Skadden

Privacy & Cybersecurity Update

Landmark Data Breach Class Action Brought Against Equifax Limited

A landmark data breach class action seeking £100 million in compensation recently was launched in the English High Court against credit reference agency Equifax Limited (Equifax U.K.), relating to the agency's failure to protect the personal information of approximately 15 million individual records during a cyberattack in 2017.

Background

In 2017, Equifax Inc. suffered a cyberattack in the U.S. affecting more than 147 million customers globally across a broad range of personal data, including names, dates of birth, home addresses, telephone numbers, passwords, driver's licenses, credit card numbers, email addresses and financial details. Some of the data affected was from U.K. data subjects, including information that should have been migrated to the U.K. as part of the transfer of data from Equifax Inc. to Equifax U.K. It took Equifax Inc. a month after the breach occurred to tell Equifax U.K. of the attack and two months after the breach to notify the U.K. Information Commissioner (ICO).

Equifax U.K. informed the ICO that the compromised data was held in a plaintext file, which it described in the regulatory investigation as a "snapshot in time" of the dataset, rather than the actual database. The ICO observed, however, that passwords were stored in plaintext form, going against the company's data handling and cryptography standards that required passwords "to be stored in encrypted, hashed, masked, tokenized or [an]other approved form."

Working in tandem with the Financial Conduct Authority (FCA), the ICO revealed serious inadequacies relating to data retention and the safeguarding of data transferred outside the European Economic Area, thereby increasing the likelihood of unauthorized access. The ICO also found that the breach could have been prevented, as Equifax Inc. had been warned by the U.S. Department for Homeland Security in March 2017 about the vulnerability that was exploited by the cyberattack. The gravity of the situation was further highlighted in a letter from FCA Chief Executive Andrew Bailey to the former Chair of the House of Commons Treasury Committee Nicky Morgan, which outlined the potential serious harm of the attack to consumers, as well as the concerning delay of Equifax U.K. to establish and report the full facts to the FCA.

The Regulatory Findings

The ICO concluded that Equifax U.K. had contravened multiple data protection principles in the Data Protection Act 1998 (DPA 1998),[1] including:

- principle 1 (fair and lawful processing of data);
- principle 2 (obtaining personal data only for one or more specified lawful purpose);
- principle 5 (poor retention practices);
- principle 7 (failure to secure personal data); and
- principle 8 (lack of legal basis for international transfers of U.K. citizens' data to the U.S.).

In September 2018, the ICO fined Equifax £500,000 for failing to protect the personal information of U.K. citizens. The monetary penalty imposed upon Equifax U.K. was the maximum that could be administered under the DPA 1998 at the time.

2018 High Court Action

The Particulars of Claim dated October 16, 2019, stipulates that it is a representative action brought by Richard Atkinson against Equifax U.K. on his own behalf and on behalf of members of the class (the claimants) pursuant to Rule 19.6 of the Civil Procedure Rules (CPR). The claim consists of damages for:

- misuse of private information;
- breach of statutory duty pursuant to Section 13(1) of the DPA 1998; and
- loss of control of personal data and privacy rights.

The claim is based on the premise that the claimants' private information, including personal data, was that which "the claimant had a reasonable expectation of privacy," but was unjustifiably infringed and misused as Equifax U.K. failed in its role as a data controller to take adequate steps to protect such private information.

Key Takeaways

The class action launched against Equifax U.K. in the High Court is significant for several reasons. First, it is among the first data breach class actions that have been permitted to proceed in English courts, and now that there is some precedent for allowing data breach class actions to proceed, the number of such actions may increase. Second, this class action follows an amendment of the CPR by the CPR Committee (an advisory, nondepartmental public body sponsored by the Ministry of Justice) whereby any misuse of private information and data protection claims shall be issued in the Media and Communications List. This indicates that English courts intend to have personal data breach cases heard by the most technically proficient and specialist judges.

[1] Note that the Equifax case arose before the General Data Protection Regulation had been implemented.

FTC Files Complaint Against RagingWire for Misrepresenting Participation in EU-US Privacy Shield

The Federal Trade Commission (FTC) filed a complaint against Nevada data colocation services company RagingWire Data Centers, Inc. (RagingWire) for misrepresenting its participation in the EU-U.S. Privacy Shield and failing to comply with the Privacy Shield while it was a participant.

Background

The EU-U.S. Privacy Shield Framework (Privacy Shield) was designed by the U.S. Department of Commerce and the European Commission to provide a mechanism for companies to transfer personal data from the EU to the U.S. in a manner deemed adequate under EU data protection standards. To join the Privacy Shield, a U.S.-based organization is required to self-certify with the Department of Commerce and publicly commit to comply with Privacy Shield principles and related data requirements. The framework requires U.S. companies to be transparent about their privacy practices and describe such practices in a public notice. The FTC enforces the commitments companies make when joining the Privacy Shield under Section 5 of the Federal Trade Commission Act.

RagingWire Complaint

RagingWire is a data colocation services company that offers specialized storage facilities for servers owned and operated by its customers. The company obtained its Privacy Shield certification in January 2017, and, according to the complaint, its certification lapsed in January 2018. However, until October 2018, the company continued to state in its online privacy policy and sales materials that it was compliant under the Privacy Shield. Between January and October, the Department of Commerce warned RagingWire on two separate occasions to remove its false Privacy Shield claims unless it took steps to renew its participation. According to the complaint, RagingWire did not remove its Privacy Shield statements until October 2018, when it was contacted by the FTC.

The complaint alleged one count of misrepresentation in connection with RagingWire's claims of Privacy Shield participation during the period that it was no longer certified to the framework. The complaint also alleged that during the time RagingWire was a participant in the Privacy Shield, it failed to comply with certain requirements. Specifically, the complaint alleged that RagingWire failed to (a) annually verify, through either self-assessment or outside compliance review, assertions it made about Privacy Shield practices as required by the framework; (b) provide independent dispute resolution services for customers with privacy-related complaints as required by the Privacy Shield; and (c) notify and affirm to the Department of Commerce that, when its certification had lapsed in 2018, it would either take steps to continue to comply with the Privacy Shield or delete or return EU data as required by the framework. For these alleged failures to comply with the requirements of the Privacy Shield, the FTC also raised three counts of misrepresentation regarding verification, dispute resolution and continuing obligation practices.

The complaint issued a proposed order to prohibit RagingWire from making misrepresentations about the company's participation in or compliance with the Privacy Shield in the future. It also issued a proposed order requiring that, in the event that RagingWire withdraws or allows its certification to the framework to lapse in the future, the company continues to apply Privacy Shield protections to personal information it collected while participating in the program, or return or delete the information.

Key Takeaways

U.S. companies that self-certify under the Privacy Shield must be careful to remain compliant with the framework after they have self-certified, and be sure to delete any reference to the Privacy Shield in external documents if they are no longer certified.

Utah-Based Business-to-Business Company Settles FTC Allegations Over Failure To Safeguard Data

Pursuant to a settlement reached with the FTC, InfoTrax Systems, L.C. (InfoTrax), a Utah-based business-to-business company, will have to comply with certain affirmative obligations for the next 20 years, including implementing a comprehensive information security program, obtaining biennial assessments of the program by a third party and certifying its compliance with the program. The settlement resolves FTC allegations that the company failed to implement readily available and low-cost security measures, which allowed a hacker to obtain the personal information of approximately 1 million consumers.

Background

InfoTrax serves multilevel marketers, which are defined as marketers who encourage existing product distributors to recruit new distributors by giving them a percentage of their recruits' sales. The company typically operates the marketers' website portals, which individuals use to register as distributors, place orders for products on behalf of themselves and the consumers who purchase from them, and enroll new distributors. In performing these activities, distributors provided InfoTrax with the personally identifiable information of approximately 11.8 million consumers, including Social Security numbers, bank account and payment card information, and accounts' user IDs and passwords. By contract, InfoTrax assumed responsibility for the security of this consumer information.

During a nearly two-year period between 2014 and 2016, a hacker accessed InfoTrax's servers more than 20 times by exploiting a network vulnerability. The hacker uploaded malicious code, allowing remote access to query databases on the company's server and obtain the personal information of consumers, including legacy data that InfoTrax allegedly did not know existed because it had not conducted a data inventory. The hacker also used a distributor's stolen user ID and password to access that distributor's website portal, enabling it to obtain credit card information and install malicious code that provided elevated access to infiltrate another InfoTrax client's web portal. InfoTrax only discovered the intrusion when it began receiving alerts that one of its servers had reached maximum capacity because a data archive file the hacker had created caused the server to run out of space.

The hack resulted in unauthorized credit card charges, fraudulent opening of new credit lines, tax fraud and the misuse of information for employment purposes. The hack also incurred costs to InfoTrax's clients who dealt with fallout from the breach, including costs associated with providing notice to consumers pursuant to data breach notification laws.

The FTC's Allegations

The FTC's complaint alleged that InfoTrax violated Section 5(a) of the Federal Trade Commission Act by failing to employ reasonable data security practices.[2] Specifically, the complaint alleged that InfoTrax engaged in unfair practices by failing to:

- have a systemic process for inventorying and deleting personal information that was no longer needed;
- perform adequate code review of its software and penetration testing of its network and software;
- implement protections, such as input validation, against malicious file uploads;
- limit the locations to which third parties could upload unknown files on the network;
- segment its network so one client would not have access to another client's data;
- implement safeguards to prevent or detect intruders' unauthorized access, queries, file alterations and data exfiltrations; and
- encrypt personal data so it was not stored in "clear, readable text."

The FTC alleged that InfoTrax could have addressed each of these failures by implementing "readily available and relatively low-cost security measures." It also alleged that the company's distributors and consumers who bought the distributors' products had no way of knowing about these security failures.

The agency also named the company's CEO as a defendant because he "reviewed and approved InfoTrax's information technology security policies, regularly discussed data security issues with clients, was involved in the company's long-term data security strategy, studied computer science in college, and listed his college study of computer science on the InfoTrax website as part of his biography."

The Settlement

Under the FTC's consent order, InfoTrax must undertake several affirmative obligations for the next 20 years or risk losing the ability to deal with personal information. The company must implement an information security program that, at a minimum, provides for the deletion of unnecessary personal information; software code reviews and penetration testing; limitations on the locations to which third parties can upload files; network segmentation so one client cannot access another client's data; encryption of personal information; and mechanisms to detect network intruders, unauthorized file alterations and the exfiltration of data outside the network. InfoTrax also must conduct yearly testing of these safeguards, retain a third party to assess its security efforts every two years, keep detailed records demonstrating compliance with the consent order and annually certify its compliance with the information security program. In addition, the company must provide detailed reports to the FTC for any future incident that triggers data breach notification laws. The consent order carries the force of law and each violation may result in a civil penalty of up to $42,530.[3]

Key Takeaways

Companies and their executives face potential liability for failing to implement reasonable data protection and cybersecurity measures, regardless of whether the business' end customers are consumers or other businesses. The FTC's decision to name the CEO in his individual capacity underscores the importance of carefully reviewing the statements a company and its executives make about data security practices. To avoid such liability, companies should review their data security practices to ensure they are meeting the standards set forth in the consent order and ensure their statements about their data security practices are accurate.

[2] The complaint is available here.

[3] The order is available here.

2020 Cybersecurity Protocol for International Arbitration Released

A new cybersecurity protocol for international arbitration was released on November 21, 2019. The protocol provides a framework for determining reasonable information security measures for individual arbitration matters and increases awareness about information security in international arbitrations.

The Protocol on Cybersecurity in International Arbitration[4] (protocol) is the culmination of two years of work by the ICCA-NYC Bar-CPR Working Group on Cybersecurity in International Arbitration, consisting of representatives of the International Council for Commercial Arbitration (ICCA), New York City Bar Association (City Bar) and International Institute for Conflict Prevention & Resolution (CPR).

The protocol reviews the importance of cybersecurity in arbitration, which has become a largely digital process; the high stakes and risks inherent in international arbitration, including the concerns surrounding the cross-border nature of the process, which often involves extensive travel and the use of multiple networks; and factors to be considered when developing reasonable cybersecurity measures. While arbitration is not uniquely vulnerable to data breaches, the process is not immune to the increasingly pervasive cyberattacks against corporations, law firms, government agencies and individuals. The working group recognized that the credibility and integrity of any dispute resolution process depends on maintaining a reasonable degree of protection over the data exchanged during the process.

The protocol recognizes that there is no one-size-fits-all solution for arbitrations. Accordingly, it includes 14 principles that address the protocol's scope and applicability; establishes a standard of reasonableness; sets out a series of factors to be considered in determining what information security measures are reasonable in a particular matter (and how they should be applied); and suggests procedural steps to address information security issues in an individual arbitration. The protocol also includes schedules that contain more detailed guidance on appropriate baseline security measures, a checklist of risk factors that can be used to assess the risk profile of a particular arbitration, examples of information security measures and sample language for incorporating security measures into an arbitration clause or procedural order.

[4] The 2020 Edition of the Cybersecurity Protocol for International Arbitration is available here.

The working group published an initial consultation draft in April 2018, together with a request for comments that was sent to more than 240 individual consultees representing arbitral institutions, law firm arbitration practice groups, expert witnesses in arbitration proceedings and nongovernmental organizations, such as bar associations. Since then, the working group also solicited feedback at more than 25 public workshops and other events held around the world. The 2020 edition of the protocol reflects that feedback. As the subject area is rapidly evolving, the working group will solicit feedback from users of the protocol and anticipates issuing updated editions from time to time in coming years.

Target Seeks Coverage Under General Liability Policies for Claims Arising From 2013 Data Breach

Retail giant Target Corporation (Target) recently brought a suit against two of its general liability insurers for their alleged wrongful denial of coverage for claims related to a 2013 data breach that compromised the payment card data of millions of Target customers. Target alleges that the claims, which were brought by financial institutions seeking damages for the costs associated with cancelling and reissuing physical payment cards, fall squarely within the policies' "property damage" liability coverage.

On November 15, 2019, Target filed a complaint in the U.S. District Court for the District of Minnesota against two of its primary and excess general liability insurers, Chubb units ACE American Insurance Co. and ACE Property & Casualty Insurance Co. (collectively, ACE), alleging that ACE wrongfully denied coverage for claims brought by banks against Target for the costs associated with cancelling and reissuing physical payment cards to customers whose cards were compromised in a 2013 data breach.

The Data Breach Litigation

According to the complaint, in December 2013, Target discovered that a hacker had installed malicious software on the company's network that allowed the hacker to steal credit and debit card information from millions of customers. The data breach allegedly rendered the payment cards unusable, forcing financial institutions to cancel the compromised cards and issue replacement cards to customers.

The financial institutions subsequently sued Target, seeking damages for the costs associated with cancelling and reissuing the cards, which included the cost of producing the plastic

cards, mailing the cards to customers and otherwise reissuing the physical cards.[5] According to Target's complaint, the financial institutions alleged that as a result of the data breach, the physical payment cards associated with the compromised accounts could no longer be used and that the financial institutions were forced to dedicate substantial resources to cancelling and reissuing physical payment cards. Target eventually reached settlements with the financial institutions totaling approximately $138 million, at least $74 million of which went to settle claims for costs attributable to replacing compromised payment cards.

ACE's Denial of Coverage and Target's Suit Against ACE

Target alleges that it sought and was denied coverage under the ACE policies for the settlement amounts related to the replacement of payment cards. After unsuccessful attempts to resolve the dispute, Target commenced suit against ACE for breach of contract and declaratory relief.

According to Target's complaint, the policies provide coverage for loss because of "property damage," which is defined to include "[l]oss of use of tangible property that is not physically injured." Target alleges that this definition covers "precisely this case" because the company "was held liable for the loss of use of plastic payment cards that were not physically injured."

ACE has not yet responded to the complaint.

Key Takeaways

This case raises an important question for both policyholders and insurers: whether a traditional general liability policy can provide coverage for loss of use of physical property resulting from a data breach or other cyber incident. Additionally, while the scope of coverage available for any given cyber incident always will depend on the particular loss scenario and policy language, this case serves as an important reminder to policyholders and insurers to review their insurance policies to determine the scope of coverage provided for cyber incidents.

[5] The financial institutions also sought damages for the cost of credit card fraud perpetrated against certain Target customers as a result of the data breach, but the company's lawsuit does not seek coverage for such costs from ACE.

IAPP Holds European Data Protection Congress in Brussels

In November 2019 the International Association for Privacy Professionals (IAPP) held its European Data Protection Congress in Brussels (Congress), bringing together a range of data privacy professionals for two days to share ideas on the current and future state of data privacy.

While last year's Congress aimed to set the tone for what General Data Protection Regulation (EU) 2016/679 (GDPR) implementation and enforcement entailed, this year's discussion focused on: (1) EU data protection authorities' efforts to engage in dialogues with companies and outlining sets of corrective measures to be used instead of the threat of GDPR fines; (2) the increasing level of cooperation between EU data protection authorities and competition, consumer law and financial authorities, (3) the development of artificial intelligence (AI) systems and the associated data protection and ethics risks; (4) the notion of joint controllership under the GDPR; and (5) the introduction of the California Consumer Privacy Act (CCPA). These five focus areas are discussed below.

Enforcement

Data security is key in any transaction and the focus increasingly is on preventing data processing activities that would put data at risk due to a lack of compliance with applicable data protection laws. Irish Data Protection Commissioner Helen Dixon shed light on the importance of coaching companies to correct areas of noncompliance and encourage greater compliance within organizations. A representative from the EU Commission emphasized that while fines need to remain proportionate, they also must act as a deterrent. What is yet to be observed is the interpretation of GDPR requirements by national courts and how the protection of fundamental rights at the national level will be affected in coming cases.

Privacy and Competition Authorities

EU Commissioner for Competition Margrethe Vestager, who was nominated as executive vice president-designate of the EU Commission for a Europe fit for the Digital Age in 2019, was invited to speak at the closing session of the Congress. In Vestager's words, controlling data can "shut up" competition. People share much more online than in the physical world and it is now easier to manipulate online data sets. When reviewing mergers,

the EU Commission will not refrain from prescribing a series of commitments to ensure continued competition by allowing continued access to data, while being mindful of GDPR requirements. An example of this would be obliging a purchaser to share data with external parties within the same industry post-merger in a GDPR-compliant manner. This was echoed by a representative of the Dutch Competition and Consumer Authority (CCA), who confirmed that the CCA regularly consults their data protection peers as data protection can be a parameter of competition. Where a merger case gives rise to a conflict of laws between competition and data protection laws, the CCA gives priority to data protection laws. Similarly, if companies jointly agree not to impose privacy standards beyond the statutory minimum in order to gain further market share and reach a dominant status in said market, competition authorities would analyze this pattern through the lens of data protection laws and notify such market players that this would lead to a breach of competition law.

Artificial Intelligence

The AI panel, which included a lawyer and a data scientist, shed light on the impact of data protection legal requirements on the day-to-day work of data scientists when creating algorithms for AI systems. For example, the panel discussed requiring some level of explainability at each stage of the AI creation process to account for and justify the decision points that led to the processing of the input data to the outcome data. As part of this, the panel said AI systems should incorporate data protection training within the system through human input to enable companies using it to be in a position to address data subject rights (*e.g.* access rights or the right to be forgotten). The panel noted the growing standard among data scientists, when building AI systems, of responsible disclosure in order to reconcile the benefits of open AI while respecting individuals' civil liberties. Further concerns the panel raised about ethics and individual rights surrounding the use of AI systems centered on the use of personal data for secondary purposes and the practical effect of data minimization.

Joint Controllership

While a few recent cases at the Court of Justice of the European Union (CJEU) have given rise to fears of potentially broadening the definition of joint controllers as defined under Article 26 of the GDPR, we are still awaiting official regulatory guidance from the European Data Protection Board that would clarify the matter. Additionally, further clarity is needed regarding joint controllers and the obligations and liability resulting from data subject requests, as well as regulatory and legal action. So far, the CJEU clarified in the *Fashion ID* case[6] that for a joint controllership to exist, there must be a unity of purpose (in the form of a shared interest, which can be of economic nature) and means between the joint controllers. Additionally, the CJEU clarified that when looking at whether a joint controllership would be aligned with GDPR requirements (1) joint controllers would be able to rely on the legitimate interests as the appropriate legal ground for the processing of the data and (2) it is the "first data controller" from a chronological standpoint (*e.g.* the organization who puts up a social plug-in is obliged to seek individuals' consent to do so and is better placed to address any future data subject rights requests) who would be responsible for obtaining consent and responding to data subject rights requests.

California Consumer Protection Act

Aside from the GDPR, the Congress also heavily discussed the CCPA, which is set to be enforced beginning January 1, 2020. As there was with the introduction of the GDPR, there is a degree of uncertainty around how to comply with a new piece of legislation, especially given that it does not directly overlap with GDPR requirements. Further, the draft CCPA was only published for notice and comment in October 2019 and the legislation is not expected to be finalized by California's attorney general until March 2020, adding another level of anxiety for businesses.

Key Takeaways

The rate of development in the data protection space continues its rapid pace and the topics considered at this Congress will undoubtedly evolve considerably over the coming year as new concerns arise for companies. Thoughtful consideration should be given to the matters discussed at the Congress, however, as a broad spectrum of companies and organizations are affected by data protection matters.

[6] Please see our discussion of this case in the September 2019 edition of our *Privacy & Cybersecurity Update* here.

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
213.687.5381
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

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

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