Skadden

Privacy & Cybersecurity Update

1 EU and UK Developments

2 UK's Cybersecurity Agency Will Not Report Data Breaches to Regulator

3 UK Information Commissioner's Office Levies 'Unprecedented' Fine for Illegal Sharing of Personal Data

5 SEC Reminds Firms to Follow Their Privacy Policies

6 Canadian Privacy Commissioner Concludes Investigation into Equifax Breach

7 Eleventh Circuit Finds no Coverage Under CGL Policy in Junk Fax Putative Class Action

EU and UK Developments

Recent developments in the European Union and United Kingdom's cybersecurity policies and programs — most prominently the adoption of the EU Cybersecurity Act — continued to demonstrate the region's focus on improving cybersecurity in the public and private sectors, while also providing practical guidance and tools to assist companies and their boards with cyber risk management.

The Cybersecurity Act

On April 9, 2019, the General Affairs Council of the European Council adopted the "Regulation on ENISA (the European Union Agency for Network and Information Security) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013" (Cybersecurity Act).[1] Whereas ENISA previously operated off of a limited mandate that would have ended in 2020, the Cybersecurity Act gives the agency a permanent role as the EU agency for cybersecurity. The act also creates a mechanism for establishing a common framework for EU-wide cybersecurity certification schemes for information and communications technology (ICT).

The Cybersecurity Act recognizes the pervasive and "vital role" that network and information systems play in society and economic growth, noting that they are the "cornerstone of the digital single market." As the EU faces a greater number of cybersecurity challenges from "borderless […] cyber threats," the Cybersecurity Act aims to increase cooperation between EU authorities and across countries. Accordingly, the Cybersecurity Act envisions a one-stop shop, regardless of the differences between schemes, in which national authorities will issue cybersecurity certifications for ICT products that meet certain standards, while also ensuring these certificates will be valid across the EU.

The certification schemes will be adopted by the European Commission and implemented by national authorities, but ENISA will help support their uptake and policy development. The schemes will be designed for specific groups of ICT products, processes and services, and may involve some elements of self-certification or third-party certification of product,

[1] The General Affairs Council's regulation can be read here.

process and service resilience and security. The Cybersecurity Act will come into force 20 days after publication in the EU's official journal and certification will be voluntary (unless member state or EU law specifies otherwise).

Recommendation on 5G Networks

On March 26, 2019, the European Commission recommended[2] operational steps to promote cybersecurity in European 5G networks. The recommendation included a national risk assessment of 5G network infrastructures to be completed by each member state by the end of June 2019. ENISA also will complete a coordinated risk assessment by October 1, 2019, via a Cooperation Group of competent authorities as dictated under the Security of Network and Information Systems Directive. The recommendation also mentions the implementation of the EU-wide certification framework as discussed in the Cybersecurity Act and encourages member states to cooperate with the European Commission and ENISA to prioritize a certification framework for 5G networks. Lastly, the recommendation states that, by October 1, 2020, member states shall assess the effects of the recommendation and determine whether further steps are merited.

UK Department for Digital, Culture, Media & Sport Cybersecurity Survey Results

On April 3, 2019, the U.K.'s Department for Digital, Culture, Media & Sport (DCMS) published its Cybersecurity Breaches Survey,[3] a report on information about cybersecurity issues garnered from surveyed U.K. businesses and charities.

Thirty-two percent of U.K. businesses surveyed identified cybersecurity breaches or attacks in 2018, and 48 percent of that group experienced at least one breach or attack per month. As well, around 60 percent of medium and large businesses reported cybersecurity breaches or attacks. While the overall number of businesses reporting breaches or attacks in this survey shows a decrease from 2017, the businesses that have reported cyberattacks are experiencing higher volumes of attacks than in the past.

DCMS presented some hypotheses for this trend, suggesting that businesses could stand to be more secure, or that attackers could be focusing more narrowly on larger businesses. DCMS also hypothesized that "[the EU General Data Protection Regulation] might have changed what businesses consider to be a breach, or led to some businesses becoming less willing to admit to having cyber breaches." The survey separately showed that the financial cost of cybersecurity breaches in which data or assets were lost has consistently increased since 2017.

UK National Cybersecurity Centre Releases Toolkit Supporting Corporate Defences

The U.K. National Cybersecurity Centre (NCSC), an independent government organization under the auspices of the U.K. Government Communications Headquarters (GCHQ) tasked with providing the private and public sectors with cybersecurity guidance, support and assistance with cybersecurity incident responses, recently released a "Board Toolkit."[4] The Toolkit emphasizes board responsibility for good cybersecurity practices, especially in light of high-profile media coverage of cyberattacks, their high risk and impact, and new regulations (such as the General Data Protection Regulation (GDPR)) "rais[ing] expectations of partners, shareholders, customers and the wider public." The Toolkit also provides boards with guidance on how to promote cybersecurity within their companies.

The NCSC also runs a "cyber accelerator"[5] (as a part of the U.K. National Cyber Security Strategy 2016-2021[6]), fostering the growth of cybersecurity startups that promise to bring "'better, faster and cheaper' security products to the market." These initiatives are geared toward making the private sector more self-sufficient when it comes to cybersecurity policies and more resilient to cyberthreats.

Key Takeaways

As 2019 has posed novel cybersecurity challenges for states and businesses, cybersecurity-related bodies both at the EU and the member state level are taking additional measures to increase cooperation and transparency in the interest of further cyber resilience. The approaches thus far have been all-encompassing, providing support for governments and corporations alike, signalling that the EU has a continued focus on preventing cyberattacks and promoting overall cybersecurity.

Return to Table of Contents

UK's Cybersecurity Agency Will Not Report Data Breaches to Regulator

Seeking to address a common concern about sharing cyberthreat information with government authorities, the U.K.'s national cybersecurity agency and data protection authority announced that information provided to the former will not automatically be shared with the latter.

[2] The commission's recommendation can be read here.

[3] The survey can be read here.

[4] The Board Toolkit can be found here.

[5] Information on the cyber accelerator can be found here.

[6] The U.K. National Cyber Security Strategy 2016-2021 can be found here.

The U.K.'s national cybersecurity agency announced that it will not automatically report data breaches to the country's data privacy regulator without the victim's consent. The joint decision of the NCSC and the Information Commissioner's Office (ICO), announced on April 25, 2019, is designed to address concerns that companies would be less willing to share information about data breaches with the NCSC out of concern of being fined by the ICO.

The European Union's GDPR allows the ICO to impose fines of up to 4 percent of a company's global revenue in the event of a data breach. The NCSC, a separate U.K. government agency from the ICO, is tasked with strengthening the U.K.'s national infrastructure against cyberattacks. It offers free, confidential advice to British businesses on how to mitigate cyberattacks and provides assistance to victims of such attacks. When the GDPR came into effect in May 2018, the NCSC worried that the threat of steep fines from the ICO would have a chilling effect on companies' willingness to provide information regarding cyberthreats they had experienced.

James Dipple-Johnstone, the ICO's deputy commissioner, said that while the regulator agreed to this "clarification of roles," organizations still have a legal obligation to report data breaches to the ICO, or risk substantial penalties. The decision means the NCSC may find itself in the potentially awkward position of knowing about GDPR violations and withholding that information from the ICO or other parts of government. The NCSC said in a statement that while it would not notify the ICO of breaches without the victim's permission, it would encourage organizations to comply with the law. The NCSC also said that it would seek to establish a similar arrangement with U.K. law enforcement agencies that investigate cyberattacks.

The NCSC has not seen any change in the number or size of breaches being reported since the GDPR took effect, according to Paul Chichester, the NCSC's director of operations, who commented on the announcement at a cybersecurity conference in Glasgow, Scotland, on April 24, 2019.

Key Takeaways

The joint announcement by the ICO and NCSC is intended to alleviate a common tension across many jurisdictions. Sharing information about cyberthreats helps the community at-large defend against those threats, but companies fear that disclosing attacks they have suffered may provide a roadmap for regulators and others to make claims against them.

Return to Table of Contents

UK Information Commissioner's Office Levies 'Unprecedented' Fine for Illegal Sharing of Personal Data

The U.K. data protection authorities have levied an unprecedented fine against a company that shared information about pregnant women and their children without providing proper notice.

On April 12, 2019, the U.K.'s ICO levied what it described as an "unprecedented" £400,000 fine to Bounty UK Ltd., a pregnancy and parenting club, for illegally sharing the personal data of more than 14 million people.[7] The ICO imposed the fine under the Data Protection Act of 1998 (DPA of 1998), the predecessor to the EU's GDPR and the U.K.'s Data Protection Act of 2018 (DPA of 2018), which implements the GDPR, but is nevertheless instructive for two reasons. Firstly, it shows that the DPA of 1998 continues to be relevant today, and, secondly, it is an indication of the types of behaviors that can still give rise to liability, even under the GDPR.

Bounty's Data Collection

Bounty is a pregnancy and parenting club headquartered in the United Kingdom. Founded in 1959, the company was initially a promotions business, offering sample products to new mothers through hospital networks across England and Wales. With the increasing prevalence of social media, Bounty expanded to offer fertility, pregnancy and parenting mobile apps, as well as free online guides to new parents. Bounty invited users to register for its digital platform and product distribution in three ways: in person at hospitals, through its mobile app or through its website. Bounty collected personal information of expecting parents as well as their newborn children through all three avenues.

Bounty's Privacy Policy

Bounty collected personal information from individuals, but did not always provide complete information on its privacy practices to the affected data subjects. For example, although Bounty shared personal information with a number of organizations, including credit reference and marketing agencies such as Acxiom, Equifax, Indicia and Sky, it did not identify all of these organizations until it updated its privacy policy in 2018. Furthermore, although Bounty made its privacy policy available on its website and on its mobile app, it did not provide the policy

[7] A copy of the ICO's decision is available here.

to users who registered in person. In other words, users who registered in person not only did not receive an initial general description of how their information may be shared with third persons, but they also did not receive the more specific listing of the actual organizations that would receive it.

Similarly, online users were given an option to opt-in to receiving marketing communications from Bounty and third parties, while in-person or "offline" users were given notice that their information may be shared, but no opportunity to opt-out.

Between June 1, 2017, and April 30, 2018, Bounty sent approximately 34.4 million records to Acxiom, Equifax, Indicia and Sky. Approximately two-thirds of the records shared consisted of data acquired through offline registrations.

The Data Protection Act of 1998

The ICO is the U.K.'s independent regulator for data protection charged with enforcing various data and privacy regulations, including the DPA of 1998. The office applied the DPA of 1998 to Bounty's actions because they took place before the GDPR and the DPA of 2018 took effect. The DPA of 1998 requires that personal data be processed fairly and lawfully, including in particular, the prohibition of the processing of personal data unless one of six conditions is met. The ICO looked closely at two of these conditions as potentially relevant:

- the data subject has consented to the processing; and
- the processing is necessary in order to pursue the legitimate interests of the "data controller" or "third parties" (unless it could unjustifiably prejudice the interests of the data subject).

Under the DPA of 1998, the ICO is authorized to impose monetary fines up to a maximum of £500,000, depending on various criteria, including the severity of the violation, whether the violation would likely cause substantial damage and whether the violation was deliberate.

ICO Decision

In finding Bounty violated the DPA of 1998, the ICO noted that the "fairness" requirement of data collection and processing imposed a transparency duty on data controllers to outline the purposes for which data subjects' information will be used, and that Bounty failed to fulfill that duty. In addition, the ICO stated that the "fairness" requirement also calls for data controllers to treat individuals fairly when using their personal data, including by setting "reasonable expectations of how their data will be used and not using their data in ways that risk causing them damage or distress, unless there is some sufficiently weighty justification for doing so." Regarding this final point, Steve Eckersley, ICO's director of investigations, shed some light on the office's special consideration given to pregnant women and young children as a uniquely vulnerable class of subjects, as well as the illegitimate purpose of collecting information for sale to unaffiliated third parties:

> "Bounty was not open or transparent to the millions of people that their personal data may be passed on to such large number of organisations. Any consent given by these people was clearly not informed. Bounty's actions appear to have been motivated by financial gain, given that data sharing was an integral part of their business model at the time.
>
> "Such careless data sharing is likely to have caused distress to many people, since they did not know that their personal information was being shared multiple times with so many organisations, including information about their pregnancy status and their children"

Importantly, the ICO found that, with respect to online users, the violations continued until Bounty updated its privacy policy to identify the specific organizations that received the information. For offline users — to whom Bounty never provided the original or amended policy — the ICO concluded that the violations were ongoing.

The fine, while not the maximum the ICO is authorized to impose under the DPA of 1998, reflects the seriousness of the violation, considering:

- the number of affected data subjects;
- the fact that some of the affected individuals' data was shared on multiple occasions;
- the sustained and prolonged duration of the violation;
- the vulnerability of the class of data subjects;
- the violation of the privacy notices;
- the nature of the data involved; and
- the loss of control over the data.

Furthermore, the ICO found that the violation was likely to cause substantial damage or distress, and that Bounty's actions in sharing the data were "plainly deliberate."

Key Takeaways

Despite the newer regulations, the ICO is still enforcing the DPA of 1998 despite newer regulations, including the DPA of 2018 and the GDPR, imposing even stricter obligations on companies that collect and process data, and authorizing enforcement agencies to levy even harsher fines in the event of a breach. As

demonstrated by the Bounty case, the ICO is closely reading privacy policies and carefully reviewing the opportunities that data subjects are offered to opt out. As such, companies that sell information to third parties need to be transparent with their users that they are doing so.

Return to Table of Contents

SEC Reminds Firms to Follow Their Privacy Policies

The SEC has issued a risk alert identifying a range of privacy and cybersecurity compliance issues its staff has identified in the past two years. Many of these issues relate to failure to properly implement firms' written policies

On April 16, 2019, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) released a risk alert reminding investment advisers and broker-dealers that they must actually implement the promises they make with respect to protecting investors' personal information in order to fulfill their regulatory obligations.[8] The OCIE explained that it had found a number of firms had inadequate policies, or had failed to implement the measures they described in their policies, thus prompting the alert. The risk alert provided useful guidance to firms on the OCIE's priorities with respect to privacy policy and related implementation requirements.

Regulation S-P and Required Privacy Practices

In the risk alert, the OCIE reminded firms that Regulation S-P requires firms to provide clear and conspicuous notice to their customers that accurately reflects their privacy policies and practices, to update that notice annually, and to accurately explain to investors their right to opt out of certain types of personal information disclosures. The regulation explains what must be included in these privacy and opt-out notices.

In addition, Regulation S-P's Safeguard Rule requires firms to adopt written policies and procedures that address the administrative, technical and physical safeguards firms use to protect customer records and information. These must be "reasonably designed to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of [investor] records and information, and protect against unauthorized access to or use of [investor] records or information that could result in substantial harm or inconvenience to any [investor]."

Common Deficiencies in OCIE Investigations

The OCIE's risk alert identified a number of common issues it has encountered over the last two years with respect to complying with these Regulation S-P requirements.

Lack of Required Notices

First, the OCIE reported a number of deficiencies with respect to the actual notices given to investors. It found that a number of firms did not provide the required notices when establishing the initial relationship with the investor, did not provide the required annual update notice and/or did not provide the required explanation of the investors' opt-out rights.

Lack of Written Internal Policies

Second, the OCIE found that some firms did not have the written policies for protecting customer information required under the Safeguards Rule. Some firms' policies simply restated the Safeguards Rule, but did not include policies and procedures for the actual safeguards. Others had policies and procedures that still contained blank spaces to be filled in by the firms. Still others had policies for delivering required privacy notices, but lacked any description of personal information safeguards.

Implementation and Adequacy Issues

Finally, the OCIE identified a number of examples of situations where it found that firms either did not adequately implement the policies they provided to investors or that the policies did not properly address the potential risks to investor information. Specifically, the OCIE identified 10 different areas where it found issues:

- **Personal Devices.** Policies and procedures did not appear reasonably designed to safeguard investor information on personal devices. The OCIE's staff found that some firm employees regularly stored and maintained investor information on their personal laptops, but that the firm's policies and procedures did not address how to properly protect this information on these devices.
- **Electronic Communications.** Policies and procedures did not address the inclusion of personal information in electronic communications. For example, the OCIE's staff found firms that did not appear to have policies and procedures reasonably designed to prevent employees from regularly sending unencrypted emails containing this information.

[8] The risk alert is available here.

- **Training and Monitoring.** Firms failed to properly train employees on how to follow their policies and procedures. For example, the OCIE found that some firms had policies and procedures that required investor information to be encrypted, password-protected and transmitted using only registrant-approved methods, but that employees were not provided adequate training on these methods and the firm failed to monitor if the policies were being followed by employees. This lack of training and monitoring rendered the policies and procedures themselves inadequate under Regulation S-P.
- **Unsecure Networks.** Policies and procedures did not prohibit employees from sending investor personal information to unsecure locations outside of the firms' networks.
- **Outside Vendors.** Some firms failed to follow their own policies and procedures regarding outside vendors. For example, the OCIE's staff found firms that failed to require outside vendors to contractually agree to keep investors' personal information confidential, even though such agreements were mandated by the firms' policies and procedures.
- **System Inventory.** Policies and procedures did not identify all systems on which the firm maintained investor personal information. Without an inventory of such systems, the OCIE staff noted, firms may be unaware of the categories of information that they maintain, which could limit their ability to adopt reasonably designed policies and procedures, and adequately safeguard that information.
- **Incident Response Plans.** Written incident response plans did not address important incident response topics, such as role assignments for implementing the plan, actions required to address a cybersecurity incident and assessments of system vulnerabilities.
- **Insecure Physical Locations.** Unsecure physical storage of investor information, such as in unlocked file cabinets in open offices.
- **Login Credentials.** Login credential practices were not secure, such as using login credentials that had been disseminated to more employees than permitted under the firms' policies and procedures.
- **Departed Employees.** Instances existed where former employees retained access rights after their departure and therefore could access restricted investor information.

Key Takeaways

The OCIE's risk alert highlights the care that firms should take in designing and implementing their cybersecurity and data privacy policies to ensure that they adequately address the risks that they face. Further, it is important for firms to not simply adopt a "boilerplate" policy and assume they have satisfied their regulatory obligations. Rather, firms should be sure to adapt the policies to meet their regulatory obligations and to reflect their actual practices, and then train their staff on how to comply with the policies they adopt.

Return to Table of Contents

Canadian Privacy Commissioner Concludes Investigation into Equifax Breach

The Office of the Privacy Commissioner of Canada (OPC) recently concluded its investigation on the impact of the Equifax breach on Canadians. In its report, the OPC found that Equifax Canada and its U.S.-based parent company fell short of its obligations under Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

On April 9, 2019, the OPC released its report on the 2017 Equifax data breach, outlining how the actions of Equifax and its Canadian-based subsidiary Equifax Canada, impacted Canadians. The report concluded that the two companies had failed to meet their obligations under Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).[9]

Background on the Equifax Breach

In September 2017, U.S.-based credit reporting company Equifax publicly announced that attackers gained access to the personal information of more than 143 million individuals, including approximately 19,000 Canadians who had purchased credit monitoring or fraud alert products from Equifax Canada. Almost all of the impacted Canadians had their social insurance number and other accompanying identifying information compromised.

According to the OPC's report, the attackers gained access to Equifax's systems in May 2017 and operated undetected for more than two months. Equifax did not notify Equifax Canada of the breach until shortly before Equifax disclosed the breach to the public in July 2017. Canadians who were impacted by the breach did not receive notifications that their personal information had been compromised until October 2017.

Although Equifax Canada provided free credit monitoring to the affected Canadians, the company did not provide the same post-breach protections that its U.S. parent company provided. For example, Equifax offered Americans the opportunity to freeze

[9] The full text of the OPC report can be found here.

their credit files, while Equifax Canada did not provide that same credit freeze option to affected Canadians.

The OPC Report

After investigating the cause of the breach and the impact on Canadian residents, the OPC published a report that addressed the gaps in Equifax and Equifax Canada's data protection practices and makes several recommendations for Equifax and Equifax Canada going forward. The report noted the following gaps with respect to Equifax and Equifax Canada's compliance with PIPEDA:

- Equifax and Equifax Canada did not provide safeguards appropriate to the sensitivity of the personal information at issue;
- Equifax did not comply with PIPEDA's data retention and destruction requirements;
- Equifax Canada did not demonstrate adequate accountability for protecting the personal information of Canadians; and
- Equifax Canada did not provide mitigation measures to the affected individuals that were adequate to protect their personal information from unauthorized use, such as future identity theft.

The OPC also found that Equifax Canada failed to obtain express consent to transfer personal information to a separate entity in the U.S. PIPEDA generally requires organizations to obtain express consent prior to such a transfer, where individuals would not reasonably expect the cross-border transfer of their information to a separate entity or where the proposed transfer involves certain types of sensitive information. Equifax Canada's Canadian customers interacted exclusively with Equifax Canada and were not given any express notice that their information would be processed in the U.S. However, the OPC concluded that Equifax Canada acted in good faith in not seeking express consent for these disclosures because of previous OPC guidance that indicated that the transfers at issue did not require express consent.

- The OPC concluded the report with the following recommendations to Equifax Canada:
- implement a procedure to ensure that the written arrangement between Equifax and Equifax Canada concerning the collection and disclosure of Canadian personal information remains up to date;
- implement a robust monitoring program to ensure compliance with that written arrangement;
- identify personal information that should no longer be retained by Equifax according to a set retention schedule, and delete such information; and
- every two years for a six-year term, provide the OPC (1) a report regarding the monitoring program described above, (2) an audit report and certification conducted by an appropriate external auditor against an acceptable security standard that covers all Canadian personal information for which Equifax Canada is responsible, including information processed by Equifax, and (3) a third-party assessment of Equifax's data retention practices that covers all Canadian personal information processed by Equifax.

Equifax Canada entered into a compliance agreement with the OPC under which Equifax Canada agreed to comply with these recommendations and other requirements aimed at improving Equifax Canada's data protection practices.[10] For example, the agreement also requires Equifax Canada to improve the process by which it obtains consent to transfer personal information. As part of the agreement, Equifax Canada also agreed to extend its free credit monitoring service to impacted Canadians. However, Equifax Canada did not agree to provide the free or low-cost credit freeze product offered to impacted Americans after the breach.

Key Takeaways

The Equifax breach and the OPC's response provides a useful reminder about the importance of compliance with local data protection laws to companies that store or process personal information from consumers in multiple jurisdictions. Years after the breach, Equifax and its local subsidiaries remain subject to extensive audit periods from government regulators and increased obligations to improve and maintain their data protection practices. The potential costs of a breach can outweigh the costs of implementing and maintaining comprehensive data protection policies and practices.

Return to Table of Contents

Eleventh Circuit Finds no Coverage Under CGL Policy in Junk Fax Putative Class Action

A federal appeals court, applying Georgia law, recently held that Travelers unit St. Paul Fire & Marine Insurance Company (St. Paul) did not need to cover a multimillion-dollar settlement in a junk fax putative class action alleging Telephone Consumer Protection Act (TCPA) violations. According to the court, the alleged unsolicited faxes did not constitute an "accident" under St. Paul's insurance policies — a condition precedent to coverage.

On April 12, 2019, the Eleventh Circuit affirmed a district court's holding that St. Paul has no obligation under a series of commercial general liability (CGL) policies issued to Atlanta-based

[10] The full text of the compliance agreement can be found here.

manufacturing sourcing provider MFG.com (MFG) to cover a $22 million settlement reached in a putative class action alleging TCPA violations.[11]

The Junk Faxes

As part of a fax advertising campaign, MFG purchased lists of individuals who MFG believed had consented to receive marketing materials via fax. Between September 2005 and November 2008, MFG sent approximately 494,212 unsolicited fax advertisements to those individuals. Although MFG believed that its advertising campaign complied with all applicable laws, MFG was mistaken, as the fax recipients had not in fact consented to MFG's unsolicited advertisements. The junk faxes allegedly caused property damage to the fax recipients in the use of their fax machines, depleting their ink and paper.

The St. Paul Policies

At the time MFG sent the junk faxes, it had in place a series of CGL policies (the policies) that covered liability for "property damage" caused by an "event." The policies defined "property damage" as "physical damage to tangible property of others, including all resulting use of that property" or "loss of use of tangible property of others that isn't physically damaged." The policies defined "event" as "an accident, including continuous or repeated exposure to substantially the same general harmful conditions." The policies did not define "accident."

The TCPA Putative Class Actions

In November 2008, G.M. Sign, Inc. (GM Sign), a commercial sign manufacturer and recipient of MFG's junk faxes, commenced a putative class action in Illinois state court against MFG. The lawsuit alleged that MFG sent GM Sign and the putative class members fax advertisements without their permission, in violation of the TCPA. MFG noticed the claim to St. Paul, which denied coverage.

MFG removed the underlying case to federal court, and on July 29, 2009, the parties stipulated to dismiss the lawsuit without prejudice to refile. One day later, GM Sign commenced another lawsuit in Illinois state court alleging the same TCPA claims on behalf of the same putative class. The lawsuit eventually settled for $22,536,500, though the parties agreed that MFG would pay only $460,000 of that amount. MFG then assigned to GM Sign and the putative class MFG's claims against and rights to payment, if any, under the policies.

The Coverage Action and the District Court's Decision

GM Sign, as assignee of MFG's rights under the policies, then filed a declaratory judgment action against St. Paul in Georgia state court seeking a declaration that the policies covered the settled claims. St. Paul removed the coverage action to Georgia federal court and filed a counterclaim that it owed no coverage. On the parties' cross-motions for summary judgment, the court granted St. Paul's motion, holding that under the Eleventh Circuit's decision in *Mindis Metals, Inc. v. Transportation Insurance Co.*, "the intentional delivery of fax advertisements does not qualify as an 'accident' under Georgia law, even if the sender erroneously believed that it had consent to send the fax advertisements." GM Sign appealed.

The Eleventh Circuit's Decision

The Eleventh Circuit agreed with St. Paul and the district court, holding that the settled TCPA claims were not covered under the policies because the alleged property damage was not caused by an "accident," a condition precedent to coverage. In reaching its conclusion, the court determined that it was bound by its decision in *Mindis Metals*, which held that intentional conduct premised on erroneous information does not constitute an accident. "MFG intended to send the faxes and thus intended to cause the resulting property damage, the use of the fax machines and the depletion of the machines' ink and paper," the court wrote. Moreover, "[t]he fact that MFG mistakenly thought the recipients had consented to receive the faxes is insufficient under *Mindis Metals* to render the property damage an accident under Georgia law." Accordingly, the court concluded, the settled TCPA claims were not covered under the policies.

Key Takeaways

As the court's decision in *G.M. Sign* illustrates, TCPA claims may not fit neatly into coverage. However, given the increased frequency of TCPA lawsuits in recent years and their significant costs, policyholders should nonetheless consider all coverage lines that may respond to such claims, including, for example, CGL, directors and officers liability, errors and omissions liability and cyber liability. In addition, policyholders faced with TCPA exposure would be well-advised to proactively work their insurance brokers, advisers and carriers in an effort to obtain the most favorable coverage possible.

Return to Table of Contents

[11] *G.M. Sign, Inc. v. St. Paul Fire & Marine Ins. Co.*, No. 17-14247, 2019 WL 1579792 (11th Cir. Apr. 12, 2019).

Privacy & Cybersecurity Update

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

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@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

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

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@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

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

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