Skadden

Privacy & Cybersecurity Update

President Trump Appoints Acting FTC Chair With Narrower View of FTC Authority; Vacancies Remain to Be Filled

President Donald Trump has appointed an acting FTC chair, who has advocated a more restrained approach to cybersecurity matters. With the current chairwoman resigning from the commission in February, three vacancies will remain.

On January 25, 2017, President Trump designated Maureen K. Ohlhausen as the acting chairwoman of the Federal Trade Commission (FTC). Ohlhausen, a Republican and President Barack Obama appointee, was sworn in as a commissioner in 2012. She previously has advocated for regulatory restraint and criticized the commission's ex ante approach to lawmaking. The current chairwoman, Edith Ramirez, announced in January that she would be leaving the FTC on February 10, 2017. President Obama appointed Ramirez as an FTC commissioner in April 2010, and she later became chairwoman in March 2013. During her tenure at the FTC, Ramirez prioritized actions protecting consumers and regulating technology.

With Ramirez's resignation, the five-member commission will be down to two commissioners, and President Trump will have the opportunity to nominate the other three. While new commissioners are subject to Senate confirmation, the president appoints an existing commissioner to be the chairperson without further Senate approval. Confirmed commissioners are appointed to seven-year terms and no more than three members may be from the same political party. The Obama administration did not nominate successors for the other two vacant seats, which became vacant in August 2015 and March 2016.

Acting Chairwoman Supports a Narrower Approach to Cybersecurity

In a statement released by the commission, Ohlhausen indicated several priorities, including an effort to "minimize the burdens on legitimate business." Throughout Ohlhausen's term as a commissioner, she has advocated for regulatory restraint and criticized the commission's ex ante approach to lawmaking.

Ohlhausen's stance on the direction of the FTC leaves some questions about the commission's future regulations of the privacy and cybersecurity space. The FTC is a consensus-driven organization, so the chairperson does not solely control the commission's actions. However, with three of five seats open, and only one needing to be filled by a Democrat, President Trump will have the opportunity to select commissioners who share Ohlhausen's views. Ohlhausen's appointment likely will mean that FTC regulations will be more exacting and based on proof of substantial and real harm to consumers, suggesting a reduction in ex ante rulemaking.

Effect on Businesses

For companies under FTC jurisdiction, Ohlhausen's appointment may signal a more business-friendly regulatory future. While the FTC has a mandate to protect consumers and their privacy, Ohlhausen has advocated publicly for "regulatory humility," a principle she has coined in recognition of the inherent limitations of regulation. For example, Ohlhausen has voiced criticism of certain prescriptive guidelines published by the FTC, such as the commission's 2016 report "Big Data: A Tool for Inclusion and Exclusion." The report warned that some uses of big data may create unfair social biases that would adversely affect vulnerable, low-income and disadvantaged consumers. While lauding the report, Ohlhausen issued a separate statement expressing concerns that the report failed to take into account market and economic forces, and was distracted by hypothetical harms. Ohlhausen also issued a separate statement in response to the commission's report on the internet of things, noting her opposition to baseline privacy legislation and the commission's allegedly unsubstantiated recommendation for data minimization.

A common thread throughout her public critiques has been her hesitation to regulate areas of hypothetical harm to consumers and a desire to refocus the commission on regulation based on genuine, substantial harms. Speaking at the January 2017 State of the Net Conference, Ohlhausen suggested that if tapped to be the FTC chair, she would begin an effort to define substantial harm. In recent interviews, Ohlhausen has stressed that regulatory enforcers should tread carefully in the intellectual property space generally and has advocated for a less broad and more transparent interpretation of the FTC's authority under Section 5 of the FTC Act, which provides the FTC with jurisdiction to regulate cybersecurity and consumer privacy.

Key Takeaways

Acting Chairwoman Ohlhausen's public dissents and critiques of previous FTC actions — together with the prospect of three new presidential nominees to the commission — suggest that the FTC will be taking a narrower view of its own authority to establish and enforce privacy and cybersecurity requirements, especially with respect to what constitutes sufficient consumer harm for the FTC to take action. Companies that collect and use data should watch closely for indications of the FTC's direction over the next few years.

Return to Table of Contents

Massachusetts Makes Data Breach Reports Publicly Available Online

A new Massachusetts initiative increases the public's access to information regarding companies' data breaches. The change could have far-reaching implications for cybersecurity efforts both within and outside the state.

The Massachusetts Office of Consumer Affairs and Business Regulation started 2017 with a push to make cyberattacks more transparent to the public. On January 3, the office announced that it would make reports of potential identity theft available on its website. Previously, an individual only could obtain these reports through a public records request. Ironically, because the ease of access to this information raises the specter of greater adverse publicity for companies that have experienced data breaches, the new policy actually may discourage companies from reporting breaches under Massachusetts law.

Disclosure of Breaches

Massachusetts state law requires any company that maintains or stores personal data about Massachusetts residents to notify state officials and affected residents if the company knows or has a reason to know of a security breach or unauthorized access to personal data.[1] Under the new policy, the Office of Consumer Affairs and Business Regulation has begun posting spreadsheets using the information it has received through these notifications. The spreadsheets detail data breaches that affected Massachusetts residents from 2007 to 2016 and reveal the organization involved, the date the breach was reported, whether the breach involved electronic or paper records, the number of residents affected and the type of information that was compromised (*e.g.*, social security number, account number, driver's license, or credit or debit card numbers). In addition, the publicly available reports indicate whether the data was encrypted and whether the organization provided credit monitoring.[2]

[1] M.G.L.c. 98(H).

[2] The data breach reports can be found here.

Potential Implications

The greater accessibility of this information may lead companies to increase their privacy efforts and lead to the development of industry standards in this area. For example, although Connecticut is the only state to require companies to offer free credit monitoring services to state residents who are victims of data breaches, many companies do offer such services following a security incident. With Massachusetts publishing which companies offered credit monitoring, there may be a greater incentive for companies to provide this service as a matter of course. In addition, there may be greater support for companies to encrypt personal data, because the spreadsheets highlight which companies use this additional security effort.

Although increased public awareness might benefit consumers, putting companies in the spotlight following a data breach also may have some downsides. For example, the increased publicity might cause companies to be wary of disclosing data breaches to Massachusetts residents if they are not legally required to do so.

De Facto National Database?

The Massachusetts data has the potential to become a *de facto* national database on data breaches. To date, no other state has followed Massachusetts in making data breach reports public. However, very few data breaches are limited to residents of one state, and many of the companies identified in the Massachusetts reports are national and international organizations. As a result, the Massachusetts reports will provide consumers, security experts and litigators with information about nationwide (and even global) data breaches and data practices.

Key Takeaways

The Massachusetts decision to make information about data breaches more readily available may help consumers gain information about these events, but it also may make companies more wary of reporting them. Whether companies will become more aggressive in challenging the scope of their disclosure obligations remains to be seen.

Return to Table of Contents

FTC Files Complaint Against D-Link in its Effort to Increase Privacy in Internet-of-Things Devices

The FTC has filed a complaint against D-Link, alleging that the internet-of-things device manufacturer put consumers' privacy at risk, despite assurances of its products' security.

On January 5, 2017, the FTC filed a complaint against internet-of-things (IoT) device manufacturer D-Link, alleging unfair and deceptive business practices in violation of Section 5 of the FTC Act.[3] This is the third action against a device manufacturer that the FTC has taken relating to IoT. The complaint against D-Link highlights how critical it is for IoT businesses to ensure sufficient safety precautions for their consumer products.

Background on D-Link

D-Link designs, develops, markets and manufactures networking devices such as routers and internet protocol (IP) cameras. IP cameras are devices, such as baby monitors and home security cameras, that stream a signal over the internet so users can view them remotely. According to the complaint, D-Link's products had widely been reported to have security flaws. Despite the reports, D-Link assured its customers of its products' safety. From 2013-15, because of the negative press reports, D-Link posted a "Security Event Response Policy" on its website, stating that D-Link prohibits "any intentional product features or behaviors which allow unauthorized access to the device network." In addition, D-Link emphasized the security of its products through various promotional statements on its website describing the security of its routers and cameras. Finally, D-Link presented its "graphical user interface" (GUI), which requires users to set up a password to begin using the router or camera, as a security feature.

The FTC's Complaint

The FTC complaint claims that, despite D-Link's assertion of security measures to its customers through the Security Event Response Policy, promotional materials and GUI "security" feature, the company failed to take reasonable steps to protect its routers and IP cameras from widely known and reasonably foreseeable risks of unauthorized access, leaving thousands of consumers at risk.

In particular, the FTC alleged that D-Link failed to:

- protect against software security flaws, such as "hard-coded" user credentials and other backdoors, and command injection flaws, which would allow remote attackers to gain control of consumers' devices;
- maintain the confidentiality of the private key it used to sign into its software, resulting in the exposure of the private key on a public website for approximately six months; and
- secure users' mobile app login credentials, and instead stored those credentials in clear readable text on users' mobile devices.

[3] The complaint is available online here.

The complaint alleges that D-Link engaged in both unfair and deceptive business practices under the FTC Act. The unfair business practice claim is based on D-Link's failure to take reasonable steps to secure the software for its routers and IP cameras. The deceptive business practice claim is based on the various statements D-Link made in its marketing materials and Security Event Response Policy regarding the security of its products.

FTC Efforts in Relation to the Internet of Things

The complaint against D-Link demonstrates that the FTC intends to remain diligent in protecting consumer privacy in the IoT age. It is the third complaint the FTC has filed against device manufacturers for poor security measures. The first, in 2014, was against TRENDnet, a California company that sold similar networking devices, for failing "to provide reasonable security to prevent unauthorized access to sensitive information, namely live feeds from the IP cameras." TRENDnet settled, and the FTC approved a final order in early 2014 requiring the company to establish a comprehensive information security program and to obtain third-party assessments of its security programs every two years for the following 20 years.[4]

In its second effort, in 2016, the FTC charged ASUSTeK, a Taiwanese hardware manufacturer that sells routers and related software and services, with failure to provide reasonable security in the design and maintenance of software it developed. ASUSTeK also settled. Similar to the agreement reached with TRENDnet, the final order required ASUSTeK to establish and maintain a comprehensive security program that would be subject to independent audits for the following 20 years.

Implications for Device Manufacturers

Following the massive attack on IoT devices in October of 2016 that temporarily disrupted legitimate internet activity, IoT device manufacturers reportedly have been redoubling their efforts to protect their products. An increased threat of FTC scrutiny over these devices will provide still greater incentives for these companies.

According to Jessica Rich, director of the FTC's Bureau of Consumer Protection, "hackers are increasingly targeting consumer routers and IP cameras [...] When manufacturers tell consumers that their equipment is secure, it's critical that they take the necessary steps to make sure that's true."[5] The three suits in the past three years demonstrate that failure to do so can result in an FTC complaint.

In order to prevent accusations of insufficient security measures, companies can adopt the FTC best practices, including:

- building security into devices at the outset, rather than as an afterthought, in the design process;
- when a security risk is identified, considering a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk; and
- considering measures to keep unauthorized users from accessing a consumer's device, data or personal information stored on the network.

So long as the FTC deems itself a watchdog for consumers' privacy in the IoT, companies should take security precautions seriously to avoid FTC action.

Return to Table of Contents

OCR Announces Settlement of First Action Under its Untimely Breach Notification Rule

The Department of Health and Human Services announced a settlement of its first enforcement action under the HIPAA Data Breach Notification Rule.

On January 9, 2017, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) announced it had entered into a settlement with Presence Health (Presence) related to violations of the breach notification requirements of the Breach Notification Rule (rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[6] Presence agreed to pay $475,000 after failing to give notice of a breach of unsecured protected health information (PHI) within the timeframes described in the rule. Presence also has agreed to take corrective action to protect such information in the future. The case against Presence was the OCR's first enforcement action under the rule.

On January 31, 2014, the OCR received a breach notification from Presence. As one of the largest health care networks serving Illinois, Presence operates approximately 150 facilities, including hospitals, physicians' offices, health care centers, and long-term care and senior living facilities. The breach notification indicated that on October 22, 2013, Presence discovered that paper-based operating room schedules containing the PHI of 836 individuals were missing from one of Presence's medical centers.

[4] For more information on the TRENDnet, Inc. case, see our October 2013 edition of *Privacy and Cybersecurity Update*, available here.

[5] Press Release, FTC, "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras" (January 5, 2017), can be found here.

[6] The OCR's announcement is available here.

The schedules included the affected individuals' names, dates of birth, medical record numbers and information about medical procedures. The OCR's investigation found that Presence failed to follow the Breach Notification Rule's requirements that institutions notify the affected individuals, prominent media outlets (which is required for breaches affecting 500 or more individuals) and the OCR of the breach without unreasonable delay and within the required 60 days of discovery.

Key Takeaway

As data breach notification requirements continue to flow from state legislators and federal and state regulators, companies should ensure they have procedures in place to meet their notification obligations.

Return to Table of Contents

NIST Updates Cybersecurity Framework, Calls for Comments

The National Institute of Standards and Technology has issued an update to its cybersecurity framework, which has become a key cybersecurity assessment tool for regulators.

On January 10, 2017, the National Institute of Standards and Technology (NIST) issued an update[7] to its voluntary risk-based cybersecurity framework (the framework). While the framework initially was intended to help operators of critical infrastructure to manage cybersecurity risk, it has since been adopted by many different organizations nationally and internationally as a standard with which organizations should or must comply. The updated framework incorporates feedback NIST received since its initial release. Matt Barrett, NIST's program manager for the framework, also noted that the updates aim to make the document easier to use while maintaining its voluntary and flexible nature.

Key Updates

While the framework remains substantively unchanged, new details have been added to clarify key cybersecurity concepts, address supply chain management and improve internal communication of cybersecurity issues.

The updated framework also discusses supply chain risk management and includes a vocabulary to allow collaborators to more easily work together in coordinating cybersecurity efforts. For example, the framework updated the different tiers of risk profiles to reflect supply chain management considerations, including by describing that a tier four organization (the highest level) would be one that can "quickly and efficiently" manage emerging cyber supply chain risks and implement formal and informal arrangements with its suppliers, partners, and individual and organizational buyers to manage risk.

In addition, the framework noted that all the stakeholders in the supply chain have an interest in communicating and verifying their cybersecurity requirements. One way stakeholders can manage supply chain risk is to implement formal agreements regarding cybersecurity requirements, communicate how the cybersecurity requirements will be verified and validated, and govern and manage those activities.

The framework also revised its "How to Use" section by further explaining how organizations can use the framework throughout the lifecycle of a cybersecurity program. For example, the framework noted it is best for organizations to work to meet the outcomes prioritized in their risk profiles during the development or build phase, or the purchase or outsourcing of the system during the buy phase. The framework also noted that outside of these time frames, it will continue to be useful to organizations, as an occasional reassessment tool, to verify that the cybersecurity requirements are still being met.

The concepts of "metrics" and "measuring" were added to the framework in an effort by NIST to help organizations determine the cause-and-effect relationships between cybersecurity outcomes and business outcomes. Mr. Barrett indicated that they will help start conversations about cybersecurity risks, stating that "measurements will be critical to ensure that cybersecurity receives proper consideration in a larger enterprise risk management discussion." Understanding the causal relationship can help organizations achieve a business objective while managing cybersecurity risks. The framework asserts that the implementation tiers, subcategories and categories can be used as "metrics," as well as to aggregate and gather "measures," or quantifiable data that supports the metrics. The framework encourages organizations to track security metrics and business objectives in order to provide insight into how changes in an organization's cybersecurity management practices impact business outcomes.

Seeking Comments

NIST is seeking additional comments to the updated framework. The deadline for sending comments is April 10, 2017.

Return to Table of Contents

[7] The update is available here.

Switzerland and US Agree on Privacy Shield to Replace Safe Harbor

The United States and Switzerland have agreed on a Privacy Shield for allowing the transfer of personal information from Switzerland to the United States. The Swiss-U.S. Privacy Shield closely resembles the EU-U.S. Privacy Shield finalized in 2016.

On January 11, 2017, the Federal Council of Switzerland and the U.S. International Trade Administration (ITA) announced a new agreement to govern the transfer of personal data from Switzerland to the United States. Called the Swiss-U.S. Privacy Shield, this agreement will replace the U.S.-Swiss Safe Harbor Framework, which, following the invalidation of the similar EU-U.S. Safe Harbor in October 2015, was deemed inadequate to guarantee that U.S. companies provided sufficient data protection.

The requirements under the new Swiss-U.S. Privacy Shield substantially mirror the EU-U.S. Privacy Shield, with only a handful of notable differences. In a statement released in conjunction with the announcement of the agreement, the Swiss Federal Data Protection and Information Commissioner (the FDPIC) noted that having the "same standards apply for Swiss exports of personal data to the USA as for data exports from the EU … is fundamental to legal certainty in commercial transactions and in particular for the free exchange of data between Switzerland and the EU."

Requirements Under Swiss-US Privacy Shield

Similar to the EU-U.S. Privacy Shield, the Swiss framework fundamentally focuses on providing data subjects greater transparency and control over their personal information, as well as on holding data processors accountable through certain restrictions, cost-free individual recourse mechanisms and more comprehensive government oversight.

Because the Swiss-U.S. Privacy Shield applies the same standards to organizations as the EU-U.S. Privacy Shield, companies who have self-certified under the EU framework already have made many of the changes necessary in order to self-certify under the Swiss framework.[8] Notable new requirements include:

- organizations must pay a separate annual fee, the amount of which will be tiered based on the organization's annual revenue;
- privacy policies must specifically reference commitment to the Swiss-U.S. Privacy Shield, and any references to the U.S.-Swiss Safe Harbor must be removed;
- the category of sensitive information for which individuals must express affirmative consent ("opt in") to be disclosed to a third party or used for any purpose other than those for which it was originally collected or subsequently authorized is expanded under the Swiss framework to include ideological views or activities, information on social security measures, or administrative or criminal proceedings and sanctions treated outside pending proceedings. These categories are not identified as "sensitive" under the EU framework;
- under the Swiss framework, the FDPIC takes the role of the European data protection authorities, and thus certified companies must cooperate with the FDPIC in order to satisfy principles related to data subject recourse, enforcement and liability; and
- at the first annual joint review of the functioning of the Swiss-U.S. Privacy Shield, the Department of Commerce will work with the Swiss government to install the binding arbitration body that will settle claims under the Swiss framework that remain unresolved through other available remedies.

Self-Certification

Companies will be able to self-certify compliance with the Swiss-U.S. Privacy Shield on the ITA website starting April 12, 2017. The Department of Commerce will maintain a list of organizations that are certified at any given time, as well as a list of organizations that were at one time certified but are no longer covered by the Swiss-U.S. Privacy Shield, including the reason that such entities were removed from the certification list. As under the EU-U.S. Privacy Shield, although self-certification under the new Swiss framework is voluntary, once certified a company has made a commitment to maintain the requisite data protection that is enforceable by either the Federal Trade Commission or Department of Transportation. Companies alternatively may employ other mechanisms currently recognized by the FDPIC in order to transfer personal data from Switzerland, including the EU's standard contractual clauses, the Council of Europe's model contract to ensure equivalent protection in the context of transborder data flows, and the FDPIC's standard contract for the transborder outsourcing of data processing.

Next Steps

Whether a company decides to self-certify to the Swiss-U.S. Privacy Shield[9] or employ model contracts, it will be important

[8] For more detailed information regarding the requirements of the EU-U.S. Privacy Shield, please see our July 2016 *Privacy and Cybersecurity Update*, available here.

[9] Click here for detailed information regarding the requirements of the Swiss-U.S. Privacy Shield.

to keep abreast of developments in this area. Both the EU-U.S. Privacy Shield and the EU standard contractual clauses are currently facing legal challenges, and the FDPIC expressly has retained the right to revise its evaluation as to whether any approved mechanisms provide adequate protection based on the actual implementation of such mechanisms and court judgments in Switzerland and the EU.

Return to Table of Contents

Report by Insurance Think Tank Discusses Insurability Challenges Facing the Cyber Insurance Market

A report by the Geneva Association, an insurance think tank, considers insurability challenges facing the cyber insurance market. The report also includes recommendations to the insurance industry and international governments regarding preventing cyber risk and the global development of the cyber insurance market.

The world's increasing dependency on information and communications technology has led to the emergence of a plethora of cyber risks, which have the power to hinder the momentum of technology and adversely impact the world economy. While these cyber risks present a significant opportunity for the insurance industry, a number of insurability challenges exist. A recently report titled "Ten Key Questions on Cyber Risk and Cyber Risk Insurance" (the report)[10] published by the Geneva Association (Geneva), a leading international insurance think tank, considers three principal challenges to the insurability of cyber risk and offers recommendations to insurers and governments for combating cyber risks and supporting the cyber insurance market.

Status Quo

Geneva reports that the cyber insurance market is still relatively small, but is expected to grow in the coming years. The market has emerged most prominently in the U.S., Geneva reports, due in large part to the U.S.'s regulatory reporting requirements for cyberattacks, which carry heavy fines in the event of a violation. According to the report, these regulations have increased awareness of cyber risks and increased demand for third-party liability cyber insurance coverage. Geneva predicts that a regulatory approach also will be an important driver in the development of the European cyber insurance market. With respect to premium levels, the report notes that the current annual gross premiums for cyber insurance in the U.S. are $2.75 billion and growing between 26 and 50 percent per year on average.

Cyber Risk Insurability Challenges

Geneva finds three primary insurability challenges in the cyber insurance market. First, Geneva maintains that cyber loss exposure is unpredictable due to insufficient data on cyber risk to measure loss exposure. The unpredictability of cyber loss makes it difficult for insurers to pool risks. Furthermore, even when historical data is available, Geneva questions whether the data is a meaningful indicator of future losses due to the dynamic nature of cyber risks.

Second, Geneva identifies information asymmetry as a significant problem affecting the insurability of cyber risks. According to Geneva, companies that have experienced serious cyberattacks are more likely to buy insurance, which results in adverse selection in the cyber insurance marketplace. Cyber insurers try to alleviate adverse selection through a number of measures, such as screening processes (*e.g.*, audits), self-selection (*e.g.*, underwriting questionnaires) and signaling (*e.g.*, requiring certificates for IT compliance). Geneva reports that information asymmetry also creates moral hazard problems whereby companies might be less likely to invest in preventative measures once they have a cyber insurance policy in place. According to the report, insurers reduce moral hazard through screening processes and risk sharing (*e.g.*, deductibles and coverage limits).

Third, Geneva reports that coverage limits pose a problem for the insurability of cyber risks. Geneva explains that cyber insurance policies tend to cover only limited maximum losses ($10 million-$500 million) and contain several key exclusions (*e.g.*, self-inflicted losses, access to unsecure websites or terrorism), which make it virtually impossible to adequately insure against extreme scenarios. Geneva also points out that cyberattacks may cause indirect losses, such as reputational harm, which cannot be measured and therefore are difficult to insure against. Another problematic aspect of coverage limits is the complexity of cyber insurance policies. The numerous policy exclusions and variations in terminology across policies, coupled with the dynamic nature of cyber risks, creates uncertainty about what the policies actually cover. Geneva questions whether the coverage limits insurability problem is the result of a supply shortage or insufficient demand for coverage.

Practical Recommendations

To prevent cyber risks and promote the cyber insurance market, Geneva recommends that the insurance industry work with other stakeholders globally to diminish insurability challenges. For

[10] *See* the Geneva Association, "Ten Key Questions on Cyber Risk and Cyber Insurance," December 2016, available here.

example, Geneva advises that insurers should collect and spread information in order to increase data on cyber risks and ameliorate information asymmetry. To this end, Geneva recommends that the insurance industry publish standards and best practices for cyber risk assessment and management. In particular, risk management protocols with respect to complex crises are necessary, which should be developed by the insurance industry in collaboration with other industries as well as the government. Geneva also suggests that insurers develop an anonymized data pool, which would have the benefit of reducing uncertainties with respect to data and modeling, promote the underwriting of heavy risks and permit the industry to better understand and calculate risks overall.

Geneva also recommends that governments take action to reduce cyber risks. For example, the report urges governments to impose more severe punishments on cyber criminals, as a major share of cyber losses are caused by cyber criminality, and to ensure that law enforcement agencies are equipped with sufficient resources to keep up with increasingly sophisticated cyber criminals. Geneva cautions, however, that purely national frameworks are unlikely to be effective given that cyber criminals are not restricted by national boundaries, and, therefore, a collaborative international framework should be implemented. Geneva suggests that all governments introduce cyberattack reporting obligations in order to reduce cyber risk and promote the development of the cyber insurance market. Under such a scheme, according to Geneva, managers would be even more incentivized to prevent cyber risk and purchase cyber insurance because they could expect significant market discipline from investors and customers in the event of a cyber incident. Moreover, to provide a minimum level of cyber security across the board and reduce moral hazard, Geneva suggests that governments impose cyber risk standards.

In its concluding remarks, Geneva lays the groundwork for future research on the development of the cyber insurance market. Geneva finds that additional research, particularly regarding the demand for cyber insurance, is necessary to better understand cyber risk and further develop the cyber insurance market. For example, an analysis of consumers' risk perceptions may help the insurance industry learn how to educate customers on their cyber risks and correspondingly enable the industry to more effectively address those risks. Furthermore, from a macro perspective, Geneva indicates that research is necessary to analyze the systemic risks potentially emerging from underwriting cyber risks and to manage the accumulation of those risks. Further research, together with the collective efforts of the insurance industry, governments and other key players as outlined in the report, may advance the development of the cyber insurance market and result in the overall reduction and management of cyber risks.

Return to Table of Contents

(Attorney contacts appear on the next page.)

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

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

James R. Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian W. Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David C. Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

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

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

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

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Richard J. Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Amy S. Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

Ivan A. Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David E. Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

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

Jennifer L. Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Helena J. Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

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

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@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