August 2015

Skadden

Privacy & Cybersecurity Update

Third Circuit Affirms FTC's Authority Over Cybersecurity

In the Wyndham case, the Third Circuit affirmed that the FTC has the authority to regulate cybersecurity under Section 5 of the FTC Act, and that the language of the act itself constituted fair notice to Wyndham that its practices may be unlawful.

In a highly anticipated ruling, the U.S. Court of Appeals for the Third Circuit has ruled unanimously that the Federal Trade Commission (FTC) has the authority to bring actions against companies alleging that cybersecurity activities constitute unfair trade practices under Section 5 of the FTC Act.[1] The August 24, 2015, ruling upheld the decision of the U.S. District Court for the District of New Jersey on two questions, namely: (i) whether the FTC has authority to regulate cybersecurity under Section 5 of the FTC Act, and (ii) if so, whether Wyndham had fair notice that its cybersecurity practices could violate Section 5. The Third Circuit affirmed the district court's findings that the FTC does have such authority and that Wyndham did have fair notice.

Background

The action began in 2012 when the FTC issued a complaint against Wyndham related to three separate data breach incidents that occurred between 2008 and 2009. The incidents exposed more than 600,000 consumer payment card numbers and led to more than $10.6 million in fraudulent charges. Rather than settle with the FTC, as numerous companies had previously done when faced with a similar complaint, Wyndham moved to dismiss the claim. Wyndham based its motion on three main arguments: (i) the unfairness standard under Section 5 of the FTC Act did not encompass unreasonable data security measures, (ii) the FTC had not given companies notice that unreasonable data security measures could be deemed an unfair trade practice, and (iii) the FTC's complaint did not sufficiently allege consumer injury as required by the FTC Act.[2] The district court rejected all of these arguments and denied Wyndham's motion to dismiss the complaint. Wyndham filed an interlocutory appeal, and in August 2014, the Third Circuit agreed to hear the case.[3]

[1] *Federal Trade Commission v. Wyndham Worldwide Corp. et al (3d Cir), No. 14-3514.*

[2] In its opinion, the Third Circuit noted that Wyndham did not request an interlocutory appeal on this third point, and so the court did not address it.

[3] For more detailed background on this case, see our *Privacy & Cybersecurity* updates from December 2013, February 2014, April 2014 and June 2014.

As reported in our March 2015 *Privacy & Cybersecurity Update*, during oral arguments, the Third Circuit seemed more skeptical of the FTC's positions than of Wyndham's. The court questioned whether the FTC was asking federal courts to declare, for the first time, that unreasonable cybersecurity practices were "unfair." The FTC ultimately conceded that if the court determined that the FTC had not yet declared those practices unfair, it was indeed asking the court to do so. The court also focused on the legislative history of the FTC Act, suggesting that the act could be interpreted to prevent the agency from bringing cases of first impression, like this one, into federal court without first going through the cumbersome administrative procedure of notice and rulemaking.

The Decision

Despite the court's focused questioning of the FTC during oral arguments, the court ultimately decided that Wyndham's arguments were not persuasive on any of the issues under consideration.

The FTC's Authority Over Cybersecurity

First, the court considered the scope of the FTC's regulatory authority under Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce, and says that an act may not be deemed unfair unless (i) it is likely to cause substantial injury to consumers, (ii) the injury is not reasonably avoidable by consumers, and (iii) the injury is not outweighed by benefits to consumers or competition. The court noted that Congress had explicitly considered, and then rejected, the notion that specific "unfair" practices should be enumerated in the act. Wyndham argued that the plain meaning of the word "unfair" imposes independent requirements that were not met in this case, such as injury through "unscrupulous or unethical behavior," which the court noted had already been rejected by the U.S. Supreme Court,[4] and "inequitable" practices by the company, to which the court responded that Wyndham's practices were, in fact, inequitable.

Wyndham also argued that its conduct could not be deemed unfair when Wyndham itself was the victim of criminal activity, but the court stated that a company's conduct need not be the proximate cause of the injury in order for the company to be liable for foreseeable harm. In the Wyndham case, the court noted that Wyndham could not plausibly argue that the second and third attacks were unforeseeable. Significantly, the court went on to say that conduct could be unfair even before an actual injury occurs.

Next, Wyndham argued that even if Section 5 originally covered cybersecurity, three subsequent legislative acts (an amendment to the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act and the Children's Online Privacy Protection Act) directing the FTC to take certain actions to safeguard consumer privacy online would be inexplicable if the FTC already had general authority to regulate cybersecurity. The court rejected this argument, noting that the three cited acts required the FTC to issue certain regulations, rather than authorizing it to do so. The court also rejected Wyndham's argument that prior statements by the FTC acknowledged that the FTC lacked authority in this area, saying that the FTC had acknowledged only that it lacked the ability to regulate certain aspects of companies' conduct, such as the amount of information that they collect.

Fair Notice

Having found that the FTC does have the authority to deem a company's cybersecurity practices unfair under the FTC Act, the court next examined Wyndham's argument that it did not have fair notice that its practices could violate Section 5. The court first considered the appropriate legal standard to apply to the notice required in this case. Wyndham asserted that it was entitled to "ascertainable certainty" of the specific cybersecurity practices required by Section 5, since the "ascertainable certainty" standard applies to conduct legally required by a civil regulation. The court rejected this assertion, noting that Wyndham itself had, on numerous occasions, pointed out that the FTC has not issued any regulations with respect to cybersecurity and that, as a result, the federal courts must interpret the meaning of Section 5 in the first instance (which is consistent with the FTC's responses during oral arguments). As such, the court focused on the question of whether Wyndham had fair notice of what the statute (rather than the FTC's interpretation of the statute) requires. The applicable legal standard for this approach is whether the statute is not "so vague as to be no rule or standard at all."

In considering whether Section 5 is impermissibly vague, the court cited the portion of Section 5 that asks whether the practice at issue is likely to cause substantial injury to consumers that cannot reasonably be avoided and that is not outweighed by benefits to consumers or competition. The court stated that this language informs parties that the relevant inquiry is a cost-benefit analysis. Accordingly, while acknowledging that this is not precise guidance, the court found that Section 5 is sufficiently specific in its requirements.

The court acknowledged that there could be borderline cases where it would be less clear whether a company's conduct was unfair or not, but noted that "under a due process analysis a company is not entitled to such precision as would eliminate all

[4] *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233 (1972).

close calls." Moreover, the court found that this particular case was not even a close call. Wyndham did not attempt to argue that its practices survive the application of a cost-benefit analysis. Indeed, according to the FTC's complaint, Wyndham failed to use any firewalls, did not restrict IP addresses at all, did not use any encryption for certain customer files and did not require some users to change default passwords. In addition, the court noted that Wyndham actually did have notice that its practices were unlikely to survive the cost-benefit analysis in the form of the 2007 FTC guidebook titled "Protecting Personal Information: A Guide for Business,"[5] which advised against many of Wyndham's practices and, in the form of the consent decrees, related to cybersecurity that were published on the FTC's website. With respect to the latter, the court acknowledged in a footnote that it may be unfair to expect that in 2008, parties were routinely examining consent decrees, but noted that Wyndham did not argue that it was unaware of the consent decrees, only that the consent decrees did not provide fair notice of the requirements.

Takeaways

There are several important takeaways from the ruling:

- Companies should be asking themselves whether their cybersecurity practices could reasonably be said to survive the cost-benefit analysis cited by the court, by weighing the risks to their consumers presented by their cybersecurity practices against the benefits of such practices to consumers or competition. The court also suggested that the actual costs of cybersecurity practices could be taken into account.
- If they have not done so already, companies should consider whether their practices conform with the guidance in the FTC's 2007 data security guidebook. For example, companies should not retain customer credit card information after the business need for such information has passed and should not store sensitive information on a computer with an Internet connection.
- Companies should be mindful that, particularly given the current awareness of cybersecurity risks, the fact that the company was a victim of a cybersecurity attack will likely not be viewed by the FTC or the courts as a defense to liability. Further, the court's statements regarding the foreseeability of the attacks on Wyndham suggest more broadly that companies should expect that third parties will attempt to obtain unauthorized access to their systems and act accordingly.

Concluding Thoughts

While the Wyndham case supports the FTC's authority to bring Section 5 cases for cybersecurity shortcomings, Wyndham's alleged practices were so egregious that the ruling still leaves a fair amount of uncertainty for companies that employ certain cybersecurity safeguards but not others. For example, companies that install firewalls but do not use robust encryption, or that have policies requiring individuals to change default passwords but no procedure to enforce the policy, may have a difficult time deciding whether their practices would survive the cost-benefit analysis. Companies may never get such additional guidance since, as the Third Circuit noted, "a company is not entitled to such precision as would eliminate all close calls."

It remains to be seen whether the FTC will view the Third Circuit's ruling as a green light to be more aggressive in bringing actions against companies for unfair cybersecurity practices, although there has been nothing to suggest that the FTC has been holding back on cybersecurity enforcement actions pending this decision. Nonetheless, it will be interesting to see whether the FTC begins to allege that a company's cybersecurity practices are unfair even in the absence of a data breach.

Return to Table of Contents

D.C. Circuit Vacates and Remands District Court Decision That Found NSA Metadata Collection Likely Unconstitutional

In *Obama v. Klayman*, the D.C. Circuit removed the preliminary injunction on NSA bulk metadata collection put in place by the district court.

On August 28, 2015, the U.S. Court of Appeals for the District of Columbia Circuit issued its decision in *Obama v. Klayman*, overturning the preliminary injunction on government collection of bulk metadata by the National Security Agency (NSA) that had been put in place by Judge Richard Leon in 2013. The injunction, which had been stayed pending appeal, was based on Judge Leon's finding that the plaintiffs had a substantial likelihood of showing that the collection program constituted an unreasonable search under the Fourth Amendment. The circuit court panel did not agree that that threshold test for injunctive relief had been met, given plaintiffs' limited showing of evidence that they, in particular, had been targeted by the NSA program, and vacated the injunction accordingly. However, each of the three members of the panel had a different opinion on the question of the plaintiffs' standing to bring suit against the program, with two of three members of the panel agreeing to remand to the district court for further proceedings.

[5] The guidebook is available here.

Background

As noted in our June 2015 *Privacy & Cybersecurity Update*, the NSA program first came to light in June 2013 based on information leaked by former government contractor Edward Snowden. The information Snowden provided and certain statements from the NSA revealed that a number of telecommunications operators have been ordered by the Foreign Intelligence Surveillance Court to produce telephone metadata for calls within the U.S. or from the U.S. to foreign points on a daily basis. The government then queries the resulting metadata for information that it suspects is related to specific terrorist organizations.

The NSA collection has been undertaken pursuant to authority granted to the government under Section 215 of the USA Patriot Act. In May 2015, the U.S. Court of Appeals for the Second Circuit, in *ACLU v. Clapper*, vacated a district court decision upholding the program and found that the NSA collection program was not permitted under Section 215. However, Congress subsequently passed the USA Freedom Act in early June 2015, in part to reform those Section 215 collection authorities. The new law effectively reinstates Section 215 for 180 days to permit an orderly wind-down of the program and allow the intelligence agencies to prepare for the new legal collection regime. As a result, Director of National Intelligence James Clapper announced in July 2015 that analytic access to historical metadata collected under Section 215 will cease on November 29, 2015.

The Decision

In *Klayman,* the court first issued a brief *per curiam* decision indicating that despite the expiration of the original Section 215, the court did not view the question of the constitutionality of the collection program as moot. At a minimum, the court stated, as long as collection and analysis continues under Section 215, the plaintiffs and the government stand in the same positions that they did before the Freedom Act was passed.

Each of the three panel judges then provided a separate analysis of the plaintiffs' standing and likelihood of success in bringing the cause of action. Judges Janice Rogers Brown and Stephen Williams separately concluded that the plaintiffs had not met the burden of proof required for a preliminary injunction with regard to standing, but had established enough of a case for the district court to explore on remand through limited discovery. However, the two differed on the sufficiency of the plaintiffs' case to date. Brown stated that Klayman had demonstrated more specific knowledge of government surveillance practices than had been shown in *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013) (in which the Supreme Court dismissed a case against the NSA's warrantless wiretapping under the FISA Amendments Act for lack of standing) and thus had already met the "bare requirements" of standing. Williams argued that this more specific knowledge of government surveillance practices was not a substitute for a showing of specific targeting of the plaintiffs themselves, suggesting that the plaintiffs still face an uphill battle in making the latter showing. Judge David Sentelle, meanwhile, suggested that Clapper's dismissal of a similar cause of action was directly applicable, and the plaintiffs' case should be dismissed outright for failure to demonstrate injury.

Next Steps

The case now returns to the district court, where it faces significant obstacles. Both judges who supported the remand also acknowledged the government's legitimate interest in restricting access to information about surveillance programs. As such, they acknowledged that the facts required to show standing may ultimately not be possible for plaintiffs to establish, demonstrating once more the difficulty of obtaining clear judicial guidance on secret government programs. Moreover, the court remained silent on the continued viability of the case once the NSA ceases directly collecting bulk metadata under Section 215 in November 2015; the end of the NSA program may well render the issue moot. Like the plaintiffs in both *Clapper* cases before them, the *Klayman* plaintiffs may find that their case has more of an impact on the public discourse than traction in the courts.

Return to Table of Contents

Fiat Chrysler Recalls 1.4 Million Vehicles Amid New Concerns About Car Hacking

Two hackers executed a successful remote hack on a Jeep Cherokee, leading to a recall by Fiat Chrysler amid various efforts to address vehicle cybersecurity, including the introduction of new legislation and auto industry standards.

An unauthorized demonstration performed on a Jeep Cherokee that was detailed in an article in Wired magazine highlighted concerns regarding the ability to hack remotely into a vehicle's systems and culminated in Fiat Chrysler recalling approximately 1.4 million vehicles.

On July 21, 2015, Andy Greenberg published an article in Wired[6] detailing how the Jeep Cherokee he was driving at 70 mph down a St. Louis highway had begun to act on its own — the air conditioning blasted cold air, the radio blared rap music and the windshield wipers began spraying wiper fluid and swiping back and forth, all without Greenberg touching the controls.

[6] The article is available here.

The situation escalated rapidly when the transmission cut out with traffic bearing down on him. Greenberg was aware that 10 miles away, two hackers — Charlie Miller, a Twitter employee, and Chris Valasek, head of vehicle research at IOActive — were testing their research on vehicle hacking with Greenberg as the driver. They claimed they would have been able to kill the engine completely had they wished to.

In the summer of 2013, Miller and Valasek demonstrated that they were able to take control of a Ford Escape and Toyota Prius by wiring their PC to the vehicle's onboard diagnostic port (used by technicians to access the vehicle's electronic systems). When the hackers demonstrated their research at a hacking conference, the general public was not overly alarmed because the hackers needed physical access to the vehicle to exert control over it. After the 2013 conference, Miller and Valasek set out to prove that remote hacking was possible. Valasek realized that they could remotely hack the Jeep through a vulnerability in the vehicle's Internet-connected computer.

The hacking team issued a report in August 2014 detailing their methods, findings and recommendations.[7] In order to meet consumer demand for increased connectivity and unique safety features, manufacturers have increased the number of computer components (Electronic Control Units or ECUs) in vehicles and the ECUs' ability to communicate internally and with the outside world. Safety features such as adaptive cruise control, collision prevention systems and lane-keep assist have become increasingly popular and may make it easier for hackers to take physical control over a vehicle since they require connectivity to systems outside the vehicle.

Even given increased use of ECUs, Miller and Valasek note in their report that vehicles are not easy to hack, as the hack of the Jeep took significant work and the work would not easily apply to vehicles manufactured by other companies. Still, their success has clearly demonstrated that the increased connectivity and complexity of vehicle features is paired with increased risk, especially if manufacturers do not focus on bolstering the security of the vehicles when they add the more vulnerable features. In response to Miller and Valasek's hack of the Jeep, Fiat Chrysler issued the recall of 1.4 million vehicles so it could update the software in the vehicles.

Miller and Valasek proposed several technical solutions that manufacturers should implement such as securing remote endpoints, mitigating the ability for hackers to inject Controller Area Network (CAN) messages on an ECU and designing automotive networks that isolate ECUs with remote functionality. They also noted that manufacturers need to have a method to automatically and remotely patch vehicles to address any newly identified security weaknesses. (Recall notices for the 2010 Ford Escape and 2010 Toyota Prius required the vehicles to be brought to a dealership to be updated following the 2013 hacking disclosures.)

In addition to the recalls, in late July, Sens. Ed Markey and Richard Blumenthal introduced the Security and Privacy in Your Car Act of 2015 (SPY Car Act) to the U.S. Senate.[8] The SPY Car Act charges the Federal Trade Commission and National Highway Traffic Safety Administration (NHTSA) with enforcing cybersecurity standards on vehicle manufacturers. The SPY Car Act states that vehicles manufactured in the U.S. must be "equipped with reasonable measures" to protect against hacking attacks, including isolating critical software systems that affect a driver's control over a vehicle from noncritical software systems. If the SPY Car Act is passed, the FTC and NHTSA would have three years to develop final regulations to carry out the act, and manufacturers would have two years to comply with those standards. In addition, manufacturers would be required to affix standardized labels to vehicles detailing the extent to which the vehicle protects the cybersecurity and privacy of the vehicle's owners and occupants.

In addition, the Alliance of Automobile Manufacturers and the Association of Global Automakers recently adopted a set of privacy principles that address some of these same issues, primarily those related to data collection and use.[9]

It remains to be seen whether there will be a legislative solution, or whether the auto industry will rely on self-regulation to address cybersecurity vulnerabilities in vehicles. Either way, these developments are indicative of increasing concern regarding these issues by consumer advocates and the auto industry.

Return to Table of Contents

Target Reaches Settlement With Visa

Target has reached a $67 million settlement with Visa to reimburse Visa's issuing banks for losses sustained as a result of Target's 2013 data breach.

Target Corp. has reached an agreement with Visa Inc. to settle certain claims arising from Target's 2013 data breach. Under the agreement, Target may be liable for up to $67 million to reimburse banks issuing Visa cards for costs incurred in connection with the data breach, such as the cost of issuing new cards and increasing staffing at call centers to field customer inquiries.

[7] The report is available here.

[8] See our February 2015 *Privacy & Cybersecurity Update* for a discussion of Markey's report "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk."

[9] See our November 2014 *Privacy & Cybersecurity Update* for a summary of these principles.

In December 2013, Target announced that over a period of more than three weeks during the holiday shopping season, computer hackers stole credit and debit card information for approximately 110 million Target customers by installing malware on Target's computer servers. Lawsuits were filed on the heels of the announcement and consolidated into a multidistrict litigation in Minnesota, consisting of two types of claims: those brought by consumers and those brought by financial institutions who provided credit to consumers and issued their payment cards. The consumer claims were settled in March 2015 for $10 million,[10] but the claims brought by financial institutions are ongoing.[11]

Visa has said that its largest issuing banks have already approved the deal with Target. A tentative deal reached between Target and MasterCard for $19 million was scuttled in June when it was not accepted by a sufficient number of MasterCard issuing banks. Target continues to work on a deal with MasterCard and has said such a deal will be made on "comparable economics," which means it will likely result in a settlement amount significantly higher than $19 million.

The settlement with Visa might be used as a benchmark in future claims by issuing banks arising out of payment card data breaches and demonstrates that merchants that accept credit cards may be liable to issuing banks for significant damages. These damages may be higher than those paid out to consumers, in part because the issuing banks can often more easily point to actual damages suffered as a result of the breach.

Return to Table of Contents

FTC to Improve Technology Expertise

The FTC has announced its intention to improve its technology expertise.

Federal Trade Commissioner Julie Brill said in August at a meeting of the National Academies of Sciences, Engineering and Medicine's Forum on Cyber Resilience that the FTC is actively seeking to improve its technology expertise.

The FTC has continued to focus on technology and cybersecurity-related issues impacting consumers, as evidenced by the report the FTC released in January detailing its privacy and security expectations for companies developing internet-connected devices.

However, Brill noted that the FTC staff is largely comprised of lawyers and economists, and lacked technology expertise. More recently, Ashkan Soltani, the FTC's current chief technologist (a position created relatively recently) has been leading efforts to hire more technologists and dedicated technology staffers. The FTC also has emphasized the importance of hiring young technology-savvy lawyers.

Return to Table of Contents

FTC Enters Safe Harbor Compliance Settlements

Thirteen companies have settled claims by the FTC that the companies falsely claimed safe harbor certification, either by failing to obtain or renew certification.

Thirteen companies that were alleged to have violated the FTC Act by falsely claiming to have a current certification in the U.S.-E.U. or U.S.-Swiss Safe Harbor Frameworks agreed to settle with the Federal Trade Commission in August. Safe Harbor certification allows a U.S. company to receive personal information from the E.U. or Switzerland in compliance with the data protection laws of the E.U. member states and Switzerland. The frameworks each require that a company make an annual self-certification to the Department of Commerce. The self-certification requires that a company state that it complies with the EU's adequacy standard, which consists of seven privacy principles: notice, choice, onward transfer, security, data integrity, access and enforcement. After self-certifying, a company can communicate to consumers that it complies with the Safe Harbor Frameworks and may display a certification mark on its website.

The 13 companies against which the FTC alleged violations had either not renewed such certifications or had never applied for certification. Administrative complaints are issued by the FTC when the commission has "reason to believe" that the FTC Act has been or is being violated and a proceeding would be in the public interest. The proposed settlement agreements will prohibit the companies from misrepresenting the extent to which they participate in any government-sponsored or self-regulatory privacy or data security program.

The administrative complaints issued against these 13 companies, and the proposed settlement agreements, demonstrate the importance of ensuring a company's actual compliance with the self-certification requirements and of diligently applying for re-certification each year.

Return to Table of Contents

[10] See our March 2015 *Privacy & Cybersecurity Update* for a summary of the consumer claim settlement.

[11] See our September 2014 *Privacy & Cybersecurity Update* for a summary of the claims made by the financial institutions.

Brokers Report Increased Demand for Cyber Insurance

Recent reports by Marsh & McLennan and AON demonstrate an increased demand for cyber insurance across a number of industries.

Insurance brokers Marsh & McLennan Companies and AON Risk Solutions each recently reported a strong increase in demand for cyber insurance coverage across companies of all types and sizes.[12] It has been reported elsewhere that the annual gross written premium for the U.S. cyber risk market alone may now be as high as $2.75 billion. As the frequency, severity and sophistication of cyberattacks continue to escalate, this upward trend is likely to continue as more and more companies consider cyber insurance as one component of a comprehensive risk management plan.

According to the Marsh report, 16 percent of US-based Marsh clients purchased standalone cyber insurance in 2014, a 32 percent increase over 2013. Gains were seen across-the-board, with data-rich industries having the largest take-up rates: health care (50 percent); education (32 percent); hospitality and gaming (26 percent); services (22 percent); financial institutions (21 percent); power and utilities (21 percent); retail/wholesale (18 percent); communications, media and technology (12 percent); and manufacturing (8 percent).

The AON report, which is based on surveys of companies around the world, similarly reported that 21 percent of respondents said their companies purchased cyber insurance coverage, while 18 percent intend to do so. The following industries had the largest take-up rates: health care (57 percent); retail trade (50 percent); banks (49 percent); telecommunications and broadcasting (42 percent); technology (39 percent); insurance, investment and finance (35 percent); hotels and hospitality (35 percent); educational and nonprofits (32 percent). Organizations in North America were most likely to procure cyber coverage at 42 percent.

Market capacity varied by industry according to the Marsh report. Most industries were able to purchase aggregate cyber insurance limits in excess of $200 million, though certain perceived high-risk industries, such as retailers and financial institutions, reportedly faced a more challenging market. At present, more than 30 insurers appear to be offering cyber coverage, a number likely to rise as the insurance industry obtains a better understanding of these risks. In addition, the recent entrance of Berkshire Specialty into the excess cyber market is seen by many as a welcome development and should serve to further stabilize, if not increase, excess capacity.

Marsh also reported an overall increase in the amount of cyber insurance limits being purchased, a 22 percent uptick in 2014 for companies with revenues of $1 billion or more. Of the companies that purchased cyber insurance, program limits averaged $12.8 million, varying by industry and company size. Companies with revenues of $1 billion-plus averaged $34.1 million in coverage, with financial institutions ($57 million); power and utilities ($44.4 million); communications, media and technology ($43.7 million); and services ($41.2 million) leading the way.

Premium volatility for both primary and excess layers also trended higher according to the Marsh report, with rate increases fluctuating between 2.3 and 4.2 percent throughout 2014. Certain insureds, including retailers, faced particular pricing challenges with increases between 5 and 10 percent. This is undoubtedly due to increased claim frequency and severity in certain sectors (and surrounding media coverage) and the heightened perceived risk.

Takeaways

There is no right or wrong answer as to whether any particular company should procure standalone cyber insurance and, if so, how much. However, what is clear is that more and more companies are approaching cyber exposures like any other more traditional risk by adding cyber coverage to their insurance programs. Poised to tap into this growing and rapidly evolving market, insurers have responded with various products, and capacity appears to be stabilizing if not increasing. As additional and more accurate loss data are obtained and insurers become more comfortable in the cyber arena, premium volatility should eventually level off as well.

Return to Table of Contents

[12] *See* Marsh & McLennan Companies, "Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise," Mar. 2015; AON Risk Solutions, "2015 Global Risk Management Survey."

Contacts in the Privacy and Cybersecurity Group

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Cyrus Amir-Mokri
Partner / New York
212.735.3279
cyrus.amir-mokri@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000