed to disclose all material information in response to questions on the insurance application, most often financial information or claims history. An insurer claiming rescission may rely on common law equitable principles as well as policy language which purports to render the policy voidable in the event information provided in the application is later discovered to be false or incomplete.

Rescission of the policy is permitted in Washington only when (1) the insured represented certain information as truthful during the negotiation of the insurance contract; (2) those representations were untruthful, that is, they were misrepresentations; (3) the misrepresentations were material; and (4) they were made with the intent to deceive.67 The insurer must prove each element by clear, cogent, and convincing evidence.68

However, rescission claims can be far less difficult to establish in other jurisdictions, many of which do not require a showing of deceptive intent.69

An insurer intending to rescind a policy must issue a refund of the premiums to its insured. An insured who cashes the refund check may be held to have consented to the rescission, despite having previously disputed the insurer’s right to rescind.70

b. **Discovery: Extensive and Expensive**

Although rescission claims are difficult to prove, they still present insureds with difficulty because they can be used to justify extensive discovery into the insured’s prior knowledge of claims, including depositions of key persons involved in the application process as well as extensive document discovery of placement correspondence and broker files. Worse, they place the insured on the defensive in its pursuit of the benefits of its own insurance policy, which can drastically (and negatively) affect the insured’s litigation strategy and bargaining position.

---

69 E.g., Cont’l Cas. Co. v. Marshall Granger & Co., LLP, 921 F. Supp. 2d 111, 119 (S.D.N.Y. 2013) (under New York law, even innocent misrepresentations will support a claim for rescission if they are material).
Given all this, the best practice is to handle the insurance application process (and encourage your clients to do so) with the utmost care and candor.

c. **Severability**

Be aware the policy may restrict the insurer’s ability to rescind to only those individuals responsible for the misrepresentation (called a “severability” provision). The purpose of a severability clause is to allow coverage to be provided to innocent co-insureds in the event one insured is excluded from coverage because of misconduct, fraud, or criminal behavior. Often the severability provision is invoked when one insured fails to disclose certain material information in an application potentially to the detriment of other insured.\(^{71}\)

The specific wording of the severability provision is important. Some severability provisions advise that a material misrepresentation by one officer or director or one of many professionals in a company will not be imputed to any other officer, director, or professional. In this case, innocent co-insureds will be entitled to coverage notwithstanding the misconduct of another insured. On the other hand, there are severability provisions that restrict the ability of a policyholder to argue for the innocent co-insureds. For example, a severability provision may provide that facts known to specific officers will be imputed to all other officers and directors.\(^{72}\)

In defending or preempting a rescission claim, careful review of the policy and application language is essential.

---


\(^{72}\) See, e.g., *ClearOne Comm’ns, Inc. v. Nat’l Union Fire Ins. Co. of Pittsburgh, Pa.*, 494 F.3d 1238 (10th Cir. 2007); *Cutter & Buck*, 306 F. Supp. 2d 988.