Skadden

Privacy & Cybersecurity Update

Court's Denial of Wendy's Motion to Dismiss Reflects Growing Belief That Merchants Have a Duty To Safeguard Customer Information

In *First Choice Fed. Credit Union v. Wendy's Co.*, the U.S. District Court for the Western District of Pennsylvania allowed a data breach class action to proceed, holding that plaintiff financial institutions advanced plausible claims for negligence, negligence *per se*, violation of the Ohio Deceptive Trade Practices Act, and declaratory and injunctive relief in connection with Wendy's handling of customer information.

On March 31, 2017, Hon. Nora Barry Fischer of the Western District of Pennsylvania adopted Chief Magistrate Judge Maureen P. Kelly's report and recommendation to deny a motion by defendants The Wendy's Company, Wendy's Restaurants, LLC and Wendy's International, LLC (Wendy's) to dismiss a putative class action brought by financial institutions affected by data breaches at Wendy's restaurants in 2015 and 2016. Judge Fischer held that Wendy's failed to demonstrate that the magistrate judge's recommendations were clearly erroneous or contrary to law. The magistrate judge's recommendations and the district judge's adoption thereof are the latest decisions reflecting a growing hostility in the courts toward arguments that merchants have no duty to safeguard sensitive customer information or to provide adequate notification of a data breach.

Background and Claims

The plaintiffs are 26 financial institutions that issued credit and debit cards to Wendy's customers. The plaintiffs allege that customers used their cards to make purchases at Wendy's restaurants, after which Wendy's stored customer payment card data in its computer systems. According to the plaintiffs, beginning in or about October 2015, hackers used the credentials of a third-party vendor to install malware through which they stole Wendy's customers' payment card data from at least 1,000 restaurants. With that data, hackers were allegedly able to make fraudulent purchases on the credit

and debit cards issued by plaintiffs. The plaintiffs allege that Wendy's knew of a data breach in December 2015 and that by January 2016 unauthorized charges had been made to Wendy's customers' cards.

The plaintiffs allege that Wendy's breached duties to use reasonable care in safeguarding payment card data and to notify the plaintiffs of any breach in a timely manner, and that customers suffered financial losses as a result. The plaintiffs asserted claims for negligence, negligence *per se*, a violation of the Ohio Deceptive Trade Practices Act (ODTPA) and sought declaratory and injunctive relief. As to negligence *per se*, the plaintiffs alleged that Wendy's failure to use reasonable measures to protect payment card data and failure to comply with applicable industry standards violated Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) and similar state statutes. The plaintiffs sought to recover the costs of canceling and reissuing the compromised cards, and reimburse customers for fraudulent charges.

Wendy's filed a motion to dismiss, arguing that the plaintiffs' claims fail because, among other reasons, there is no common law duty to safeguard sensitive information or for a merchant to notify a financial institution of a breach.

The Magistrate's Recommendations and the District Court's Decision

On February 13, 2017, Chief Magistrate Judge Maureen P. Kelly issued a report and recommendation to deny Wendy's motion to dismiss. Although the parties disputed which law governed, Judge Kelly did not resolve that dispute, finding the matter was dependent on factual issues that could be probed only with the assistance of a fully developed record.

Regarding the negligence claim, Judge Kelly concluded that the plaintiffs had advanced a plausible claim based on Wendy's failure to delete cardholder information after the time period necessary to authorize a transaction; employ systems to protect against malware; comply with industry standards for software and point-of-sale security; and maintain an adequate firewall, among other failures. Although the magistrate judge was cognizant of the various concerns about choice of law, third-party criminal acts and public policy in this evolving area of the law, she concluded that the plaintiffs had adequately pled a negligence claim accepting all alleged facts as true.

Next, Judge Kelly concluded that the plaintiffs had sufficiently pleaded a negligence *per se* claim based on alleged violations of Section 5 of the Federal Trade Commission Act. Judge Kelly relied on a 2016 decision from the Northern District of Georgia — one of a growing number of courts finding that Section 5 supports a claim for negligence *per se* when asserted by financial institutions against a retailer whose data breach caused damages.

Judge Kelly next concluded that the plaintiffs had stated a claim for violation of the ODTPA based on Wendy's alleged misrepresentations regarding the security of their point-of-sale payment systems. Noting that Ohio courts look to cases interpreting the Lanham Act for guidance on the ODTPA, Judge Kelly concluded that the plaintiffs were required to plead causation and that their allegations that they incurred damages "as a direct and proximate result" of Wendy's misrepresentations regarding the security of its payment card system were sufficient.

Lastly, Judge Kelly recommended that Wendy's motion to dismiss be denied as to the plaintiffs' request for declaratory and injunctive relief. The plaintiffs sought a judgment declaring that Wendy's owed a legal duty to secure customer data and notify financial institutions of a data breach, and an injunction directing Wendy's to utilize specified data encryption protocols. Wendy's objected, stating that the plaintiffs sought a determination as to past liability that certain plaintiffs did not have standing to seek declaratory relief and that plaintiffs did not lack an adequate remedy at law. Judge Kelly disagreed with Wendy's and found that (a) the plaintiffs' allegations concerned not only past actions but also continuing actions, (b) associational standing is appropriate where the associate seeks declaratory and injunctive relief, and (c) the plaintiffs lack an adequate remedy at law because of the potential loss of good will with customers that could result from a future data breach.

On March 31, 2017, District Judge Nora Barry Fischer adopted the magistrate judge's report and recommendations and denied Wendy's motion to dismiss. Judge Fischer conducted a *de novo* review and concluded that Wendy's failed to demonstrate that the magistrate judge's recommendations were clearly erroneous or contrary to law. The district judge also did not fault the magistrate judge for eschewing a comprehensive choice-of-law analysis at such an early stage of the case.

Key Takeaway

These decisions reflect a growing hostility in the courts toward arguments that merchants have no duty to safeguard sensitive customer information or to provide adequate notification of a data breach. However, without specific laws or legal standards in place regarding when merchants and businesses are responsible for protecting customer data, companies face uncertainty in determining when they may face liability for the costs related to data breaches.

Return to Table of Contents

Tennessee Clarifies its Data Breach Notification Law

After a period of uncertainty over whether companies had to notify data subjects of breaches of encrypted data, the state of Tennessee has amended its data breach notification law to confirm that no notification is required. The state also made changes to the timing for data breach notifications.

On April 4, 2017, Tennessee's governor signed into law an amendment to the state's data breach notification law, eliminating confusion that had been caused by a March 2016 amendment as to whether breaches of encrypted data were subject to the state's notification requirement. Like most states, Tennessee's data breach notification law had provided an exception if the compromised data was encrypted. However, a March 2016 amendment appeared to remove that "safe harbor." The new amendment states that Tennessee's data breach notification law is not applicable to "information that has been encrypted in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2 if the encryption key has not been acquired by an unauthorized person." In summary, this most recent legislation restores the encryption safe harbor: If data is encrypted as defined under the act, then a breach of that data does not trigger notification requirements.

In addition to clarifying the status of encrypted information, Tennessee also altered its timing requirements for notification. Under the amended law, notification must be made within 45 days of discovery of the breach. The start of this 45-day period is tolled if law enforcement requests a delay because notification might compromise an investigation. Once law enforcement determines that no delay is required, the 45 days are counted from the date of that determination.

Return to Table of Contents

Article 29 Working Party Provides Guidance on GDPR

The Article 29 Working Party has issued guidance on aspects of the General Data Protection Regulation (GDPR) relating to the designation of lead supervisory authorities, the role of data protection officers and data portability. Although it has already met some resistance from within the EU, this guidance should be helpful for companies seeking to become GDPR compliant.

On April 5, 2017, the Article 29 Working Party approved a revised set of guidelines interpreting aspects of the EU's GDPR. Although they are not binding, the Working Party's views likely will carry a good deal of weight with data protection authorities and EU courts as the GDPR goes into effect.

The Working Party, an EU advisory body charged with providing expert guidance on data protection issues and promoting uniform application of data protection laws across the EU, provided three separate sets of guidance on the GDPR:

- guidelines for identifying a controller's or processor's lead supervisory authority,[1]
- guidelines on data protection officers (DPOs),[2] and
- guidelines on the right to data portability.[3]

The Working Party released a draft of its guidance in December 2016 and invited comments from the community. The final guidance adopted in April reflects the Working Party's response to the comments it received.

Guidelines for Identifying a Controller's or Processor's Lead Supervisory Authority

One issue presented under the GDPR is how to determine which government supervisory authority should take the lead in regulating a company that engages in "cross-border processing." The lead supervisory authority has primary responsibility for dealing with cross-border data processing activity and will coordinate any investigation. The GDPR defines "cross-border processing" as either (a) the processing of personal data that takes place in more than one EU member state where the data controller or processor is established in more than one member state; or (b) the processing of personal data that takes place in one EU member state but which substantially affects, or is likely to substantially affect, data subjects in more than one member state. The stated intention of this approach was to ensure that not all processing activity with any cross-border effect falls within the definition of "cross-border processing," however it left some ambiguity as to the specific parameters regarding which activities qualify.

The Working Party's final guidance on identifying a controller or processor's lead supervisory authority noted several steps to making that identification.

[1] Available online here.
[2] Available online here.
[3] Available online here.

Identify the "Main Establishment" for Controllers

The key point underlying the "lead authority" concept in the GDPR is that supervision of cross-border processing should be led by one authority within the EU. This is particularly important in instances where a multinational company makes decisions relating to cross-border processing activity at one central facility in the EU. In such cases, there should be a single lead supervisory authority of the various data processing activities instead of, for example, one in each country. The GDPR implies that the lead authority should be the location in the EU where decisions about the purposes and means of the processing of personal data are made and which has the power to have such decisions implemented.

Where a controller's main office (which the GDPR refers to as its "main establishment") is not the place of its central administration in the EU (*e.g.*, if decision-making is spread across different offices or controllers), the Working Party noted that the GDPR lays out several (non-exhaustive) questions to consider to determine the location of the controller's main establishment:

- Where are decisions given regarding processing final "sign off"?
- Where are decisions made about business activities that involve data processing?
- Where does the power to have decisions implemented effectively lie?
- Where is the director (or directors) with overall management responsibility for the cross-border processing located?
- Where is the controller or processor registered as a company, if in a single territory?

Where processing is carried out by a group of companies headquartered in the EU, the location of the overall control is presumed to be the location of the decision-making center related to the processing, and that location will therefore be considered the group's main office. The parent, or operational, headquarters of the group of companies in the EU is likely to be the main office because that would be the place of its central administration.

The GDPR does not explicitly deal with the issue of designating a lead authority in the case of joint data controllers. In such situations, the GDPR says the controllers shall, in a transparent manner, determine their respective responsibilities for compliance with their obligations under the regulation. The joint controllers should designate which location of the joint controllers will have the power to implement decisions about processing with respect to all joint controllers. This will be the main location for the processing carried out in the joint controller situation.

Cases Involving Both a Controller and a Processor

The GDPR states that the processor's main location will be the place of the central administration of the processor in the EU. However, for companies that have both a controller and a processor, the Working Party opined that the competent lead supervisory authority is the lead supervisory authority for the controller. In this situation, the supervisory authority of the processor will not be considered the lead, but is still expected to participate in decisions regarding data processing.

Guidelines on DPOs

Under the GDPR, certain controllers and processors are required to appoint DPOs if they are (a) a public authority or body, (b) an organization that monitors individuals systematically and on a large scale, or (c) an organization that processes special categories of personal data on a large scale as a core activity.[4] The Working Party's guidance on DPOs is intended to further clarify this GDPR requirement.

The guidelines provide an overview of the designation of a DPO, a description of the position of the DPO and a list of tasks the DPO should undertake.

Designating a DPO

The GDPR requires the designation of a DPO in three specific cases:

- the processing is carried out by a public authority or body;
- the core activities of the controller or the processor consist of processing operations, which require regular and systemic monitoring[5] of data subjects on a large scale; or
- the core activities of the controller or the processor consist of large-scale processing of special categories of data, or personal data relating to criminal convictions and offenses.

Companies may not appoint multiple DPOs. A single DPO must be responsible for the entire organization in all relevant jurisdictions, but he or she may be supported by a team. When several

[4] The appointment of a DPO also is mandatory for other competent authorities under Article 32 of Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties.

[5] The Working Party has clarified that data-driven marketing activities are considered examples of "regular and systematic monitoring" that require a designation of a DPO. Examples of such activities include operating a telecommunications network and profiling and scoring for purposes of risk assessment (*e.g.*, credit scoring).

organizations engage in joint data processing activity, the GDPR allows a group of companies to designate a single DPO provided that he or she is "easily accessible from each establishment." To ensure the DPO is accessible, the Working Party recommends that the DPO be located within the EU, whether or not the controller or processor is established in the EU. Companies with no EU presence can locate their DPO outside the EU if his or her responsibilities will be better carried out there.

When data controllers or processors determine whether they must appoint a DPO, they should keep that assessment on file for review by data protection authorities. These records are part of the organization's overall accountability obligations to the authorities, and may be requested at any time. Whether or not they have determined they were required to appoint a DPO, companies must reassess that decision each time they contemplate adding new activities or services affecting personal data.

Expertise of the DPO

According to the GDPR, the DPO "shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39." The required level of expertise is not strictly defined but must be commensurate with the sensitivity, complexity and amount of data an organization processes. The DPO should have a position within their organization that permits the DPO to fulfill the required tasks. According to the Working Party, DPOs must have expertise in national and European data protection laws and practices, and an in-depth understanding of the GDPR. The DPO also should have a good understanding of the processing operations being carried out by the organization, as well as the information systems, data security and data protection needs of the controller. Finally, the Working Party notes that the ability to fulfill the tasks incumbent on the DPO requires both proper personal qualities and knowledge (*e.g.*, integrity and professional ethics).

The GDPR requires that a DPO's other tasks within an organization may not present a conflict of interest with his or her DPO responsibilities. The Working Party clarified that senior managers, such as CEOs, COOs, CTOs, CFOs, chief medical officers, and the heads of marketing and public relations are likely to present too great a conflict of interest to also serve as DPO.

Position of the DPO

The GDPR provides that the controller and processor shall ensure that the DPO is "involved, properly and in a timely manner, in all issues which relate to the protection of personal data." The DPO should be involved from the earliest stage possible in all issues relating to data protection. If the organization ensures that the DPO is informed and consulted at the outset of any data protection impact assessments, the DPO will be better able to comply with the GDPR and promote a privacy by design approach.

The GDPR requires the organization to support its DPO by providing resources necessary to carry out their tasks and to maintain their expert knowledge. For example, the organization should provide active support by senior management, adequate financial and infrastructure support, official communication of the designation of the DPO to all staff to ensure their existence and function are known within the organization, and continuous training. In addition, employees must feel free to communicate with the DPO without fear of retaliation, meaning there must be a way for them to communicate directly with the DPO, either in person or through a service such as a hotline.[6]

Tasks of the DPO

The GDPR tasks the DPO with several duties in order to monitor the organization's compliance with the GDPR. Once appointed, a DPO becomes responsible for all of the organization's data processing activities. As part of these duties, DPOs may, in particular:

- collect information to identify processing activities;
- analyze and check the compliance of processing activities; and
- inform, advise and issue recommendations to the controller or the processor.

The DPO also is responsible for cooperating with supervisory authorities and acting as a contact point for the supervisory authority on issues relating to processing, in addition to consulting with such authority with regard to other matters.

Notably, it is the task of the controller, not of the DPO, to carry out any necessary data impact assessments. The GDPR states, however, that the controller must seek advice from the DPO when carrying out a data impact assessment.

The Working Party notes it is the DPO's responsibility to assess the risks associated with the organization's various processing operations, and to prioritize his or her activities on issues that present higher data protection risks. Such an approach should help DPOs advise controllers on deciding which methodology to

[6] The Working Party also identified outside counsel as problematic DPOs, as the role likely would prohibit them from also representing their clients in cases involving data protection issues.

use when carrying out a data impact assessment, deciding which areas should be subject to a data protection audit, establishing training activities for staff and management and deciding which processing operations present the highest risk and therefore should receive the most focus.

Guidelines on the Right to Data Portability

Article 20 of the GDPR creates a new right to data portability, which is closely related to the right of access. Data portability allows data subjects to obtain the personal data that they have provided to a controller in a structured, commonly used and machine-readable format, and to request that a controller transmit that data to another controller.

The purpose of the right to data portability is twofold; it empowers data subjects by giving them more control over their personal data, and in certain industries it can foster competition between data controllers by facilitating switching between different service providers.

The Working Party's guidance discusses the right to data portability and its scope, clarifies the conditions under which the right applies and aims to help data controllers understand their respective obligations. The guidance also recommends best practices and tools to support compliance with the right to data portability.

Defining Data Portability and Setting its Scope

The right to portability includes a right to obtain personal data from a data controller and then transmit that data to another data controller. When an individual exercises the right to data portability, he or she does so without prejudice to any other right (such as continuing to use and benefit from a data controller's service after a data portability operation).

Compliance with the GDPR requires data controllers to have a clear legal basis for the processing of personal data. The principle of data portability applies to two types of data: data that can only be processed with the data subject's consent and data that was provided based on a contract to which the data subject is a party (pursuant to Article 6(1)(b)).[7] In addition, to be within the scope of the right, data must be personal data that an individual (as opposed to a third party) provided to a data controller. In addition, one person's right to data portability should not adversely affect the rights and freedoms of others, such as third-party data subjects who do not consent to a retrieval and transmission of data concerning them.[8] Finally, the right applies only if the data processing is "carried out by automated means" and does not cover data written in paper files.

Pushback from Privacy Experts

There already has been pushback from the European Commission in response to the Working Party's guidelines, specifically with respect to the Working Party's interpretation of the data portability clause. The European Commission wrote to the Working Party with its concern that the Working Party has interpreted too broad of a scope for the GDPR's right to data portability.

One commission spokesperson noted that the commission has "concerns that the [Working Party's] guidelines might go beyond what was agreed by the co-legislators in the legislative process."[9] While the spokesperson did not elaborate on that comment, it appears to relate to the issue of "observed data" as interpreted by the Working Party. This issue was one of the most controversial aspects of the draft guidelines that the Working Party issued in December 2016, and it was not fully addressed in the April 2017 revision. Article 20 of the GDPR states that "the data subject shall have the right to receive the personal data concerning him or her, which he or she has *provided* to a controller." Yet the Working Party's guidance on data portability notes that portable data includes "data that are *observed* from the activities of users." Some commentators have opined that the GDPR's language is meant to limit the scope of data portability to information the individual specifically provided to the controller — such as registration information or payment information or delivery addresses — but the Working Party's language expands to include information observed about the data subject, such as traffic patterns, location or click-through rates. Thus, it is unclear if the Working Party attempted to expand the scope of the right to portability to include the right to data portability of data observed about the data subject in addition to data provided by the person looking to exercise their right.

In addition, several commentators were critical of the absence of meaningful discussion of the security of the data subject to the right to data portability in the December draft. While the revised guidance provides some further detail, it simply notes that controllers must "assess the specific risks linked with data portability and

[7] As an example, the titles of books purchased by an individual from an online store is personal data generally within the scope of data portability because it is processed based on performance of a contract to which the data subject is a party.

[8] Such an adverse event could occur if the transmission of data from one data controller to another would prevent third parties from exercising their rights as data subjects under the GDPR, such as the rights to information or access.

[9] David Meyer, *European Commission, Experts Uneasy Over WP29 Data Portability Interpretation*, IAPP (April 25, 2017).

take appropriate risk mitigation measures," which could include multi-factor authentication techniques and suspending transfers where there is suspicion that an account is compromised.

Lastly, experts note that, while the guidelines suggest that data processors may have to be involved in answering data portability requests, the GDPR itself only discusses controllers as being involved.

Key Takeaway

Although the Working Party has sought to clarify various aspects of the GDPR, certain statements in its guidance will likely raise additional questions and require further clarification. The Working Party's guidance — and the pushback against it — shows that the GDPR remains a work in progress with additional guidance likely to come. We will continue to monitor the issues around the GDPR and its implementation as they develop.

Return to Table of Contents

New Mexico Becomes 48th State to Enact Data Breach Notification Legislation

New Mexico has joined the ranks of states that have passed data breach notification legislation, adopting a law similar in many ways to those enacted by 47 other states.

New Mexico has enacted a data breach notification law, leaving only South Dakota and Alabama as states without such legislation. The New Mexico law, which was enacted on April 6, 2017, and will come in to effect on June 16, 2017, applies to persons — other than the state of New Mexico or its political subdivisions — that own or license personal identifying information (PII) of New Mexico residents. The law conforms substantially to data breach notification laws in many other states, but it is notable for several reasons.

Data Breach Notice Requirements

The basic breach notice requirements under the New Mexico law are similar to those in other states. In general, companies must report the security breaches, which are defined as unauthorized acquisition of unencrypted computerized information that compromises the security or confidentiality of PII. Unlike many states, however, New Mexico also requires companies to report breaches of encrypted information if the means for decrypting the information — the confidential key or other decryption process — also were acquired.

As is the case in many states, the good-faith acquisition of PII by an agent of a covered person for a legitimate business purpose does not need to be reported to data subjects. Similarly, no notice is required if, after an "appropriate investigation," the company determines that the breach does not give rise to a significant risk of identity theft or fraud.

Reporting Requirements

As with most states, the New Mexico law describes the specific means by which notice must be sent, such as traditional mail or email, or, certain circumstances that require alternative methods. such as notices posted on the company's website or sent to the attorney general or major media outlets. It also identifies a number of specific requirements for the notice, including:

- the company's name and contact information;
- a list of the types of information that are reasonably believed to have been the subject of the breach (if known);
- the date of the breach, or the date range within which it occurred (if known);
- a general description of the breach;
- the toll-free number and addresses of the major credit reporting agencies; and
- advice that directs the data subject to review account statements and credit reports to detect errors, as well as of the recipient's rights pursuant to the federal Fair Credit Reporting.

If the breach involved more than 1,000 New Mexico residents then, in addition to the notice to the affected data subjects, the company also must notify New Mexico's attorney general and the major consumer reporting agencies.

Definition of PII

The New Mexico law is similar to most states' laws, defining PII as an individual's first name or initial and last name and either a social security number, driver's license number, government-issued identification number, or bank account or credit/debit card number plus security code or password. Unlike most states, however, the New Mexico law also includes biometric data in its definition of PII.

Timing of Notice

Unlike many states, the New Mexico law has a specific deadline for providing notice. Many states require notification by the breached service provider "without unreasonable delay" or "immediately," to the affected customers. New Mexico has joined a minority of states that require notification provided in the most

expedient time possible and no later than 45 days following discovery of the breach, unless either (a) a law enforcement agency determines that the notification would impede a criminal investigation, or (b) a delay is necessary to determine the scope of the breach and restore the integrity, security and confidentiality of the system.

Additional Data Security Requirements

The New Mexico law also requires companies with PII to provide for proper disposal of the information when it is no longer reasonably required for business purposes. The act defines "proper disposal" as shredding, erasing or otherwise modifying the PII to make it unreadable or undecipherable. In addition, the law requires companies to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

Landscape of Breach Notification Laws Remains Complex

Only two states — South Dakota and Alabama — currently remain without data breach notification laws. However, as noted above with respect to the New Mexico law, there is not uniformity among the 48 states with data breach notification laws. This patchwork of laws complicates compliance for companies that have personal data from residents of multiple jurisdictions. Although many have called for a single federal standard to ease the burden of compliance, others feel that protecting data privacy should remain the province of the states, especially since states can react quicker than the federal government to new developments in this area. For now, companies that hold personal information need to closely monitor the developing laws in this area.

Return to Table of Contents

CGL Insurers Seek to Avoid Coverage for Multiple Putative Class Actions Against Policyholders Stemming from Data Breach

Two insurance companies recently asked a Florida federal court to move forward with their action that alleges they do not owe coverage to policyholders for 18 putative class actions against the policyholders arising out of a data breach affecting roughly 2 million of its patients.

In a recent commercial general liability (CGL) insurance coverage dispute stemming from data breach-related liability, insurers Charter Oak Fire Insurance Company (Charter Oak) and Travelers Property Casualty Company of America (Travelers) have asked a Florida federal judge to permit them to move forward with a lawsuit that they commenced last fall against their policyholders, 21st Century Oncology Investments LLC, a Florida-based cancer treatment center, and its affiliates (21st Century). The insurers are seeking a ruling that they owe no coverage under their respective CGL policies for a series of lawsuits arising out of 21st Century's alleged failure to protect the personal information of nearly 2 million of its patients from a data breach.[10]

According to the insurers' amended complaint, 21st Century discovered in November 2015 that it had suffered a data breach two months earlier, which resulted in the unauthorized sale of its patients' personal information, including names, social security numbers, medical treatments and insurance information. 21st Century notified the roughly 2 million affected patients of the data breach in March 2016. The amended complaint alleges that 21st Century has been hit with 18 putative class action lawsuits by its patients arising out of the data breach. These actions allege, among other things, that 21st Century negligently failed to safeguard its patients' personal information and comply with state and federal laws governing the dissemination and collection of such information.

21st Century sought coverage for the underlying actions under two primary CGL policies issued by Charter Oak (one for 2015-16 and another for 2016-17) and an excess CGL policy issued by Travelers. The insurers denied coverage and subsequently filed suit in the U.S. District Court for the Middle District of Florida against 21st Century seeking a declaration that they have no duty to defend or indemnify their insured in the underlying actions pursuant to the terms of their respective policies.

In January 2017, 21st Century moved to dismiss the insurers' amended complaint on the basis that the allegations in the underlying complaint triggered Charter Oak's duty to defend under the 2015-16 policy, thereby rendering premature and requiring dismissal of the insurers' remaining claims for declaratory relief with respect to coverage under the other policies at issue. As relevant here, the 2015-16 Charter Oak policy provides coverage for liability arising out of "personal injury," defined as including injury arising out of the "oral or written *publication* … of material that violates a person's right of privacy." 21st Century argued that the allegations in the underlying complaints fell within this coverage because (a) the underlying complaints allege publication of 21st Century patients' personal information,

[10] The case is *Charter Oak Fire Insurance Co., et al. v. 21st Century Oncology Investments LLC, et al.*, No. 2:16-cv-00732, pending in the U.S. District Court for the Middle District of Florida.

and (b) the personal injury coverage does not expressly require publication by the insured (as opposed to a third party), which triggered Charter Oak's duty to defend.

In February 2017, the insurers filed their opposition to 21st Century's motion. Relying on two cases from other jurisdictions, the insurers argued that CGL personal injury coverage is triggered only when the *insured*, not a third party, is alleged to have committed an affirmative act of publication. Accordingly, the insurers argued, because the personal information of 21st Century's patients was published by hackers and not 21st Century, the underlying actions fall outside the scope of the Charter Oak policy's personal injury coverage.

In opposing the motion, the insurers also cited an exclusion in the Charter Oak policy for personal injury arising out of an "alleged violation of a 'consumer financial protection law.'" According to the insurers, each of the underlying actions allege violations of "consumer financial protection laws" — either Health Insurance Portability and Accountability Act of 1996 (HIPAA) or other state and federal laws restricting the dissemination of private consumer information. Therefore, the insurers argued, even assuming that the underlying actions allege "personal injury," the consumer financial protection law exclusion nevertheless bars coverage for the underlying actions under the Charter Oak policy.

Next Steps

It remains to be seen whether the insurers will be permitted to move forward with their action against 21st Century. What is clear is that an increasing number of insurers are challenging coverage for data breaches under traditional CGL policies. Regardless of the merits of any such challenge, in order to avoid this type of dispute, insurers and their policyholders should discuss and, if necessary, clarify coverage for data breach-related liability to ensure that both parties to the insurance contract have a clear and mutual understanding of the extent to which the policy provides coverage, if any, for data breach-related liability.

Return to Table of Contents

European Parliament Adopts Resolution Seeking Review of EU-US Privacy Shield

The European Parliament has raised concerns over the effectiveness of the EU-US Privacy Shield, putting pressure on the European Commission to revisit the arrangement.

The European Parliament adopted a resolution on April 6, 2017, formally raising concerns about the EU-US Privacy Shield and calling for a closer review of the adequacy of the protections afforded to EU citizens under the framework. The Privacy Shield, an arrangement negotiated between the United States and the EU, replaced the Safe Harbor in 2016 as a means to allow the transfer of personal information about EU residents from the EU to U.S. companies who have self-certified to the Privacy Shield. Currently, approximately 1,900 companies have self-certified to the privacy and security requirements imposed by the Privacy Shield.

The Safe Harbor was declared invalid by the Court of Justice of the European Union in October 2015[11] because, in part, it failed to adequately protect EU residents from surveillance by the U.S. government. The Privacy Shield was designed to remedy those inadequacies. Despite the EU Commission's finding that the Privacy Shield offers adequate protections, members of the European Parliament (MEPs) have now questioned whether the Privacy Shield does, in fact, fully address the shortcomings of the Safe Harbor particularly with respect to the United States' ongoing right to conduct surveillance for national security and law enforcement purposes, and EU citizens' right to seek redress.

Concerns that Privacy Shield Does Not Provide Adequate Protections

As a general theme, the resolution expresses concern that bulk surveillance by the U.S. government is not prohibited outright under the Privacy Shield, but rather is allowed for certain purposes with assurances that such collection will be "reasonable" and "as tailored as feasible." The MEPs claim that this is a looser standard than provided under the EU Charter and thus does not provide EU citizens with sufficiently equivalent protection. The resolution also questions whether the dispute resolution mechanisms offered by the Privacy Shield provide adequate protections to EU citizens, particularly with respect to the limited avenues of redress for complaints regarding data used for surveillance and national security purposes. The resolution further highlights differences and shortcomings in the scope of protection afforded by the Privacy Shield when compared to EU privacy laws in relation to principles of notice and consent, data integrity and data minimization. The MEPs also expressed concern that the Privacy Shield does not provide specific rules on the use of personal data for automated decision-making and is generally unclear in how it applies to companies that process but do not ultimately control data.

[11] *Schrems v. Data Protection Commissioner*, Case number C-362/14, in the Court of Justice of the European Union.

Concerns that US Actions do not Match Assurances

The resolution also raises a number of particular concerns based on recent activity of the Obama and Trump administrations. The EU found that the Privacy Shield provided adequate protection from U.S. government surveillance based on letters and unilateral statements from U.S. officials assuring greater oversight, enforcement and safeguards related to collection of personal data for national security and law enforcement purposes. The MEPs' resolution expresses discomfort with the concept that the main pillar of certain assurances, an executive order (PPD-28) limiting the permitted purposes and uses of bulk data collection and ensuring certain privacy and civil liberty considerations, may be repealed by a U.S. president at any time without congressional approval. The MEPs state further that there are strong reasons to doubt the U.S. commitment to some of these assurances, citing as support: new rules passed in early January 2017 allowing the NSA to share data collected without a warrant with a number of other agencies; recent revelations about service providers acquiescing to NSA and FBI surveillance requests a year after the adoption of PPD-28; and the recent roll-back of FCC rules requiring internet service providers to obtain express consent before selling browsing data to advertisers and other companies.[12]

Concerns Over Unfilled Posts in Executive Branch

The resolution claims that the substantial number of unfilled roles in President Trump's executive branch tasked with enforcing the Privacy Shield "seriously undermines" assurances made with respect to oversight of the framework. Three of five commissioner seats remain vacant on the FTC, while the Privacy and Civil Liberties Oversight Board charged with overseeing privacy and civil liberties in relation to counter-terrorism programs lost its quorum in early January and has not seen new staff hired. While acting authority for the role of the independent ombudsperson tasked with addressing complaints related to collection of data for national security purposes has been temporarily delegated to acting assistant secretary for oceans, environment and science, Judith G. Garber, an official ombudsperson has not been appointed by the new administration, and the MEPs question whether such delegated power will provide the independence and authority necessary to provide adequate redress.

Call for European Commission Review

The resolution calls on the European Commission to review the compatibility of these new developments with the Privacy Shield, to review the adequacy of the framework generally and to seek clarification from the U.S. on the status of the guarantees it has made and assurance that these commitments will be maintained under the Trump administration. While the Privacy Shield is subject to annual joint review, the resolution creates pressure to consider these issues expeditiously, and there is likely to be further activity on the topic before the upcoming joint review slated for September 2017.

Compliance with GDPR

One area of uncertainty touched upon by the MEPs is the role of the Privacy Shield when the new GDPR is implemented in May 2018. The resolution urges the EU Commission to consider in its annual review whether the Privacy Shield is consistent with the GDPR.

Key Takeaway: Effect of Privacy Shield Rejection

When the Privacy Shield was enacted, many privacy advocates questioned whether it sufficiently addressed the concerns about U.S. surveillance raised by the European Court of Justice in *Schrems*. The MEPs' resolution highlights that these concerns remain even among EU representatives. The idea that the Privacy Shield might be invalidated or need to be amended is within the realm of possibility in an era where the Safe Harbor, which was once seen as infallible, was invalidated. Companies that rely on the Privacy Shield, or are considering whether to do so, should monitor developments in this area.

Return to Table of Contents

Proposed Chinese Cybersecurity Law Would Require Security Assessments and Consent to Export Data Overseas

As anticipated, the Chinese government has issued additional regulations under the November 2016 cybersecurity law that would require businesses to undergo security assessments and obtain consent of data subjects before transferring data abroad.

On April 11, 2017, the Cyberspace Administration of China released a draft article that would require firms exporting certain personal information and critical data (broadly defined as data related to national security, economic development and the societal and public interests) to undergo annual security assessments as part of their obligations under the recently proposed Chinese cybersecurity law. The new cybersecurity law, which was

[12] For more on the roll-back of FCC rules, see our March 2017 issue of the *Privacy and Cybersecurity Update*, available here.

announced in November 2016 and go into effect in June 2017, grants the Chinese government increased centralized power to protect network security and to safeguard cyberspace sovereignty. This latest draft article, like the cybersecurity law, appears to place increased pressure on the international business community and likely will face similar backlash from overseas critics.

Proposed Requirements for Data Transfer

The new draft article requires businesses that transfer over 1,000 gigabytes of data or data affecting more than 500,000 individuals outside of China to undergo security assessments by competent regulatory or supervisory authorities in their industry sectors. Sensitive geographic and ecological data also would undergo security assessments prior to any export. The draft article would ban the export of economic, technological or scientific data if such a transfer would pose a threat to security or public interests. Moreover, similar to the pending General Data Protection Regulation passed in 2016 by the European Parliament, the draft article would require businesses to obtain the consent of users before transferring personal data overseas.

Pundits have noted that the draft article was announced a day after Chinese state media introduced government rewards of $1,500 to $73,000 to any citizen who reports suspected spies. Industry insiders have suggested that while the draft article aims to protect personal information , the government rewards suggest that it also may be intended to help combat hacking and cyberterrorism.

Key Takeaways

Critics of the November 2016 cybersecurity law focused on the breadth of key provisions and suggested that parts of the new law will make it difficult for multinationals to operate in China, or, at the very least, will make it significantly more expensive for them to do so. Similarly, the new draft article introduces broad and vague categories of data that may affect businesses. Companies that consider China a significant part of their business model should reassess their current practices and ensure any changes are implemented to comply by June 1, 2017. The draft article is open for public comment until May 11, 2017, and if accepted, it will be put into effect June 1, 2017.

Return to Table of Contents

California District Court Denies Kimpton Hotel's Motion to Dismiss Majority of Data Breach Class Action Claims

In *Walters v. Kimpton Hotel & Restaurant Group, LLC*, the U.S. District Court for the Northern District of California denied in part and granted in part Kimpton Hotel's motion to dismiss, holding that the time and effort that the lead plaintiff expended in credit monitoring activity was sufficient to demonstrate injury for standing purposes. The ruling reflects a growing trend that costs to protect one's identity after a breach constitute injury and confer standing.

On April 13, 2017, Judge Vincent Chhabria of the Northern District of California denied in part and granted in part Kimpton Hotel & Restaurant Group, LLC's (Kimpton) motion to dismiss the plaintiff's data breach class action suit. Citing the Seventh Circuit's decision in *Lewert v. P.F. Chang's China Bistro*, 819 F.3d 963 (7th Cir. 2016), Judge Chhabria held that the theft of the plaintiff's payment card data, and the time and effort he expended in monitoring his credit, were sufficient to demonstrate injury for standing purposes. Judge Chhabria's ruling reflects a growing trend in courts across the country of holding that the expenditure of costs associated with protecting one's identity after a breach is sufficient to plead injury and confer standing.

Background and Claims

On September 20, 2016, lead plaintiff Lee Walters (Walters) filed a putative class action complaint and an amended complaint on January 6, 2017, against Kimpton arising from a data breach involving the theft of customers' personal payment card data and other data. Walters asserted claims for breach of implied contract, negligence and violations of the Unfair Competition Law (UCL) on behalf of a national class.

On December 28, 2015, and May 29, 2016, Walters used his payment card when checking into two Kimpton hotels located in California. Walters alleged that, beginning in or around February 16, 2016, and continuing through July 7, 2016, hackers utilizing malware accessed the computer systems at Kimpton hotels, including in California, and stole Kimpton customers' private

information. Walters alleged he suffered an injury in April 2016 when he discovered an unauthorized charge on the statement for the payment card he used to book his stay in December 2015. According to the amended complaint, Walters took "time out of his life" and "monitor[ed] his credit through an identity theft protection service to ensure that the information taken in the data breach at Kimpton hotels has not been used to steal his identity or otherwise cause damage to his credit and finances."

Walters alleged that Kimpton disregarded his and the putative class members' rights by (a) intentionally, willfully, recklessly or negligently failing to take adequate and reasonable measures to ensure its systems were protected, (b) failing to take available steps to prevent and stop the breach from happening, and (c) failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard customers' private information.

On February 6, 2017, Kimpton moved to dismiss the amended complaint, arguing that Walters had not alleged an injury-in-fact that was fairly traceable to Kimpton's security breach sufficient to establish his standing to sue under Article III. Kimpton also moved to dismiss, arguing that (a) an implied contract did not arise from the mere use of a payment card, (b) the plaintiff had not alleged actual damages sufficient to support his negligence claim, and (c) the plaintiff had not alleged an economic injury sufficient to establish standing under the UCL.

The Court's Decision

On April 13, 2017, Judge Chhabria denied in part and granted in part Kimpton's motion to dismiss. The key dispute surrounded Kimpton's argument that the plaintiff had not alleged an injury-in-fact that was fairly traceable to Kimpton's security breach sufficient enough to establish his standing to sue under Article III. Relying on the Sixth Circuit's opinion in *Galaria v. Nationwide Mut. Ins. Co.* and the Seventh Circuit's opinion in *Lewert v. P.F. Changs's China Bistro*, Judge Chhabria concluded that the "time and effort" the plaintiff spent on monitoring credit reports was "sufficient to demonstrate injury for standing purposes."

As an initial matter, the court agreed with Kimpton that the allegations about Walters' December 28, 2015, hotel stay did not support standing because his stay occurred several months prior to the date the malware attack allegedly began, and Walters' complaint offered no explanation as to how the breach could have placed at risk the data associated with the payment card that Walters used during that stay. However, Walters' May 29, 2016, visit occurred during the alleged "at-risk" window and, thus, it was plausible to infer from the complaint that Walters' information was among the payment card information stolen. Therefore, the court held that the theft of Walters' payment card data, and the time and effort he expended to monitor his credit, were sufficient to demonstrate injury for standing purposes. Notably, the court rejected Kimpton's argument that a plaintiff must actually suffer the misuse of his data or an unauthorized charge before he has an injury for standing purposes.

Judge Chhabria also denied Kimpton's motion to dismiss Walters' claims for breach of implied contract, negligence and violations of the UCL based on unfair and unlawful business practices. Specifically, the court held that Walters' claim that an implied contract arose out of Kimpton's privacy policy, which states Kimpton is "committed" to safeguarding customer privacy and personal information, was sufficiently pled. The court denied Kimpton's motion to dismiss the plaintiff's negligence claim because it lacked sufficient information to rule on whether the economic loss rule bars Walters' claim. Lastly, although the court held that Walters had sufficiently pled a UCL claim for unfair and unlawful business practices, the court held that Walters failed to plead that he actually relied on Kimpton's alleged misrepresentations, and thus dismissed his fraud-based UCL claim.

Key Takeaway

The decision is one among many across the country holding that plaintiffs who do not know if their personal information was stolen in a data breach may nonetheless plausibly state claims based on allegations they expended time and money to protect against misuse of their information, such as purchasing third-party credit monitoring services. There is a clear trend, at least in the Sixth, Seventh and Ninth circuits, that claims based on costs associated with protecting one's identity after a breach adequately plead injury and confer standing.

Return to Table of Contents

Illinois District Court Grants Motion to Compel Discovery in Class Action Over P.F. Chang's 2014 Data Breach Following Seventh Circuit's Ruling in Favor of Plaintiffs

In *Lewert v. P.F. Chang's China Bistro, Inc.*, No. 14-cv-04787 (N.D. Ill.), the U.S. District Court for the Northern District of Illinois ordered a data breach putative class action to proceed to discovery following the Seventh Circuit's holding that the plaintiffs had alleged sufficient facts to support Article III standing.

On April 26, 2017, U.S. District Court Judge Elaine Bucklo of the Northern District of Illinois denied defendant P.F. Chang's China Bistro, Inc.'s (P.F. Chang's) motion to dismiss the case and granted a motion by plaintiffs John Lewert and Lucas Kosner (together, the plaintiffs) to compel P.F. Chang's to participate in a Rule 26(f) conference and begin discovery.

Background and Claim

On June 12, 2014, P.F. Chang's announced that its computer system had been breached and customer credit and debit card data had been stolen. By August 4, 2014, P.F. Chang's reported that it had determined that data from only 33 restaurants had been stolen, but allegedly did not identify which restaurants. The company encouraged customers to monitor their credit card statements and credit reports for any incorrect or fraudulent charges.

The plaintiffs were two customers who dined at an Illinois location that P.F. Chang's alleged was unaffected by the breach. The plaintiffs filed putative class action suits against P.F. Chang's, alleging breach of implied contract and violation of the Illinois Consumer Fraud and Deceptive Business Practices Act. Plaintiff Lewert alleged that, although no fraudulent charges had been made on his card and no fraudulent accounts had been opened in his name, he had spent time and effort monitoring his account statements and credit report. Plaintiff Kosner alleged that four fraudulent transactions had been made with the card he used when he dined at P.F. Chang's. The plaintiffs also claimed they had expended time and effort obtaining replacement cards. The actions were subsequently consolidated.

P.F. Chang's moved to dismiss the action for lack of standing and failure to state a claim. On December 10, 2014, Judge John W. Darrah of the Northern District of Illinois granted the motion, without prejudice, based on lack of standing, holding that the plaintiffs had not alleged injuries that were concrete and particularized enough to support Article III standing. Judge Darrah did not address P.F. Chang's arguments regarding failure to state a claim. The plaintiffs appealed the ruling.

The Seventh Circuit, following its 2015 ruling in *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015), reversed the Northern District ruling, holding that the plaintiffs' alleged injuries were sufficiently concrete and particularized because (a) the fact that the data breach had already occurred made the risk of future identity theft and fraudulent charges sufficiently imminent, and (b) the plaintiffs' purchase of third-party credit monitoring services were a cognizable injury in addition to the fraudulent transactions. To the extent P.F. Chang's disputed that the plaintiffs' data was exposed in the breach, the Seventh Circuit found the distinction "immaterial" for pleading purposes. The Seventh Circuit also determined that causation was plausibly alleged, reasoning that P.F. Chang's defenses that the plaintiffs' data was never compromised and that fraudulent charges could not be attributed to the data breach could be pursued at the merits stage. Furthermore, the court concluded that a favorable judgment would redress the plaintiffs' injuries. Therefore, the Seventh Circuit held that the plaintiffs had alleged enough to support Article III standing, and remanded the case to the district court.

Following remand and after significant delay in beginning discovery, the plaintiffs moved to compel P.F. Chang's to participate in a Rule 26(f) conference and begin discovery. P.F. Chang's opposed the motion and asked the district court to adjudicate the company's previously advanced arguments regarding failure to state a claim before permitting discovery. Thereafter, the case was reassigned from Judge Darrah to Judge Elaine E. Bucklo.

The Court's Decision

On April 26, 2017, at a hearing on the plaintiffs' motion to compel, Judge Bucklo ruled from the bench that she was "letting this case go forward" because she felt "the Seventh Circuit ha[d] spoken." Although Judge Bucklo did not issue a written opinion, she appeared convinced that the Seventh Circuit's decision clarified that the plaintiffs' claims for mitigating potential identity theft were valid. Accordingly, Judge Bucklo (a) granted the plaintiffs' motion to compel, directing discovery to proceed, and (b) denied P.F. Chang's motion to dismiss, citing the "reasons stated in open court." There was no written opinion.

Key Takeaway

The court's decision reflects the continuing trend in the Seventh Circuit of finding that costs associated with protecting one's identity following a data breach constitute injury sufficient to confer standing, even where the question of whether the plaintiffs' data was actually exposed in the breach is in dispute.

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

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

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

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

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