April 2021

Skadden

# Privacy & Cybersecurity Update

## Second Circuit Allows Data Breach Claims for Increased Risk of Identity Theft

**The U.S. Court of Appeals for the Second Circuit has ruled that plaintiffs can establish standing to pursue claims arising out data breaches based solely on an increased risk of identity theft, provided that the plaintiffs can demonstrate that the risk is sufficiently concrete.**

On April 26, 2021, in *McMorris v. Carlos Lopez and Associates*,[1] the Second Circuit ruled that affected data subjects who have alleged only an increased risk of identity theft following a data breach can have standing to bring a claim. The ruling is somewhat of a departure from other circuits' decisions on similar issues, in which data subjects without a concrete injury had been denied standing to sue. However, although the court ruled that it was possible to have standing based solely on increased risk, it denied standing in the specific case before it based on its determination that the plaintiffs had not shown sufficient increased risk of harm.

### Background

In June 2018, an employee of Carlos Lopez & Associates, LLC (CLA), a veterans' benefits organization, inadvertently emailed all 65 employees of the organization an attachment that included a spreadsheet containing sensitive information (such as Social Security numbers, home addresses, dates of birth and telephone numbers) of approximately 130 current and former employees. CLA later contacted the current employees to address the accidental disclosure, but not the former employees.

Three individuals whose information was shared filed a class action complaint against CLA, asserting state law claims for negligence, negligence *per se* and statutory consumer protection violations. The individuals did not allege that they were victims of actual identity theft or fraud as a result of the disclosure, nor did they claim that their information was taken or misused by third parties. Instead, they claimed that they were at "imminent risk of suffering identity theft" and of becoming the victims of "unknown but certainly impending future crimes." The plaintiffs also claimed that they had cancelled credit cards, purchased credit monitoring and identity theft protection services, and spent time assessing whether they should apply for new Social Security numbers. However, the district court dismissed the case for lack of standing due to the lack of tangible injury to the plaintiffs.

[1] A copy of the decision is available here.

### Split on Increased Risk Cases

To date, there has been a split among U.S. circuits over whether an increased risk of identity theft establishes standing. The Sixth, Seventh,[2] Ninth and D.C. circuits[3] have held that an increased risk of future identity theft does establish standing, while the Second, Third, Fourth, Eighth and Eleventh circuits have reached the opposite conclusion, and have denied standing in a number of cases.[4]

### Second Circuit Ruling

In *McMorris*, the Second Circuit disagreed that there is a circuit split on the question of standing for increased risk of identity theft, though it noted that some courts have perceived one to exist. Instead, the court noted that, in its view, no court of appeals has explicitly foreclosed plaintiffs from establishing standing on that basis, and that those courts that had denied standing had done so on the specific facts before them. The court also noted that the Supreme Court's 2014 ruling in *Susan B. Anthony List v Driehaus* suggested that risk of harm could be a valid basis for standing, quoting in part "[a]n allegation of future injury may suffice to establish Article III standing if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur" (internal quotations omitted). Following that guidance, the Second Circuit ruled that "plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data."

The Second Circuit decision noted, however, that simple increased risk of identity theft would not always be sufficient to establish standing to make a claim. Accordingly, the court identified a non-exhaustive list of factors for courts to consider in determining whether to grant standing in these types of cases; none of which by themselves are determinative, but each of which bears on whether the injury is sufficiently "concrete, particularized and imminent" to confer standing. The court then applied these factors to the case before it, as outlined here:

- **Whether the Plaintiff's Data Has Been Disclosed as the Result of a Targeted Attempt To Obtain That Data.** Courts should consider whether the data was disclosed as a result of targeted attack or from a more benign sequence of events. Data obtained through a targeted attack would be more likely to be used to commit identity theft or fraud, whereas data released by accident would be less likely to be used in such ways. In the *McMorris* case, where the data was released accidentally and only to employees, the court decided that this factor did not weigh in favor of conferring standing.
- **Whether Any Portion of the Dataset Already Has Been Misused, Even if the Plaintiffs Themselves Have Not Yet Experienced Identity Theft.** If a plaintiff can show that some of the data that was disclosed has been misused — even if not the plaintiff's data but that of another data subject — a court can take that as evidence that the plaintiff's data is likely to be misused as well. Further, if the plaintiff can show that his or her data was misused (such as made available for sale on the dark web) — even if that misuse has not yet resulted in actual identity theft — then a court can take that as evidence of a concrete risk of identity theft. In this case, the plaintiffs had not made any showing of misuse of any of the data that was disclosed, so the court concluded that this factor also did not weigh in favor of conferring standing.
- **Whether the Type of Data That Has Been Exposed Is Sensitive Such That There Is a High Risk of Identity Theft.** Some types of data are more likely to be misused than other types, so a disclosure of more sensitive information can indicate a greater risk of identity theft. By contrast, a disclosure of publicly available information is generally less likely to be used to commit identity theft or fraud. Here, the information was extremely sensitive, which weighed in favor of finding a substantial risk of identity theft.

Taking these three factors into consideration, the court concluded that, even though the information was extremely sensitive, the absence of other facts indicating a heightened risk of theft showed that there was not a sufficiently concrete risk of harm to confer standing on the plaintiffs.

### Self-Help as a Basis for Standing

In addition to the risk of identity theft, the plaintiffs cited the efforts they had taken — and the costs incurred — to prevent identity theft as sufficient harm to confer standing. The court rejected that argument as well, noting that the plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of a hypothetical future harm that is not certainly impending."

### Key Takeaways

The Second Circuit's ruling in *McMorris* adds to the circuit split on the issue of standing to bring a data breach claim based only on an increased risk of identity theft. It remains to be seen whether courts in other circuits adopt the approach of the Second Circuit in similar cases going forward.

Return to Table of Contents

[2] For more on the Seventh Circuit ruling, please see Skadden's May 2020 "Privacy & Cybersecurity Update."

[3] For more on the D.C. Circuit cases, please see Skadden's July 2019 "Privacy & Cybersecurity Update."

[4] For more on the Eighth and Eleventh circuit cases, see Skadden's February 2021 "Privacy & Cybersecurity Update."

## European Commission Publishes Draft Artificial Intelligence Regulation

**The European Commission (EC) has published a draft regulation on artificial intelligence (AI), addressing both the development and use of AI, as well as AI-related compliance with the General Data Protection Regulation (GDPR).**

Regulators around the world have, to date, taken different approaches to potential regulation of AI systems, with the U.S. thus far adopting a light-touch approach and the EU taking a more interventionist position. In opting for this role, the EU's goal, according to European Commission President Ursula von der Leyen, is to foster "trust, not fear" in the hope that better regulation will win consumers' trust and encourage wider adoption of AI. To that end, on April 21, 2021, the EC published its draft regulation on AI (Draft AI Regulation) in hopes of establishing a harmonized legal framework for the development and use of AI, while ensuring compliance with the GDPR.

### Background

Though AI has the potential to produce enormous economic and societal benefits, including by companies who can use AI-influenced data to optimize digital solutions to gain a competitive advantage, the improper application of AI can potentially cause harm to consumers and businesses alike. Accordingly, the Draft AI Regulation proposes strict obligations on "high-risk AI systems" and those who use such systems. However, it does so within a risk-based framework, with the stringency of the requirements correlating with the level of risk.

### Key Features of the Draft Regulation

- **"AI system" Definition.** The Draft AI Regulation defines an AI system as "software that is developed with one or more of the techniques and approaches specified in an Annex to the Regulation, and can … generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with." The current draft of the Annex contains common AI approaches, such as machine learning, logic-based and knowledge-based approaches, as well as statistical approaches and Bayesian estimations.

- **Extraterritoriality.** Like the GDPR, the Draft AI Regulation seeks to have extraterritorial effect. Accordingly, the regulation would apply to (a) providers who place AI systems on the market in the EU, irrespective of whether they are established in the EU, (b) users of AI systems in the EU, and (c) providers and users of AI systems located in a third country, where the output produced by the system is used in the EU. Under these parameters, the scope of the regulation would potentially be very broad. For example, the Draft AI Regulation would apply to a provider that trains its AI system in the U.S. and produces insights used in the EU.

- **Risk Hierarchy.** The Draft AI Regulation takes a risk-based approach, providing different rules for uses of AI that create (a) an unacceptable risk (see Prohibited Practices section below), (b) a high risk and (c) a low risk. For example, high-risk AI systems are permitted subject to compliance with certain mandatory requirements, such as safeguards against biases in data sets and the establishment of data governance practices to ensure the integrity of data collection practices, examine possible biases and identify any possible data gaps. Although the Draft AI Regulation is silent on instances in which personal data is processed and the interplay with the GDPR, the GDPR's obligation requiring companies who process personal data to perform a data protection impact assessment seems likely to still apply in addition to the requirements of the Draft AI Regulation. What constitutes "high risk" is left open as well, though the Draft AI Regulation's explanatory memorandum states that the assessment should be based on the intended purpose of the AI system and the function it performs.

- **Prohibited Practices.** The Draft AI Regulation lists proposed practices to be prohibited on grounds that they contravene the values of EU law (*e.g.*, by violating individuals' fundamental rights). According to the Draft AI Regulation's explanatory memorandum, these practices have the potential to "manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups … in order to materially distort their behavior in a manner that is likely to cause them or another person psychological or physical harm." One such high-profile prohibition would be a ban on the use of real-time facial recognition technology systems in publicly accessible spaces for law enforcement purposes, although this is subject to various exceptions.

- **European Artificial Intelligence Board.** At the governmental level, the Draft AI Regulation proposes the establishment of a European Artificial Intelligence Board (EAIB), which, similar to the European Data Protection Board (EDPB) under the GDPR, would be made up of representatives from EU member states. Like the EDPB, the EAIB would facilitate the smooth implementation of the Draft AI Regulation, contribute to effective cooperation and enforcement, and provide advice and expertise.

- **AI Regulatory Sandboxes.** The Draft AI Regulation aims to foster innovation by allowing EU member states to provide a controlled environment to facilitate the development, testing and validation of innovative AI systems. These AI "regulatory sandboxes" would establish a framework to allow companies to innovate on the basis of a testing plan agreed upon with the competent supervisory authority. Participants in the AI regulatory sandbox would ensure appropriate safeguards are put in place and cooperate at all times with the competent supervisory authority.
- **Enforcement.** As noted in the Draft AI Regulation, any breach of the proposed prohibitions or of the data provisions for high-risk AI would be subject to heavy fines of a maximum of the higher of 6% of worldwide turnover or €30 million. Breaches of any other substantive provision of the regulation would be subject to fines of up to 4% of worldwide turnover or €20 million. Providing incorrect, incomplete or misleading information to conformity or enforcement bodies would be subject to fines of up to 2% of worldwide turnover or €10 million. Fines would be imposed at national level.

### Key Takeaways

Given the breadth of the Draft AI Regulation's definition of an AI system and its GDPR-like extraterritorial scope, these developments could be relevant for any organization developing, or considering developing, any software that has an AI element. That said, the legislative process regarding the proposal is at an early stage. For context, the GDPR was finalized after more than four years of legislative scrutiny.

Further, the Draft AI Regulation states that it shall apply two years following its entry into force. The response to the Draft AI Regulation has thus far been divisive, with privacy activist groups advocating for more robust enforcement in certain areas, such as facial recognition in public spaces, and business groups asking for more clarity on some key concepts, such as the meaning of "high-risk." As such, we expect the Draft AI Regulation to be subject to significant legislative scrutiny and anticipate its final form will evolve before being enacted.

Return to Table of Contents

## US Department of Labor Issues Its First Guidance on Cybersecurity Best Practices for Retirement Plans

**The U.S. Department of Labor has issued cybersecurity guidance for retirement plan administrators and participants, featuring a variety of common cybersecurity best practices.**

On April 14, 2021, the U.S. Department of Labor's Employee Benefits Security Administration (EBSA) provided its long-awaited guidance on employee retirement plans' cybersecurity duties, offering recommendations on steps employers and plan administrators — as well as plan participants — should take to protect data. Highlighting a range of common cybersecurity practices, the EBSA's guidance makes clear the continuing importance of cybersecurity awareness and the need for vigilant efforts in preventing cyber threats.

### Background

The Employee Retirement Income Security Act of 1974 (ERISA) set minimum standards for protecting plan participants and beneficiaries in private sector employer-sponsored retirement plans. Since ERISA's enactment, plan sponsors have increasingly relied on the internet and IT systems to administer these retirement plans, often outsourcing plan administration, including recordkeeping and other services, to third-party service providers. As such, addressing and protecting against the risk of bad actors targeting these retirement plans, which collectively hold trillions of dollars of assets and benefits, as well as the personal information of millions of participants, is a paramount issue for stakeholders involved with retirement plans. The new guidance defines the appropriate precautions plan fiduciaries should take to mitigate both internal and external cybersecurity risks.

### The Guidance

EBSA's cybersecurity guidance is segmented into three parts, focusing on plan administrators, employers and plan participants. Overall, EBSA's guidelines identify best practices that should be familiar to any organization in today's cybersecurity environment. The highlights of the guidance are outlined here:

#### For Plan Administrators

EBSA guidelines[5] for recordkeepers and other service providers for plan-related IT systems and data outline the best practices for proper mitigation of cybersecurity risks. These include the following recommendations:

- have a formal, well-documented cybersecurity program;
- conduct annual risk assessments;
- have an annual security control audit by a reliable third party;
- conduct periodic cybersecurity awareness training; and
- implement strong technical controls in accordance with best security practices, such as routine patch management, network segregation and regularly updated antivirus software.

#### For Employers

The cybersecurity tips directed to sponsors of pension plans[6] recognize that business owners regularly rely on outside service providers to maintain the security of their employees' plans. With this in mind, EBSA suggests employers take the following steps:

- inquire into the service provider's information security standards, and select a provider that follows a recognized standard for information security (such as the National Institute of Technology's cybersecurity framework) and uses a third-party auditor to review and validate cybersecurity;
- ask whether the security provider has experienced past security breaches and the circumstances of such incidents, as well as whether it is covered by cybersecurity and identity theft breach insurance policies; and
- ensure that contractual provisions governing the relationship with the service provider require ongoing compliance with cybersecurity and information security standards (and be wary of those that limit the service provider's responsibility for breaches).

#### For Participants

EBSA recommendations for retirement plan participants[7] to help reduce the risk of fraud and loss highlight routine steps that participants may themselves take. This includes registering and maintaining online access to their retirement account to regularly check the activity, using unique passwords for account access, providing multiple updated means of communication listed on accounts and exercising caution when utilizing free Wi-Fi networks. It further offers brief guidance on how to identify a phishing attack and encourages plan participants to keep their computers and mobile devices safe by keeping software up to date.

### Key Takeaways

Ultimately, the guidance provided by EBSA reflects relatively commonplace cybersecurity practices. In emphasizing the importance that plan sponsors and fiduciaries should place on preventing and properly mitigating cybercrime, we see yet another governmental entity — in this case, the Department of Labor — recognizing the need for vigilance against emerging cyber threats. Businesses should be aware of this trend and take steps to keep abreast of advances in cybersecurity that can protect both the company and its stakeholders.

Return to Table of Contents

## Ransomware Attack May Be Covered Under Crime Policy, Indiana Supreme Court Says

**On March 18, 2021, the Indiana Supreme Court unanimously reversed a lower court ruling and held that policyholder G&G Oil Co. of Indiana, Inc. (G&G Oil) may be entitled to coverage for a ransomware attack under its crime policy's computer fraud coverage.[8]**

### The Ransomware Attack

After it became locked out of its computer systems in November 2017, plaintiff G&G Oil discovered that it had been victimized by a ransomware attack whereby a cybercriminal had gained access to the company's computers and encrypted the hard drives. The cybercriminal demanded four Bitcoins, valued at nearly $35,000 at that time, in order to decrypt the hard drives' contents. After consulting with the FBI and computer tech services, G&G Oil paid the ransom and thereafter regained access to its computer systems.

[5] EBSA's plan administrator guidance can be accessed here.

On March 18, 2021, the Indiana Supreme Court unanimously reversed a lower court ruling and held that policyholder G&G Oil Co. of Indiana, Inc. (G&G Oil) may be entitled to coverage for a ransomware attack under its crime policy's computer fraud coverage.

[6] EBSA's employer guidance can be accessed here.

[7] EBSA's plan participant guidance can be accessed here.

[8] *G&G Oil Co. of Indiana v. Cont'l W. Ins. Co.*, 165 N.E.3d 82 (Ind. 2021).

### Continental's Denial of Coverage and G&G Oil's Coverage Action

G&G Oil sought coverage for the ransomware attack under its crime insurance policy issued by the defendant, Continental Western Insurance Co. (Continental), which provided coverage for loss "resulting directly from the use of any computer to fraudulently cause a transfer of money." Continental denied coverage, after which G&G Oil sued.

On motions for summary judgment, the trial court ruled in favor of Continental, holding that G&G Oil's loss was a result of theft, not fraud. It further held that G&G Oil's ransom payment did not qualify as a loss "resulting directly from the use of a computer" but rather "was a voluntary payment to accomplish a necessary result." The Court of Appeals unanimously affirmed, holding that the cybercriminal did not use a computer to fraudulently cause a transfer of money. The Indiana Supreme Court then granted G&G Oil's petition to transfer, thereby vacating the Court of Appeals' decision and allowing for review of the trial court's ruling *de novo*.

### The Indiana Supreme Court's Ruling

The Indiana Supreme Court considered two issues: (1) whether the ransomware attack constituted "fraudulent" conduct under the terms of Continental's policy; and (2) whether G&G Oil's loss "result[ed] directly from the use of a computer." G&G Oil urged the court to answer both questions in the affirmative.

On the first issue, after observing that "the interplay between computer fraud coverage and computer hacking is an emerging area of the law" and consulting multiple sources, including dictionary definitions and case law, the court determined that the phrase "fraudulently cause a transfer," as used in the policy, was unambiguous. That phrase, the court concluded, "can be reasonably understood as simply 'to obtain by trick.'" Applying this "straightforward definition," the court then held that neither party was entitled to summary judgment on the issue because a question remained as to whether G&G Oil's computer systems were obtained by trick. The court reasoned, in part, that "[not] every ransomware attack is necessarily fraudulent," and neither party had designated reliable evidence to demonstrate that the ransomware was or was not caused by trick.

Turning to the second issue, the court concluded that there was a sufficient causal connection between the alleged fraud and G&G Oil's loss such that the loss resulted "directly from the use of any computer." In reaching this conclusion, the court rejected Continental's contention that the voluntary transfer of Bitcoin "severed the causal chain of events." Rather, the transfer of Bitcoin was "nearly the immediate result – without significant deviation – from the use of a computer." While recognizing G&G Oil's ransom payment was voluntary in the literal sense, the court emphasized that the company only paid after consulting with the FBI and computer tech services, all while having no access to its computer files at the expense of its business and profitability. The court opined that "[u]nder those circumstances, the 'voluntary' payment was not so remote that it broke the causal chain."

Having determined that there was a potential for coverage under Continental's policy, the court reversed the trial court's grant of summary judgment in favor of the insurer, affirmed the denial of G&G Oil's summary judgment motion and remanded the case for further proceedings.

### Key Takeaways

The Indiana Supreme Court's ruling in *G&G Oil* serves as another example of the differing approaches taken by courts in analyzing coverage for cyber losses under traditional crime policies. While some courts have adopted a narrower interpretation of what it means for a loss to directly result from the use of a computer, the *G&G Oil* court employed a broader interpretation in concluding that the subject ransomware loss resulted directly from the use of a computer despite G&G Oil's voluntary ransom payment. Given the increased frequency and severity of ransomware attacks, this case also serves as an important reminder to insurers and insureds alike to clearly set forth in insurance policies the terms and conditions of coverage for ransomware attacks and other cyber events.

Return to Table of Contents

## Contacts

**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
213.687.5010
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

**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

**William Ridgway**
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

**Jason D. Russell**
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

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

**Ingrid Vandenborre**
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@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

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

**Eve-Christie Vermynck**
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

This communication is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This communication is considered advertising under applicable state laws.

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000