Skadden

Privacy & Cybersecurity Update

EU's General Data Protection Regulation to Take Effect Despite Many Member States Not Prepared

The EU's new data protection law will go into effect in May, but many EU countries have not passed the local laws to align with the GDPR's requirements or to enable local enforcement.

Two years after it was approved, the European Union's General Data Protection Regulation (the GDPR) will go into effect on May 25, 2018. The GDPR makes a number of sweeping changes to EU privacy laws with ramifications both within the EU and abroad. However, a number of member states have not yet passed legislation to implement the GDPR's provisions for their countries, putting enforcement of the GDPR on uncertain ground.

Status of Local Regulatory Requirements for GDPR

EU member states must pass certain local laws in order to comply with the GDPR. Although the GDPR is a regulation that has the force of law without the need for individual member states to enact it for their individual jurisdictions, there are some specific actions member states must take. They must, for example, amend their existing local laws to ensure they do not conflict with the GDPR, and each country has the option to deviate from specific GDPR requirements in certain defined areas.

To date, only a handful of the 28 member states have passed such laws. Many others have legislation in progress but are not expected to have laws passed by May 25. Until these laws are passed, companies will still have to comply with the GDPR, but there may be some unresolved ambiguities as to companies' specific obligations. Further, depending on the jurisdiction, local authorities may not have a firm basis for enforcing the GDPR in their region without a local law enabling such enforcement.

Key Takeaways

Until the applicable member states have passed local laws to comply with the GDPR, companies subject to their jurisdiction should focus on compliance with the GDPR itself and should consult with local data protection authorities on any questions they may have — including on ways in which a local law is expected to deviate from the GDPR's general requirements.

Return to Table of Contents

States Take Action Against Equifax

The state of West Virginia filed a suit against Equifax related to its September 2017 data security breach; and a Massachusetts court has allowed the state's separate case against Equifax to continue.

The month of April saw two significant developments relating to state actions against Equifax stemming from its September 2017 data breach. On April 4, 2018, a Massachusetts state court denied the credit-reporting company's motion to dismiss the state's case against the company. Separately, on April 12, 2018, the state of West Virginia filed a case against the company.

Background on the Equifax Data Breach

Equifax announced the breach on September 7, 2017, revealing that attackers had gained access to sensitive personal data of more than 140 million American consumers. By the end of the month, more than 240 class actions had been filed alleging that the credit reporting agency was at fault for the massive breach.

According to the Massachusetts attorney general's (AG) complaint, Equifax relied on certain open-source software that it knew or should have known was subject to exploitation. Although Equifax allegedly knew of the vulnerability and potential patches by March 7, 2017, Equifax did not patch the vulnerability until July 30, 2017. As a result, sensitive personal data including names, addresses, Social Security numbers, dates of birth, driver's license numbers and credit card numbers were exposed in an unencrypted format.

Massachusetts Lawsuit and Recent State Court Decision

State Claim

On September 19, 2017, the Massachusetts AG filed a suit on behalf of state residents alleging that Equifax violated several of the state's strict data security and consumer protection laws.[1] Specifically, the Massachusetts AG alleged the following violations of state law:

- Equifax failed to provide notice of the data breach "as soon as practicable and without reasonable delay," as required by state law.
- Equifax failed to maintain the minimum reasonable cybersecurity standards in connection with safeguarding personal information contained in its databases.
- Equifax failed to implement and maintain a written information security program.
- Equifax engaged in unfair and deceptive practices by failing to promptly notify the public and the AG's office of the breach, failing to maintain reasonable safeguards to secure the sensitive personal data of Massachusetts residents, representing to consumers that it provided stronger privacy and cybersecurity protections than those actually implemented, and failing to make certain measures — such as free security freezes — sufficiently available that would have mitigated the harm caused by the data breach.

Equifax filed a motion to dismiss these claims under Massachusetts Civil Procedure Rule 12(b)(6) for failure to state a claim upon which relief can be granted.

Court Decision

On April 2, 2018, a Massachusetts state court denied Equifax's motion to dismiss.[2] The court noted that unlike private litigants, who must allege actual economic injury to maintain many of the claims asserted in this case, the Massachusetts AG may seek relief whenever she has reason to belief that a person is using or about to use an unfair or deceptive act. As discussed in a number

[1] The Massachusetts attorney general's complaint can be found here.

[2] The Massachusetts state court's decision can be found here.

of prior issues of our *Privacy and Cybersecurity Update*, the difficulty associated with identifying and alleging actual economic injury has plagued a number of plaintiffs in federal data breach litigation. The state court decision suggests that state attorneys general may have more success in bringing data breach-related claims given the relaxed requirement to allege actual economic injury for certain types of claims in state courts.

West Virginia

A few days after the Massachusetts court decision, the West Virginia AG filed a similar lawsuit against Equifax on behalf of the state, alleging that more than 740,000 West Virginia residents were impacted by Equifax's failure to secure its systems and promptly inform the public after it learned of the data breach. The state seeks $150,000 for each security breach and $5,000 for each violation of the state's consumer protection statute, as well as costs.

Key Takeaways

Depending on the success of claims in these cases, companies may see an increasing number of suits brought by state attorneys general in response to major data breaches. The Massachusetts state court decision suggests that states may find it easier to file these types of claims, based on the relaxed requirements for state attorneys general to allege actual economic injury in connection with certain claims. West Virginia's recent lawsuit also provides some support for that position. Companies could face significantly more exposure due to the increased risk of litigation from data breaches.

Return to Table of Contents

FTC Launches New Cybersecurity Campaign Targeted to Small Business Owners

The Federal Trade Commission has launched a new campaign to help small business owners combat the myriad cyber threats they face.

On April 10, 2018, the Federal Trade Commission (FTC) announced the launch of a national education campaign to help small businesses strengthen their cybersecurity defenses and protect the sensitive data they store. The FTC's decision to launch this campaign comes in light of the increased realization that, despite having less data, small businesses are also targets for cyberattacks.

Roundtable Discussions Informed Content of Campaign

The FTC designed the initiative, titled the Small Business Cybersecurity Education Campaign (campaign), to address key issues that were raised in a series of roundtable discussions that the FTC — working with other federal and local partners — held in 2017 to foster discussions with small business owners. The roundtable discussions took place across the country and were attended by small businesses representing various industries. The overall purpose in conducting the discussions was to learn how small business owners deal with cyber threats and security, and to hear their ideas on how the government can help them in this effort.

The main topics of concern were how to avoid phishing schemes, ransomware attacks, tech support scams and imposter scams. Additional concerns included:

- an inability to address perceived cybersecurity threats;
- employee errors that could inadvertently compromise businesses' systems;
- inadequate understanding of mobile device security, cloud security, wireless connections, email authentication and what to look for when purchasing web hosting services;
- a greater need for understanding cyber insurance and appropriate guidance for selecting qualified vendor security providers; and
- a centralized overview of cybersecurity basics.

Most of the attending small business owners reported that they generally did not have full-time information technology staff to help them keep up with the latest trends in cybersecurity, so the campaign is designed to enable non-technology specialists to become more aware of the threats they face and the tools available to address them.

The Campaign

The FTC designed the campaign to address the top concerns identified during the small business roundtable discussions. The campaign will take advantage of existing resources, which will include raising awareness of the FTC's website feature "Protecting

Small Business" and blog "Stick with Security," both of which were launched in 2017 to help small businesses navigate cybersecurity threats. In addition, the FTC plans to bolster attention for its previously developed cybersecurity-related publications (*e.g.* "Start with Security," "Data Breach Response" and "Protecting Personal Information") by partnering with private, nonprofit organizations, such as the Better Business Bureau and the National Cybersecurity Alliance, and its federal partners to distribute campaign materials and publications, all of which will be available online.

As part of the campaign, the FTC also has outlined several new methods for addressing the concerns of small business owners. For example, the commission will create training modules and videos that address topics of importance to small business owners such as:

- phishing, tech support scams and ransomware;
- email authentication;
- cloud security;
- vendor security; and
- understanding the National Institute of Standards and Technology cybersecurity framework.

Key Takeaways

The rising frequency of cybersecurity threats have not spared small businesses. The FTC's newly launched campaign signals an increasing need for small business owners to protect their networks and data with basic procedures that can be implemented, even for those businesses lacking full-time information technology staff.

Return to Table of Contents

Ninth Circuit Concludes Seafood Company's Email Scam Loss Not Covered Under Computer Fraud Policy

Amidst a growing body of case law from courts around the country concerning insurance coverage for "email spoofing" losses, the Ninth Circuit held that a policy exclusion for loss resulting from authorized access to an insured's computer system barred coverage for the losses of a company that was duped into wiring funds to a hacker posing as one of its vendors.

On April 17, 2018, the U.S. Court of Appeals for the Ninth Circuit affirmed summary judgment in favor of Travelers Casualty and Surety Company of America (Travelers) in an insurance dispute concerning the applicability of computer fraud coverage to a fraudulent wire transfer incident resulting in over $700,000 in losses to Seattle-based seafood importer Aqua Star (USA) Corp. (Aqua Star).[3]

The Email Spoofing and Fraudulent Wire Transfer

In 2013, the computer system of Longwei Aquatic Products Industry Co. Ltd. (Longwei), a seafood vendor from which Aqua Star regularly purchased frozen shrimp, was hacked by a fraudster. The fraudster then began monitoring emails between Aqua Star and Longwei before intercepting emails and communicating with Aqua Star from "spoofed" email domains designed to mimic those of Longwei employees. In response to an email from the fraudster directing Aqua Star to change Longwei's bank account information for future wire transfers, Aqua Star's treasury manager, at the direction of her supervisor, revised the bank account information, thereby resulting in the rerouting of Longwei payments to the fraudster's bank account. Aqua Star made four payments to the fraudster's account resulting in $713,890 in losses to the company.

[3] *Aqua Star (USA) Corp. v. Travelers Casualty and Surety Co. of Am.*, No. 16-35614, 2018 WL 1804338, at *1 (Ninth Cir. Apr. 17, 2018).

Aqua Star sought to invoke the computer fraud coverage provided by its crime insurance policy issued by Travelers. However, the Travelers policy contained an "authorized access" exclusion providing that the computer fraud coverage did "not apply to loss resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System." Because the modified banking information was entered by Aqua Star's treasury manager, who was an authorized Aqua Star employee, Travelers denied coverage.

The Courts' Rulings in Favor of Travelers

Aqua Star brought suit against Travelers seeking payment for its email scam loss under the computer fraud coverage section of the Travelers policy. Aqua Star moved for summary judgment on its breach of contract and declaratory relief claims, and Travelers cross-moved for summary judgment on all claims in light of the "authorized access" exclusion. On July 8, 2016, the U.S. District Court for the Western District of Washington granted summary judgment in favor of Travelers.[4] The district court found that the "authorized access" exclusion clearly applied because the bank account information was entered by an authorized Aqua Star employee (the treasury manager) and entry of the bank account information on the treasury manager's computer was an indirect cause of Aqua Star's loss. The court rejected Aqua Star's argument that the exclusion did not apply because the Aqua Star employee had to enter data into the computer system of a third party, Bank of America, as the final step leading to Aqua Star's loss. The court reasoned that the exclusion still applied because "necessary intermediate steps prior to the transfer involved entering electronic data into Aqua Star's own computer system."

In a brief opinion entered on April 17, 2018, the Ninth Circuit affirmed the district court's decision, noting that the "authorized access" exclusion was unambiguous and Aqua Star's "conduct fits squarely within the exclusion." The court reasoned that "Aqua Star's losses resulted from employees authorized to enter its computer system changing wiring information and sending four payments to a fraudster's account. These employees 'ha[d] the authority to enter' Aqua Star's system when they 'input' Electronic Data, on Aqua Star computers, to change the wiring information and authorize the four wires."

Key Takeaways

The Ninth Circuit's decision, which may seem like a straightforward case of contract interpretation, is not insignificant. Over the last few years courts have seen an influx of cases involving email spoofing and victims seeking to collect on their computer fraud insurance coverage. While some courts, like the Ninth Circuit, stay true to the plain language of the insurance policy, others have adopted broader readings of computer fraud coverage provisions in order to find coverage for email spoofing losses. As courts continue to weigh in, insurers, policyholders and brokers should keep an eye on this growing phenomenon, as it may help inform the manner in which policy wording should be drafted in order to achieve the intended coverage.

Return to Table of Contents

NIST Releases Update to Cybersecurity Framework

The National Institute of Standards and Technology issued the first update to its widely adopted cybersecurity framework. The updates reflect comments from stakeholders in the areas of supply chain risks, authentication, cybersecurity incidents and potential framework applications.

On April 16, 2018, the National Institute of Standards and Technology (NIST) issued the first update to its Framework for Improving Critical Infrastructure Cybersecurity (framework).[5] The voluntary risk-based cybersecurity framework has been adopted in many different industries across organizations of all sizes. In announcing the update, Secretary of Commerce Wilbur Ross supported widespread adoption, saying "the voluntary NIST Cybersecurity Framework should be every company's first line of defense. Adopting version 1.1 is a must do for all CEOs."

Key Updates

The updates to the framework are based on comments received from stakeholders across U.S. government, industry and academia, as well as from workshops the agency held in 2016 and 2017. The updated version remains compatible with the

[4] *Aqua Star (USA) Corp. v. Travelers Casualty and Surety Co. of Am.*, 2016 A.M.C. 2278, 2284 (D. Wash. July 8, 2016).

[5] The update is available here.

initial version of the framework and substantially tracks the changes NIST proposed in January 2017.[6] The updates focus on cyber supply chain risk management (SCRM), authentication and identity guidelines, cybersecurity incidents and vulnerabilities, and the potential uses of the framework.

One of the most substantive updates to the framework is the addition of a new control category and associated subcategories focused on how organizations can use the framework to manage cyber supply chain risks. The objective of cyber SCRM controls is to "identify, assess, and mitigate products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain." Organizations can face these issues both as a supplier to and purchaser from third parties. The framework, in part, recommends addressing these risks through appropriately designed contractual measures and routine assessments to ensure that third parties are meeting the contractual requirements.

Another substantive update to the framework's controls is refined language regarding authentication, authorization and identity proofing. Specifically, the update adds new subcategories to the renamed "Identity Management and Access Control" category that discuss proofing identities and authenticating users, devices and other assets commensurate with the risks to the organization. The changes also clarify that controls for identities and credentials for authorized devices, users and processes should include verification, revocation and auditing.

The revised framework also more clearly distinguishes between cybersecurity issues that have impacted an organization from those that may impact it as they relate to conducting incident detection and recovery actions. The framework now defines a "cybersecurity incident" as a cybersecurity event that has impacted the organization, while a "cybersecurity event" is an issue that may impact the organization. Under the revised framework, organizations should have a plan in place to respond to and report on cybersecurity incidents. The update also added a subcategory for implementing processes to receive, analyze and respond to internally and externally reported vulnerabilities.

Beyond specific control updates, the revisions provide additional guidance on the use of the framework. For example, the revisions clarify that, ultimately, organizations do not comply with the framework itself. Rather, when the framework discusses compliance, it refers to the use of the framework to comply with an organization's internal cybersecurity controls. The update also adds a section to the framework that discusses using the framework for conducting cybersecurity self-assessments and using measurements and metrics to better understand the effectiveness of cybersecurity activities and investments.

Next Steps

NIST plans to publish the "Roadmap for Improving Infrastructure Cybersecurity" later this year. The document will highlight areas NIST sees as ripe for further collaboration. NIST also will be holding a conference to discuss the framework and risk management topics in Baltimore, Maryland, on November 6–8, 2018.

Key Takeaways

Companies should pay close attention to any updates to the NIST framework, as it has been an important foundational document for cybersecurity matters in the United States and beyond. Many government agencies and self-regulatory bodies have included it in their cybersecurity guidance, and these updates reflect NIST's effort to continuously improve and expand the framework to address new issues.

Return to Table of Contents

Seventh Circuit Revives Data Breach Class Action Against Barnes & Noble

The U.S. Court of Appeals for the Seventh Circuit revived a thrice-dismissed putative class action against Barnes & Noble Inc. arising out of a 2012 data breach, holding that the plaintiffs' allegations of money spent on credit-monitoring services and lost time were sufficient to plead economic damages. The court nonetheless expressed doubt as to the ultimate viability of the case, noting that Barnes & Noble also was a victim of the breach, and questioning the ability of plaintiffs to recover damages from a fellow victim or obtain class certification in a case that has been pending for so long.

On April 11, 2018, the U.S. Court of Appeals for the Seventh Circuit in *Heather Dieffenbach et al. v. Barnes & Noble Inc.*, vacated an Illinois district court's dismissal of a putative class action alleging Barnes & Noble Inc. failed to protect its customers' financial information during a 2012 data breach. The Seventh Circuit ruled that the plaintiffs had sufficiently alleged economic damages in the form of security costs and lost time, and that the district court erred in evaluating the plaintiffs' complaint under state, rather than federal, rules.

[6] Our review on the proposed updates is available here.

Background and Claims

In October 2012, Barnes & Noble customers brought a putative class action against the retailer just days after it announced it had been the victim of a hacking operation affecting its stores in California, Connecticut, Florida, Illinois, Massachusetts, New Jersey, New York, Pennsylvania and Rhode Island. The plaintiffs alleged that Barnes & Noble breached its contractual duties by failing to provide sufficient data security and violated state consumer fraud laws by failing to sufficiently notify affected customers of the breach in a timely manner. The plaintiffs sought to recover damages resulting from the theft of their credit card and debit card information. Although the lawsuit was brought under state law, jurisdiction in the Illinois district court rested on the Class Action Fairness Act.

The district court dismissed the original complaint, holding that the named plaintiffs had suffered no loss and thus lacked standing to sue. However, following the Seventh Circuit's decisions in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015) and *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), which held that consumers who experience a theft of their data have standing to sue, the district court held that the plaintiffs in *Barnes & Noble* had alleged an injury. The district court nonetheless dismissed the complaint, holding that the alleged injuries were not economic and thus damages were not adequately pled.

The Seventh Circuit's Ruling

On appeal, a three-judge panel of the Seventh Circuit held that the plaintiffs suffered injury in fact as a result of the data theft and thus had standing to sue. The court reasoned that the district court erred in evaluating the plaintiffs' complaint based on state rather than federal rules when it dismissed the claims for failing to allege economic damages. Federal jurisdiction in this case rested on the Class Action Fairness Act and thus pleading was governed by Fed. R. Civ. P. 8 and 9. Rule 8(a)(3) requires plaintiffs to identify the remedy sought, "but it does not require detail about the nature of the plaintiff's injury," according to the court. The court also cited Rule 54(c), which provides that a prevailing party may receive the relief to which it is entitled, regardless of whether the pleadings have mentioned that relief. Thus, the federal rules did not require that any loss, other than special damages under Rule 9(g) that were not relevant in this case, be specifically alleged. The federal rules only require the complaint to allege generally that plaintiffs have been injured.

The court held that the plaintiffs' complaint adequately alleged injuries, including money spent on credit-monitoring services and time spent "to set things straight." The court held that this is all that is required under federal rules, saying "these injuries can justify money damages, just as they support standing." The court also noted that a district court could grant judgment on the pleadings under Rule 12(c) if none of the plaintiffs' injuries were compensable as a matter of law under the state statutes on which they rely. However, in assessing the state laws on which the plaintiffs' claims rested, the court determined that at least some of the alleged injuries were compensable.

The Seventh Circuit vacated the district court's judgment and remanded the case to the district court, which will have to decide whether Barnes & Noble violated state laws and whether the proposed class should be certified.

At the end of its decision, the court noted that its opinion primarily concerned injury, and that the court had not concluded whether Barnes & Noble had violated any of the state laws at issue by failing to stop "villains" from stealing the plaintiffs' names and account data. The court remarked that "Barnes & Noble was itself a victim" because the company's reputation took a hit, had to replace expensive equipment and lost business. The court noted that none of the state laws cited expressly make merchants liable "for failure to crime-proof their point-of-sale systems." The court expressed pessimism regarding the plaintiffs' claims, stating that the plaintiffs "may have a difficult task showing an entitlement to collect damages from a fellow victim of the data thieves." Finally, the court said that it was "far from clear that this suit should be certified as a class action" because the state laws and potential damages are disparate, and because the case had been pending so long that certification may be problematic under Rule 23(c)(1)(A), which requires a decision to be made at an "early practicable time."

Key Takeaways

This ruling continues the Seventh Circuit's trend of allowing data breach suits by clarifying that a complaint in federal court cannot be dismissed on the ground that the plaintiffs do not adequately allege compensable damages, even if the suit alleges violations of state laws that impose more stringent substantive pleading standards. Perhaps more importantly, the decision provides a potential roadmap for defendants to challenge data breach suits. By questioning whether (1) plaintiffs are entitled to collect damages from fellow victims of data theft under certain state laws, (2) plaintiffs suing under disparate state laws are entitled to class certification, and (3) class certification is appropriate for suits that have been pending for years, the *Barnes & Noble* decision may open up new lines of attack for defendants in data breach suits.

Return to Table of Contents

Contacts in the Cybersecurity and Privacy Group

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

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

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

David 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

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

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

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

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

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

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

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

Helena 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

William Ridgway
Counsel / Chicago
312.407.0449
william.ridgway@skadden.com

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

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