FirstLook

Issues and Developments in Insurance Law

Letter from the Insurance Company Team

Your company's computer system has been compromised by a hacker. From your initial investigation, you discover that the hacker has accessed proprietary company information and customer information including Social Security Numbers, caused an interruption in your internal computer system, and caused an interruption in service to your customers. You also realize that this may just be the tip of the iceberg. One of the first questions that arises when such an event occurs is likely to be the extent to which this event will be covered by insurance. Will your traditional commercial general liability policies ("CGL Policies") cover the cyber attack? What about your separate Cyber Liability Insurance Policies ("CLI Policies")?

Recent headlines have been replete with high-profile stories of large cyber attacks affecting a variety of industries including, for example, the health care sector, the retail sector, and the financial sector. One of the most publicized cyber attacks affecting the retail industry was the 2013 Target Corp. data breach that reportedly affected approximately 110 million Target customers. The Target breach and the related insurance issues are addressed herein.

Most businesses faced with this question have turned to the issuers of their CGL policies for relief. However, the question of available liability coverage for a cyber attack is not an easy one under a CGL policy. The common issues relating to CGL coverage and cyber losses is also addressed herein.

Many businesses are determining that CGL policies may not afford adequate coverage to cover damage done to consumers as a result of a cyber attack and insurers began developing new products termed cyber liability insurance (CLI) for their insureds to manage the risks associated with cyber liability. Common things to look for in CLI policies is another article in this issue.

The articles in this issue provide an overview of what can happen if a breach occurs that is uninsured, the issues that are seen when a company seeks CGL coverage for cyber losses, and matters a company should consider when purchasing CLI. This issue should provide a "First Look" at cyber-related insurance issues.

INSIDE THIS EDITION:

Getting the Knack of Anti-Hacker Insurance

IN THIS ISSUE

The Target Data Breach: Anecdotal Evidence of the Importance of Adequate Cyber Insurance

By: Shawn A. Morgan

Target Corporation was the victim of a massive data breach in late 2013. As one of the United States' largest retailers, Target may have thought that it had more than enough cyber insurance before the full-scale effects of the breach were determined. Even with tens of millions of dollars in cyber coverage, in the end, Target has still paid more than two hundred million dollars "out of pocket."

What Happened?

In December 2013, during the rush of the holiday shopping season, Target discovered that it had been the victim of a cyber-attack that allowed unauthorized access to customers' personal data.[1] Even though Target had cyber security software, the breach went undetected for almost three weeks. In his testimony before the Senate Committee on Commerce, Science, and Transportation following the breach, John Mulligan, the Executive Vice President and Chief Financial Officer of Target, testified that the hackers entered Target's systems on November 12, 2013, after receiving low level log-in credentials from a vendor that services Target's HVAC system.[2] The suspicious activity was initially caught by Target's cyber security software but was not further investigated because it was on the "outermost portion of [their] network."[3] In time, the hackers moved through Target's network and were able to place malware on point-of-sale registers.[4] This malware recorded payment card information in the time between its entry and its encryption.[5] The malware functioned for three weeks and remained undetected by Target's internal systems. It was only detected after the United States Department of Justice contacted Target on December 12, 2013 regarding suspicious activity involving payment cards that had been used at Target stores.[6] From there, things escalated quickly and within two days Target had met with the Justice Department and Secret Service, and had hired a team of cyber forensic experts.[7] By the third day, the malware had been identified and removed from Target's systems.[8]

What Were the Effects?

During the breach, Target estimates that more than 100 million customers were affected.[9] Of those, 40 million had credit and debit card records obtained by the hackers.[10] These records included card numbers, expiration dates, and CVV data encoded on each card's magnetic strip.[11] Target estimates that more than 70 million other customers had their personal information such as names, addresses, email addresses, and phone numbers stolen.[12] According to reports, about 12 million people fall into both groups and are at an even greater risk of identity theft.[13] As a silver lining for consumers, Target claims that no social security numbers or debit card PIN numbers were compromised in the attack.

After Target made the public aware of the data breach, the expenses started to add up quickly. These included:

- **One year of credit monitoring for every potentially affected customer**
- **Legal fees related to defending lawsuits**
- **Replacing the affected debit and credit cards**
- **Covering fraudulent charges made on affected cards**
- **Hiring a team of cyber experts to investigate**
- **Media and publications to inform consumers of the breach**
- **Settlements in two major class action lawsuits**

Altogether, in 2015, Target reported that it had suffered $291 million in expenses related to the data breach.[14] In addition, Target suffered major damage to its reputation and faced a more than $21 billion drop in sales in just the fourth quarter of 2014.[15] As part of its revitalization efforts, Target also invested $100 million into upgrading its point-of-sale terminals to safer, CHIP enabled technology.[16] These losses are reportedly not factored into the $291 million figure.

How Did Cyber Insurance Come Into Play?

Target had at least $90 million in cyber insurance.[17] Although Target was not open about the exact policies and carriers it had, several news outlets reported that "well-placed sources" said Target was self-insured for the first $10 million of cyber coverage.[18] After that, it is said that Target had the following layered policies:

- **$15 million - Ace Ltd.;**
- **$15 million - American International Group, Inc.;**
- **$10 million - Bermuda-based Axis Capital Holdings Ltd.;**

- **$10 million - American International Group, Inc.; and**
- **$40 million - quota insurance divided among four unidentified insurers.[19]**

In total, these policies would provide Target insurance for up to $90 million after its $10 million self-insured retention. While the existence of these policies and their coverage limits cannot be confirmed, Target reported in its 2015 annual report that it expected insurance recoveries to offset its $291 million in expenses by $90 million, leaving Target responsible for the remaining $201 million.[20]

The Target estimates highlight the need for businesses to obtain sufficient cyber insurance, liability, and excess coverages, as well as to understand coverage limits. They also demonstrate the extent to which even a short-term breach can have adverse, lasting consequences for a business.

---

[1] *Hearing on Protecting Personal Consumer Information From Cyber Attacks and Data Breaches before S. Comm. On Commerce, Science, and Transportation*, 113th Cong. 2 (2014) (statement of John Mulligan, Executive Vice President and Chief Financial Officer, Target Corp.).
[2] *Id.* at 3.
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.* at 4.
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] 2015 Target Ann. Rep. 54, https://corporate.target.com/_media/TargetCorp/annualreports/2015/pdfs/Target-2015-Annual-Report.pdf.
[15] Dhanya Skariachan and Jim Finkle, Insurance Journal, *Target's Cyber Insurance Softens Blow of Massive Credit Breach* (Feb. 26, 2014), https://www.insurancejournal.com/news/national/2014/02/26/321638.htm.
[16] *Hearing on Protecting Personal Consumer Information From Cyber Attacks and Data Breaches before S. Comm. On Commerce, Science, and Transportation*, 113th Cong. 6 (2014) (statement of John Mulligan, Executive Vice President and Chief Financial Officer, Target Corp.).
[17] 2015 Target Ann. Rep. 54, https://corporate.target.com/_media/TargetCorp/annualreports/2015/pdfs/Target-2015-Annual-Report.pdf
[18] Judy Greenwald, Business Insurance, *Target has $100M of Cyber Insurance, $65M of D&O Cover: Sources* (January 14, 2014), http://www.businessinsurance.com/article/20140114/NEWS07/140119934.
[19] *Id.*
[20] 2015 Target Ann. Rep. 54, https://corporate.target.com/_media/TargetCorp/annualreports/2015/pdfs/Target-2015-Annual-Report.pdf

Looking for Coverage in All the Wrong Places: Problems with Relying on Traditional CGL Policies to Cover Cyber Losses.

By: Melanie Morgan Norris

From Target to Facebook, the dissemination of electronically stored private information has garnered significant media attention, coining phrases such as "data breach" and "cyber-attack." Although only significant data breaches make the news, the fact is data breaches occur every day. As one might expect, the cost of a "cyber loss" can be significant for the compromised business. Although not clearly defined, a "cyber loss" generally refers to "any loss associated with the use of electronic equipment, computers, information technology, or virtual reality."[1] A cyber loss can result in a first-party claim, seeking to recover the insured's cost of responding to a cyber-attack, including investigation, notification to consumers and reporting agencies, remedial efforts, etc. A cyber loss can also result in third-party claims against an insured by consumers or clients whose personal information or data was impacted by a cyber-attack.

When litigation ensues, the compromised business will quickly scramble to pursue any available insurance coverage to lessen the financial blow of the cyber loss. Because commercial general liability ("CGL") policies are the most common form of insurance found in the corporate context, there is an evolving body of case law addressing coverage for cyber losses under a traditional CGL policy. Most coverage battles that have been waged were over whether the cyber loss constitutes "property damage" and/or whether the cyber loss constitutes "personal injury and advertising injury." Not unexpectedly, courts have taken different positions on these issues.

A traditional CGL policy broadly provides coverage under Coverage Part A for "property damage" caused by an occurrence, except for injury or damage that is precluded by an exclusion.[2] The insuring agreement for Part A typically provides, in relevant part:

> We will pay those sums that the insured becomes legally obligated to pay as damages because of . . . "property damage" to which this insurance applies.[3]

"Property damage" means "physical injury to tangible property . . ." and "loss of use of tangible property that is not physically injured."[4] Some courts have held that there must be evidence of damage to a tangible component of a computer or similar equipment for there to be property damage coverage. For instance, in *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*,[5] AOL, an internet service provider, filed suit against its insurer seeking a defense and indemnification against claims that AOL's software had altered its customers' existing software, resulting in the loss of stored data and causing their operating systems to crash. The Fourth Circuit rejected AOL's argument that the claim constituted "physical damage to tangible property". Instead, the Court found that because the damage was to software, as opposed to actual physical equipment, there was no damage to "tangible property" so as to trigger coverage under the policy. The court agreed that the malfunction of the software caused the actual computers to be unusable, resulting in a loss of use of tangible property under the definition of property damage. However, the court held that there was still no coverage because the "impaired property" exclusion precluded coverage for property damage resulting from the insured's faulty products.

Other courts, however, have taken a much broader interpretation, concluding that the loss of a computer or data constitutes "property damage." In the unreported case of *Nationwide Ins. Co. v. Hentz*,[6] a CD-ROM containing personal information of 30,000 participants of Central Laborers' Funds and a portable laptop were stolen from Hentz's car. The CD-ROM had been in Hentz's possession because she was an accountant hired by Central Laborers to perform auditing services. Central Laborers sued Hentz to recover the costs it incurred in responding to the theft which included notification and credit monitoring services for the participants. A subsequent coverage dispute arose between Hentz and her insurance carrier over whether the physical loss of the CD-ROM was "property damage." Hentz argued that it was property damage because she had suffered the loss of use of tangible property. The carrier, on the other hand, argued that the loss of the data on the CD-ROM was an intangible loss outside the definition of property damage. The court held that coverage existed for the claim because although the data would not have constituted "tangible property" had someone hacked into the computer and stolen it, in the case before it, the data was stored on a physical CD-ROM that was stolen.

Cyber loss claims are also frequently submitted under Coverage Part B – Personal Injury and Advertising Injury. Under the standard ISO form, the insuring agreement for Coverage Part B provides:

> We will pay those sums that the insured becomes legally obligated to pay as damages because of "personal and advertising injury" to which this insurance applies.[7]

"Personal and advertising injury" is defined as "injury . . . arising out of . . . oral or written publication, in any manner, of material that violates a person's right of privacy."[8] Coverage disputes have primarily focused on whether a data breach resulting in the dissemination of personal information constitutes a publication so as to trigger Coverage Part B. Recently, the Fourth Circuit found coverage under Part B for a cyber loss. In *Travelers Indemnity Co. of America v. Portal Healthcare Solutions*, LLC,[9] the Fourth Circuit affirmed the Eastern District of Virginia's finding that a carrier had a duty to defend and indemnify its insured in a civil lawsuit arising out of a data breach. The insured, Portal Healthcare, was engaged by a hospital to store and safeguard confidential medical records. The insured was sued in a class action alleging that it engaged in conduct that resulted in private medical records being on the internet for a period of more than four months. The District Court held that the carrier was required to defend and indemnify under Coverage Part B – personal and advertising injury, reasoning that making confidential medical records publicly accessible via an internet search fell within the plain meaning of "publication" which was undefined in the policy. The court found unpersuasive the carrier's argument that there was no evidence that a third-party had accessed and viewed the information, concluding that once the information was available to the public it was "published", regardless of whether anyone chose to read it.[10]

This opinions differs from that of *Recall Total Information Management, Inc. v. Federal Ins. Co.*,[11] wherein the Court held that the carrier was not obligated to defend or indemnify the insured, a data management firm, after several IBM computer tapes entrusted to the insured's care fell out of a transport van alongside the road and were assumed retrieved by someone. The tapes contained personal information of nearly one half million IBM employees. IBM incurred $6 million dollars in costs resulting from the loss of the tapes, including notification to the affected individuals and credit monitoring. IBM thereafter filed suit against the insured data management firm, seeking to recover its costs. The insured data management firm alleged that the loss of the tapes was a personal injury under Coverage Part B; however, the court held that the loss was not within the scope of the personal injury coverage. Although the personal information on tapes had been lost, the court concluded there had been no publication of the information resulting in a privacy violation.

Case law continues to evolve regarding coverage for cyber losses under traditional CGL policies. However, existing case law makes clear that the specific policy language and facts of the loss will be closely considered by the courts in any coverage dispute. Knowing the position of the court in the relevant jurisdiction is crucial in determining whether coverage exists for a defense and indemnification.

Likely because of the mixed reviews from courts to date, the insurance industry has taken steps "to clarify that coverage for [cyber] breaches is excluded" by adding endorsements to existing CGL policies "specifically excluding liability arising out of the disclosure of confidential or personal information."[12] In 2001, ISO revised the policy form for Coverage A to clarify that electronic data is not tangible property, and again in 2004, ISO created a new exclusion for damage and loss of use to electronic data.[13] Beginning in 2014, ISO made available new forms for optional endorsements that exclude coverage for personal injury or advertising claims arising from the access to or disclosure of confidential information.[14] As the use of such endorsements increases in popularity, we can expect to see further litigation over the effectiveness of the endorsements in eliminating any potential coverage for cyber loss claims under CGL Policies.

---

[1] Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges*, 33 Quinnipiac L. Rev. 369, 371 (2015).
[2] Due to space constraints, this article does not address all of the potentially relevant exclusions under the CGL policy. It is worth noting, however, that several exclusions are potentially implicated by a cyber loss depending upon the facts of the specific claim, including "impaired property", "damage to property", "electronic data", "damage to your product", etc.
[3] ISO Form CG 00 01 04 13.
[4] *Id.*
[5] 347 F.3d 89 (4th Cir. 2003).
[6] 2012 WL 734193 (S.D. IL, Mar. 6, 2012).
[7] ISO Form CG 00 01 04 13.
[8] *Id.*
[9] 644 Fed.App'x. 245 (4th Cir. 2016).
[10] *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC,* 35 F. Supp. 3d 765, 771 (E.D. Va. 2014), *aff'd sub nom., Travelers Indem. Co. of Am. v. Portal Healthcare Sols.,* L.L.C., 644 F. App'x 245 (4th Cir. 2016).
[11] *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 147 Conn. App. 450, 83 A.3d 664, 671–73 (2014), *certification granted in part*, 311 Conn. 925, 86 A.3d 469 (2014) and *judgment aff'd*, 317 Conn. 46, 115 A.3d 458 (2015).
[12] C. Zachary Rosenberg and Judy Selby, *Cyber Insurance: Insuring for Data Breach Risk*, Practical Law Practice Note, p. 5 (Dec. 2014).
[13] *Recovery for cyber-related loss under coverage A of commercial general liability policy,* 4Pt2 Bruner & O'Connor Construction Law § 11:574; see also ISO Form CG 00 01 10 01 and ISO Form CG 00 01 12 07.
[14] *See* FN 12, at 6.

Common Elements and Exclusions of Cyber-Security Policies: What Do Businesses Typically Look For?

By Mark A. Moses

In late June 2018, sporting goods giant Adidas warned millions of its U.S. customers about a potential data breach.[1] Per its press release, an unidentified third-party obtained contact information, usernames, and encrypted passwords, but had not obtained any credit card or other personal information at the time.[2] Although its customers' financial information was not obtained, other companies have not been so fortunate. In April of 2018, both Sears and Delta announced a similar third-party data breach that resulted in the acquisition of online customer payment information of a subset of its customers.[3] Not only do these breaches impact a company's goodwill, brand, and image, but they also affect its bottomline by way of increased investigation costs, remediation costs, and legal fees.

Consequently, the demand for adequate cyber-security insurance coverage options, above-and-beyond a company's standard CGL policy, has grown rapidly over the past decade, with the majority of this growth occurring domestically.[4] It is important for entities seeking coverage for data-breach and other cyber-security threats to properly evaluate their options for coverage, and potential exclusions, to ensure that they are protected in the event of a threat.

Key coverage components to evaluate include:

- **First-party Versus Third-party Losses:**

Arguably the most important aspect of any cyber-security policy involves the scope of coverage between first- and third-party data loss, and the necessity for coverage for both. First-party coverage generally applies to coverage that the insured entity maintains to protect its own data and losses from breach. Third-party coverage generally refers to liability coverage

that the insured entity maintains to protect itself from losses claimed by other parties—namely its customers or related business partners. Both coverages are important in order to maintain sufficient protection in the event of a data breach.

For example, first-party coverage protects against losses directly incurred by the entity and usually includes coverage for theft/fraud/extortion of data, forensic investigation costs, business interruption, and computer loss and restoration.[5] Third-party coverage typically covers losses and costs that occur outside of the insured entity including: litigation costs, regulation and fines, notification costs, credit monitoring, and/or public relations costs.[6] For a primer on the importance of ensuring that both first- and third-party losses are covered, see *Camp's Grocery, Inc. v. State Farm Fire & Cas. Co.*, No. 4:16-CV-0204-JEO, 2016 WL 6217161 (N.D. Ala. Oct. 25, 2016)(distinguishing between first- and third-party coverage in the cyber-security realm and noting that the policy endorsement at issue did not "create, recognize, or assume the existence of a duty to defend or indemnify against claims brought by third parties.").

- Investigation and Remediation Costs:

Once a data breach has occurred, the insured entity must determine the cause and extent of the breach in order to fulfill reporting requirements, assess its exposure, and prevent future occurrences. Since this investigation can often be costly, businesses typically inquire pre-loss whether post-breach investigation costs are covered in any cyber-security policy. After the cause and extent of the data breach are determined, the system must be restored and any affected parties notified. These costs can include: a loss of business income or extra expenses in repairing the system; public relations costs; notification expenses; electronic data restoration/retrieval; costs associated with extortion demands; and changes to entities' policies and procedures to prevent future occurrences. [7]

- Legal Expenses:

As noted above, liability can arise from the breach of third-party information and can lead to lawsuits and regulatory fines. Such losses can include the disclosure of personally identifiable information and, in some cases, non-public private and confidential information; unauthorized access to third-party mainframe; and others. When such losses occur, they can lead to the publication of confidential materials, which in turn may lead to suits for defamation, slander, libel, and copyright infringement. [8] Of course, insureds look to their cyber-security policy to cover defense and indemnification costs when such claims arise.

Some additional considerations include:

- Limits and Sublimits:

Insured entities should also evaluate the limits and sublimits of a given policy in order to determine which policies best suit their needs. First-party coverages and indemnification costs and fines arising from third-party claims typically are offered as sublimits of the policy limit.[9] For example, a multi-million dollar policy may provide a sublimit of $100,000.00 for the investigation costs noted above, or similar sublimits for regulatory fines and penalties.[10] However, it should be noted that the landscape is continually changing, as some policies have increased sublimits or have done away with them entirely.[11]

Another issue businesses may consider involves "burning limits" or eroding coverage policies wherein legal costs to defend the claim "burn" or erode the policy limit. This may ultimately limit the amount of indemnity available, especially when the scope of loss is significant. Accordingly, businesses often consider the total amount of indemnity coverage when evaluating cyber-security insurance under a "burning limits" or eroding policy.

- Potential Exclusions:

Assuming an entity has evaluated and negotiated the scope of coverage, it should also consider any exclusions in the policy it ultimately acquires to ensure that the necessary coverages still apply in the event of a loss. For example, some policies exclude acts of foreign enemies, which could include cyber-attacks, particularly if it is determined that the attack occurred from foreign soil (or by domestic insurgents).[12] Similarly, businesses often wish to avoid exclusions related to software patch requirements, as coverage may be denied due to the fault of the software developer and not the insured entity. Additionally, certain policies differentiate between unauthorized access and the errant release of information by authorized users, covering the former but excluding the latter.[13] All of these are important factors in selecting a cyber-security policy. Likewise, it can be important to ensure that an entity's chosen consultants, vendors, independent contractors, and incident response teams are approved by the subject policy and/or its issuing carrier. [14] Additionally, certain policies may require that an entity's network be disabled for a certain period of time for certain coverages, such as business interruption costs, to trigger. [15]

Although not exhaustive, other potential exclusions may include: (1) certain aspects of third-party liability including costs/expenses resulting from forwarding malware by the insured; (2) damages related to employment discrimination, contractual liability, or theft of intellectual property; (3) losses to third-party systems out of the policyholder's control; (4) expenses for extortion or from an act of terrorism, war, or a military action; (5) collateral damage from a malware attack not directly aimed at the insured; (6) claims by related business entities of which the insured owns a certain percentage; (7) failure to timely disclose a loss; (8) damages from outsourcing data to certain countries; (8) claims on behalf of federal, state, or local governments;[16] and (9) claims for bodily injury or property damage when the damage occurs as the result of a cyber-security breach (*i.e.* hospital mainframes, transportation systems, engineering endeavors, etc.).[17]

In sum, entities should evaluate their risks and commercial needs and select a cyber-security policy and/or related endorsements accordingly. Importance should be placed on the above elements of coverage and an evaluation of whether certain exclusions may or may not apply. Another article in this issue addresses the problems and pitfalls entities face when they rely solely on a CGL policy for cyber losses.

---

[1] Monica Rodriguez, *Adidas Warns Millions of U.S. Customers About a Potential Data Breach*, FORTUNE (June 28, 2018), http://fortune.com/2018/06/28/adidas-warns-of-potential-data-breach/.
[2] *Id.*
[3] David Meyer, *What to Know About the Latest Data Breach Hitting Sears and Delta Customers*, FORTUNE (Apr. 5, 2018), http://fortune.com/2018/04/05/sears-delta-data-breach/.
[4] FED. TRADE COMM'N, *Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk?* (2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00012-141437.pdf.
[5] *Cyber Insurance: A key element of the corporate Risk Management Strategy*, DELOITTE (2017), https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_CyberInsurance_Noexp.PDF.
[6] *Id.*
[7] Louis D'Agostino, 5 Key Coverage Elements of a Comprehensive Cyber Insurance Program for Registered Investment Advisors, ALIGN (Oct. 24, 2017), https://www.align.com/blog/key-coverage-cyber-insurance.
[8] *Id.*
[9] Lauri Floresca, *Cyber Insurance 101: The Basics of Cyber Coverage*, WOODRUFF SAWYER (June 19, 2014), https://woodruffsawyer.com/cyber-liability/cyber-basics/.
[10] *Id.*
[11] *Id.*
[12] Louis D'Agostino, *supra.*
[13] *Cybersecurity Insurance—5 Critical Elements of Your Policy*, ZENSURANCE BLOG, https://blog.zensurance.com/five-elements-check-cybersecurity-insurance-policy/ (last visited July 16, 2018).
[14] Louis D'Agostino, *supra.*
[15] Lauri Floresca, *supra.*
[16] FED. TRADE COMM'N, *supra* at 15.
[17] *The Bodily Injury & Property Damage Gap In E&O And Cyber Policies*, GB&A INSURANCE, https://www.gbainsurance.com/BIPD-Insurance-Tech-Cyber-717 (last visited July 16, 2018).

Steptoe & Johnson PLLC's Insurance Company Team

Team Leaders
Laurie C. Barbe, *Member* Morgantown
304.598.8113 laurie.barbe@steptoe-johnson.com

Melanie Morgan Norris, *Of Counsel* Wheeling
304.231.0460 melanie.norris@steptoe-johnson.com

Team Members - West Virginia
Michelle Lee Dougherty, *Member* Wheeling
304.231.0442 michelle.dougherty@steptoe-johnson.com

Eric J. Hulett, *Member* Martinsburg
304.262.3519 eric.hulett@steptoe-johnson.com

Katherine MacCorkle Mullins, *Member* Charleston
304.353.8159 katherine.mullins@steptoe-johnson.com

Chelsea V. Prince, *Member* Morgantown
304.598.8174 chelsea.prince@steptoe-johnson.com

Ancil G. Ramey, *Member* Huntington
304.526.8133 ancil.ramey@steptoe-johnson.com

Richard M. Yurko, Jr., *Member* Bridgeport
304.933.8103 richard.yurko@steptoe-johnson.com

Michelle E. Gaston, *Of Counsel* Charleston
304.353.8130 michelle.gaston@steptoe-johnson.com

Hannah Curry Ramey, *Of Counsel* Huntington
304.526.8126 hannah.ramey@steptoe-johnson.com

Devon J. Stewart, *Of Counsel* Charleston
304.353.8188 devon.stewart@steptoe-johnson.com

Mark A. Moses, *Associate* Morgantown
304.598.8162 mark.moses@steptoe-johnson.com

Andrew P. Smith, *Associate* Huntington
304.526.8084 andrew.smith@steptoe-johnson.com

Team Members - Pennsylvania
Eric W. Santos, *Of Counsel* Southpointe
(724) 873-3188 eric.santos@steptoe-johnson.com

Meredith J. Risati, *Associate* Southpointe
(724) 749-3182 meredith.risati@steptoe-johnson.com

Team Members - Texas
Dawn S. Holiday, *Member* The Woodlands
281.203.5777 dawn.holiday@steptoe-johnson.com

Lyle R. Rathwell, *Member* The Woodlands
281.203.5722 lyle.rathwell@steptoe-johnson.com

Jason R. Grill, *Of Counsel* The Woodlands
281.203.5764 jason.grill@steptoe-johnson.com

Ed Wallison, *Of Counsel* The Woodlands
281.203.5766 ed.wallison@steptoe-johnson.com

Merris A. Washington, *Associate* The Woodlands
281.203.5759 merris.washington@steptoe-johnson.com

Fast Facts about Steptoe & Johnson

More than 300 attorneys

13 Offices in Colorado, Kentucky, Ohio, Pennsylvania, Texas, and West Virginia

More than 40 areas of practice

Defense of first party cases including suits asserting "bad faith" and allegations of unfair claim handling and settlement practices

Regulatory aspects of insurance, including consumer complaints and other administrative matters involving the Insurance Commissioner

95 lawyers recognized in *The Best Lawyers in America*®

Top listed firm in West Virginia in multiple areas by *The Best Lawyers in America*®, including Employment Law-Management, Labor Law-Management, and Litigation-Labor & Employment

Top listed in a number of litigation categories including Litigation, Corporate/Commercial Law, Environmental, Labor and Employment, Mergers and Acquisitions, Personal Injury and Products Liability by the authors of *The Best Lawyers in America*®

Top listed firm in Ohio, Pennsylvania, and West Virginia in a combination of areas by *The Best Lawyers in America*®

Three Fellows of the American College of Trial Lawyers

Three Fellows of the American College of Labor & Employment Lawyers

Follow us on Linkedin and Twitter