Skadden

Privacy & Cybersecurity Update

1 New Jersey Expands Definition of 'Personal Information' to Include Information Used to Access Online Accounts

2 Washington State Amends Data Breach Notification Law

3 Danish and UK Data Protection Authorities Provide Guidance on Customer Call Recording Under the GDPR

4 SEC Issues Risk Alert Regarding Cloud-Based Storage

5 Verizon Releases Annual Data Breach Investigations Report

6 FTC Requests Federal Privacy and Data Security Legislation

New Jersey Expands Definition of 'Personal Information' to Include Information Used to Access Online Accounts

New Jersey has broadened its definition of "personal information" to include information that would permit access to any online account. Under the new law, a breach of such information would trigger the notification requirements.

On May 10, 2019, New Jersey Gov. Phil Murphy signed into law an amendment to the state's data breach notification law.[1] The amendment requires New Jersey businesses and New Jersey state and local entities to notify state residents of any breach of security related to information that permits access to online accounts.

Prior to the amendment, businesses and public entities were required to disclose breaches involving "personal information," where such information referred to an individual's first name (or first initial) and last name linked with any specified data points. Those specified data points consisted of the individual's Social Security number, driver's license number, state identification card number, financial account number, or credit or debit card numbers combined with any required security code, access code or password that would permit access to the individual's financial accounts.

The amendment broadens the definition of "personal information" to include "user name, email address or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account." Thus, under the amended law, a breach of information permitting access to any online account, rather than just a financial account, would trigger the notification requirements.

The amendment further provides that, in the case of a security breach involving information permitting access to an online account, the entity that experienced the breach may provide the required notice to New Jersey residents by electronic or other means directing the affected individual to change any password, security question or answer, as applicable, or to take other suitable steps to protect the applicable online account. The entity may not, however, provide notice to an email account affected by the security breach. The amendment takes effect on September 1, 2019.

[1] A copy of the amendment may be found here.

Key Takeaways

Companies that conduct business in New Jersey and collect user names and related passwords — or security questions — from state residents should update their security incident response plans to ensure appropriate notification of residents in the event that the company experiences a data breach involving such information.

Return to Table of Contents

Washington State Amends Data Breach Notification Law

Washington state has amended its data breach notification law, expanding the list of categories of data to which the notification requirements apply, and revising the timeline in which notifications to individuals must be made.

Washington state Gov. Jay Inslee signed HB 1071 into law on May 7, 2019,[2] amending the state's data breach notification law. The revisions add more categories of personal information to the statute's notification requirements and shorten the timeline to notify affected individuals to 30 days.

Previously, an entity conducting business in Washington only was required to notify a state resident of a breach if the individual's name was accessed in combination with the individual's Social Security number, state identification card number or financial account information. Under the new law, the definition of "personal information" is expanded to require notification to individuals involved in breaches in which the individual's name is accessed in combination with any of the following data elements:

- full date of birth;
- a private key that is unique to an individual and used to authenticate or sign an electronic record;
- a student, military or passport identification number;
- a health insurance policy number or health insurance identification number;
- any information about the individual's medical history, mental or physical condition, medical diagnosis by a health care professional or treatment of the individual; or
- biometric data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual.

In addition, the amendment requires Washington residents to be notified if any of the above-listed data elements are accessed without the individual's name if the accessed data is (1) not encrypted or redacted and (2) would enable a person to commit identity theft.

Like the New Jersey amendment summarized above, the amendment also requires entities that experience a data breach to notify individuals of a breach if their username or email address is obtained in combination with a password or security questions (and answers) that would permit access to an online account. If the breach involves a username or password, an entity may provide the required notice to the affected individuals by email. The email must advise the individuals to change their passwords and security questions and answers promptly, or take other steps to protect their online account and any other accounts using the same login information. However, if the breach involves credentials of an email account furnished by the entity, the entity may not provide notification to that email address.

Notably, the amendment decreases the amount of time an entity has to notify individuals affected by a breach to 30 days (from the previous 45 days). Notice to affected individuals must include a time frame of exposure of the relevant personal information (if known), including the date the breach occurred and the date it was discovered. As under the prior law, breaches affecting more than 500 Washington residents require notice to the attorney general. The amendment requires additional information to be included in such notice, namely, a list of the types of information affected by the breach, the time frame of exposure, a summary of steps taken to contain the breach and a sample copy of the notice to affected individuals. An updated notice to the attorney general is required if information required to be disclosed pursuant to the law is unknown at the time the notice is due.

The amendments will take effect on March 1, 2020.

Key Takeaways

Companies doing business in Washington should update their security incident response plans to ensure that their data breach notification procedures comply with the amended requirements.

Return to Table of Contents

[2] A copy of the amendment may be found here.

Danish and UK Data Protection Authorities Provide Guidance on Customer Call Recording Under the GDPR

Recent enforcement actions by Denmark's Data Protection Authority (DPA) and the United Kingdom's Information Commissioner's Office (ICO) provide new interpretative guidance on how the General Data Protection Regulation (GDPR) extends to customer service call recording and monitoring.

Background

Customers phoning into call centers with questions, complaints, reservations or other purposes, often hear a similar message that states the call "may be recorded for quality assurance and training purposes." The GDPR introduced a new layer of requirements for both European Economic Area (EEA) and non-EEA companies that process data of individuals in the EEA by recording customer calls. Although the extent of the GDPR's applicability to these activities is still developing, recent enforcement actions from national supervisory authorities provide some guidance in understanding how the GDPR governs these recordings.

Recording Customer Service Calls Under the GDPR

Broadly speaking, recording a phone conversation is considered a means of processing personal data, bringing that action within the GDPR's scope. Specifically, companies subject to the GDPR that maintain call center operations and record calls must comply with the legal obligations of data controllers since they determine the purpose and means of personal data processing. In many ways, the GDPR requirements for processing data by recording phone conversations runs parallel to requirements for processing data through other means, albeit with certain nuances and differences.

Standards for Transparency

Under GDPR Article 5, data must be processed lawfully, fairly and transparently. As a result of this transparency requirement, the controller must inform the caller of certain details (*i.e.* prior information requirements) at the point that data is collected (prior to or at the very start of the call). The prior information requirements set forth in GDPR articles 13-14 are quite lengthy. As such, the large volume of information that must be provided might not be practical in a telephone call. However, the Article 29 Working Party guidelines, published by the European Commission, provide some guidance in relation to the GDPR's standards for transparency that involve a layered approach. When the controller first engages the data subject (*i.e.* prior to recording the phone conversation), it should provide the most important information in the form of a first layer notice, including (1) the details of the purposes of processing, (2) the identity of the controller and (3) descriptions of data subjects' rights. Any additional information required under GDPR articles 13-22 can be provided through other means (*e.g.* the controller's external privacy notice), which the controller may refer to at the end of its first layer notice (*e.g.* by indicating that the full-form privacy notice may be found on the website).

Lawful Means of Processing Data

Under GDPR Article 6, the controller must have legal grounds for collecting and processing data, including the data subject's consent, which must be freely given, specific, not bundled, informed and unambiguous (often through a clear affirmative action) under the GDPR. The customer also must be able to withdraw consent at any time free of charge. It is important to note that a prerecorded message without any other action (*e.g.* asking customers to press their keypads to indicate consent to being recorded) may not, strictly speaking, comply with the GDPR's enhanced definition of "consent."

To bypass the issue of consent, a company alternatively can process data based on its legitimate interests. Although what constitutes a "legitimate interest" is a fact-intensive inquiry that will vary on a case-by-case basis, the GDPR specifically notes that the use of client data is a potential legitimate interest, but that this legitimate interest also must be balanced against the individual's interests, rights and freedoms. If the individual's interests override the legitimate interest, then the controller cannot rely on this legal ground for processing data. As such, most companies without a mechanism for allowing customers to "opt out" of recordings currently take the position that quality assurance and training purposes are legitimate interests in order to lawfully record calls from customers.

Recent Cases

On April 11, 2019, the DPA ruled that Denmark's largest telecommunications company, TDC A/S (TDC), violated the GDPR by recording customer calls for training purposes without obtaining explicit consent. The issue first came to the DPA's attention after a TDC agent informed a customer that it was "not possible" to turn off the recording mechanism when the customer asked that the call not be recorded. Although its reasoning was not entirely clear, the DPA rejected TDC's claim that the improvement of customer service qualified as a legitimate interest to bypass the explicit consent requirement, potentially signalling that companies must take additional steps in the future to comply with the GDPR's notion of "consent" (*e.g.*, allowing customers to indicate their consent through a keypad) prior to recording calls.

The DPA declined to levy the GDPR's enhanced administrative fines against TDC, but the agency did ban the company from recording customer calls until such steps were implemented.

In a slightly more nuanced case than Denmark's TDC case, in the week of May 10, 2019, the ICO issued an enforcement action related to biometric data against Her Majesty's Revenue and Customs (HMRC), the U.K. tax authority. In January 2017, HMRC implemented a voice authentication service that required callers, in some instances, to record their voices as their password for login. Per the GDPR, biometric data collected for the purposes of uniquely identifying an individual is considered a "special category of personal data," the processing of which is prohibited unless certain conditions under GDPR Article 9 are met (most notably, the data subject's explicit consent). The ICO found that because callers were not provided an option to decline the voice authentication service, HMRC did not adequately inform customers of the purpose of processing their data (in light of the transparency principle) and failed to obtain adequate explicit consent from its customers prior to collecting their biometric data. The ICO gave HMRC 28 days to delete relevant records.

Key Takeaways

Companies that are subject to the GDPR and record customer calls should review their practices in light of these recent decisions to ensure compliance. Both agencies' enforcement actions signal that companies should consider implementing mechanisms to obtain explicit consent from their customers rather than relying purely on legitimate interests as a legal ground for processing data.

Return to Table of Contents

SEC Issues Risk Alert Regarding Cloud-Based Storage

The U.S. Securities and Exchange Commission (SEC) has issued a risk alert advising that use of cloud-based storage solutions by investment advisers and broker-dealers may jeopardize the security of electronic customer information.

On May 23, 2019, the Office of Compliance Inspections and Examinations (OCIE) of the SEC released a risk alert highlighting cybersecurity issues associated with broker-dealers' and investment advisers' use of cloud-based storage and other network storage solutions.[3] Recent OCIE examinations found that firms were underutilizing third-party storage providers' security features, such as encryption and password protection, that are designed to prevent unauthorized access to customer records. Finding a number of cybersecurity lapses, the OCIE cautioned that use of network storage solutions without proper oversight may constitute a failure to comply with Regulations S-P and S-ID concerning security safeguards and identity theft rules, respectively.[4] The risk alert also included guidance regarding common deficiencies and best practices for firms using cloud-based or network storage solutions.

Cybersecurity Concerns

In the risk alert, the OCIE listed a number of security failings stemming from the failure to apply firms' internal cybersecurity policies and procedures to third-party storage providers. While the majority of the observed network storage solutions offer sufficient security measures, the agency found that firms are not fully using these third-party security features. The OCIE observed three primary cybersecurity concerns:

- third-party security settings were not properly configured by firm users at the outset, resulting in issues such as insufficient encryption and inadequate password protection;
- electronic data was not appropriately classified, and thus, appropriate controls were not applied to sensitive data; and
- firms failed to institute comprehensive security agreements with vendor-providers prior to installation of network storage solutions.

OCIE Recommendations

The OCIE recommended increased oversight by firms utilizing network storage solutions to mitigate the risk of non-compliance with S-P and S-ID. Firms are encouraged to:

- develop guidelines ensuring that third-party providers are configuring security settings in accordance with firm standards;
- implement additional policies and procedures addressing secure installation, maintenance and recurring review of the integrated security measures; and
- update software and hardware regularly, while also evaluating any changes to the security configuration resulting from those updates.

[3] The full text of the Risk Alert is available here.

[4] Regulation S-P's Safeguard Rule requires firms to adopt written policies and procedures that address the administrative, technical and physical safeguards used to protect customer records and information. 17 C.F.R. 248.30(a)

Key Takeaways

To ensure compliance with SEC rules and regulations, investment adviser and broker-dealer firms should ensure that use of third-party, cloud-based and other network storage solutions comport with firms' internal cybersecurity policies and procedures. Firms should update their policies and procedures as necessary to require the configuration of storage providers' security settings, secure installation of network storage solutions, and adequate classification of information, including sensitive customer records, stored on such systems.

Return to Table of Contents

Verizon Releases Annual Data Breach Investigations Report

Verizon released its annual Data Breach Investigations Report (DBIR), which provides a detailed summary and analysis of security incidents and data breaches that have been reported by public and private entities worldwide.[5] This year's DBIR analyzed 41,686 security incidents, of which 2,013 resulted in the confirmed disclosure or exposure of data. The report identifies general trends with respect to data breaches and security incidents, as well as several industry-specific insights.

General Trends From the DBIR

This year's DBIR noted the following general trends:

- **Focus on C-Suite Executives:** Senior officers and executives were found to be 12 times more likely to be the target of social engineering campaigns, such as targeted phishing emails, as compared to other employees. Senior-level employees are likely to have broad access to company systems and data, which makes them valuable targets for attackers. The DBIR noted that senior-level employees are also "time-starved and under pressure to deliver," which can sometimes result in the failure to review emails carefully before clicking the hyperlinks or downloading the attachments in emails.
- **Nation-State Attacks:** The report showed that 23 percent of data breaches involved attackers that were affiliated with or identified as nation-states, up from 17 percent the previous year.
- **Insider Attacks:** Companies often allocate significant resources to protect their systems and data from external threats. However, the DBIR found that 34 percent of security incidents that resulted in the confirmed disclosure or exposure of data involved insiders.
- **Ransomware Attacks:** Ransomware attacks involve malware that prevents users from accessing systems or files until the users pay the attackers a certain amount (*i.e.*, a ransom). These attacks are on the rise and now account for nearly 24 percent of security incidents involving malware.
- **Time to Discover a Breach:** The DBIR noted that 56 percent of breaches take a month or longer to be discovered.

Industry-Specific Trends

The DBIR also includes detailed summaries of certain industry-specific trends, including the following:

- **Financial Industry:** The introduction of "chip-and-pin" systems has made it more difficult for attackers to commit fraud with physical credit cards. As a result, since 2015, breaches occurring at point-of-sale have decreased by a factor of 10. However, the DBIR notes that this trend may correspond with an increase in attempts to gain unauthorized access to credit card information via web and mobile applications.
- **Health care Industry:** Out of all of the industries analyzed, health care was the only industry where security incidents were more likely to be caused by insiders than external threats. However, this conclusion should be considered in light of the extensive breach reporting requirements under HIPAA, which includes recordkeeping obligations that may result in documentation of incidents that are otherwise undocumented by companies that are not subject to sector-specific laws requiring such detailed recordkeeping. Therefore, it is difficult to determine whether the risks posed by health care insiders are unique to that industry.

Key Takeaways

Although analyses of security incidents and data breaches generally rely on self-reported data and do not identify the full scope of security threats — incidents and data breaches that companies experience — companies can consider the DBIR's findings in allocating cybersecurity resources to address known threats, such as the risk of data breaches caused by company insiders.

Return to Table of Contents

[5] This year's complete DBIR and an executive summary are available here.

FTC Requests Federal Privacy and Data Security Legislation

The Federal Trade Commission (FTC) added its voice to those calling on Congress to pass federal privacy and data security legislation, and requested the ability to impose civil penalties and additional targeted rulemaking authority.

During a hearing before the House Energy and Commerce Committee's Consumer Protection and Commerce Subcommittee on May 8, 2019, the FTC pressed Congress to pass privacy legislation that would both enable the agency to protect American consumers' data more effectively and ease the compliance burden arising from the patchwork of state privacy legislation.

The hearing followed recent criticism of the FTC's enforcement efforts, in which some complained that the penalties imposed by the FTC for certain privacy violations were not sufficient in light of the harm to consumers that resulted from such violations. As part of its testimony, the FTC requested better enforcement tools to protect data security and privacy in the United States through civil penalties, limited rulemaking authority under the Administrative Procedure Act and authority over common carriers and nonprofit organizations.[6]

The FTC commissioners explained that the agency's ability to punish companies for privacy violations is limited because it cannot directly fine companies, as is often done by its European counterparts, who have the power to impose potentially heavy statutory fines under the GDPR. Currently, rather than fining companies directly, the FTC must bring an action in court seeking an injunction, or negotiate a settlement with violators.

The FTC also called on Congress to increase the agency's budget for tackling privacy violations, explaining that it only has 40 employees dedicated to privacy and data security as compared to the U.K.'s Informational Commissioner's Office, which has roughly 500 employees.

FTC Chairman Joe Simons asked Congress to give his agency targeted, rather than broad, rulemaking authority to write privacy and data security regulations. Limited rulemaking authority, Simons explained, would ensure that Congress, rather than the five FTC commissioners, would be responsible for defining federal privacy priorities.

Key Takeaways

The FTC has joined the growing chorus calling for federal privacy legislation. While it remains to be seen whether and to what extent Congress will pass such legislation, given the FTC's prominent role in protecting U.S. consumers' data privacy, Congress may be influenced by the FTC's testimony.

Return to Table of Contents

[6] Press Release, FTC, "FTC Testifies Before the House Energy and Commerce Subcommittee on its Work to Protect Consumers and Promote Competition," (May 8, 2019) available here.

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

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