Skadden

Privacy & Cybersecurity Update

New York Department of Financial Services Issues Ransomware Guidance

The New York Department of Financial Services (NYDFS) has released guidance intended to help companies avoid becoming victims of ransomware attacks, as well as strategies for recovering from attacks that do occur.

On June 30, 2021, the NYDFS issued new ransomware guidance, including a set of recommended measures to help organizations prevent and prepare for ransomware attacks.[1] In the guidance, the agency notably recommends against paying ransoms, an approach that is aligned with the FBI's official policy.[2] Citing a 300% increase in ransomware attacks in 2020, the NYDFS also encourages all entities under its authority to implement the updated measures to the extent that entities are able to do so.

Background

As noted by the NYDFS, ransomware attacks pose a continued threat to the stability of the financial services industry. Individual attacks, as well as coordinated attacks that simultaneously target several financial services companies, could contribute to a loss of confidence in the financial system and even precipitate a financial crisis.

From January 2020 to May 2021, NYDFS-regulated entities reported 74 ransomware attacks, with 17 of the affected organizations choosing to pay the ransom to end the attack. In its guidance, the NYDFS also noted an increase in attacks against third-party entities related to the financial services sector, as well as spillover effects in the cyber-insurance industry, which experienced increased loss ratios in 2020.

According to the NYDFS, ransom payments are a key contributor to the increase in the amount of ransomware attacks. As cybercriminals demand larger amounts of money (demand amounts increased 171% from 2019 to 2020, according to the NYDFS), the payments help fund continued cybercriminal activity. With increased funds available, cybercriminals are able to launch more frequent and more sophisticated attacks, and also can recruit more hackers to work within ransomware schemes.

The NYDFS conducted a review of the 74 reported ransomware attacks from January 2020 through May 2021 and found a similar pattern of techniques that hackers used in

[1] The NYDFS's guidance is available here.

[2] The FBI's policy is available here.

© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

the attacks. Typical methods included phishing, the exploitation of unpatched vulnerabilities and infiltrating poorly secured remote desktop protocols. These findings informed the NYDFS's newly published ransomware guidance.

The Guidance

Below is an overview of the NYDFS's guidance.

- **Email Filtering and Anti-Phishing Training** – Required cybersecurity trainings for employees should include phishing training with tips on how to identify and report phishing attempts within the organization.
- **Vulnerability/Patch Management** – Organizations should have a program to identify, assess, track and correct any vulnerabilities on all cyber-related infrastructure, along with periodic penetration testing.
- **Multi-Factor Authentication (MFA)** – MFA should be used for remote access to an organization's network and any externally exposed applications, as well as for access to any privileged accounts.
- **Disable Remote Desktop Protocol Access** – If deemed necessary, remote access should be limited to preapproved originating sources and should always require MFA.
- **Password Management** – Strong, unique passwords should be used for all organizations, and large organizations should use a password-vaulting privileged-access management solution with the ability for employees to request and check out passwords.
- **Privileged Access Management** – Users and service accounts should only be granted the minimum level of access required for job performance.
- **Monitoring and Response** – Organizations should have an endpoint detection and response solution to monitor and identify anomalous or suspicious activity.
- **Tested and Segregated Backups** – Segregated backups should be accessible offline to allow for recovery of data during a ransomware attack.
- **Incident Response Plan** – Organizations should have an incident response plan with details on how to respond to a ransomware attack.

In the event of a ransomware attack, the NYDFS strongly discourages payment of the ransom, stating that payment may even violate Office of Foreign Assets Control sanctions. The NYDFS notes that in cases where victims pay the ransom, restored access to stolen data is not guaranteed, with 80% of victims who pay a ransom later experiencing subsequent attacks. Beyond this general admonishment against paying ransoms, however, the NYDFS does not provide guidance on how to respond to a ransomware attack.

Lastly, all ransomware attacks must be reported to the NYDFS "as promptly as possible and within 72 hours at the latest."

Key Takeaways

- The recommended measures, while perhaps challenging to implement for smaller organizations, are encouraged for all NYDFS-regulated entities. The NYDFS warns that failing to implement the measures "may ultimately result in greater losses as small businesses are frequently targets for ransomware and other cybercrimes precisely because they are often more vulnerable."
- Despite the recommendation not to pay ransoms, affected organizations will likely face difficult decisions regarding whether or not to make a payment when faced with an attack. Some of the NYDFS guidance, such as maintaining offline, segregated backups of their systems and/or data, is designed to help companies recover if they either refuse to pay the ransomware or the attackers fail to restore access to their systems or data. These measures should make it easier for companies to resist rewarding attackers by paying ransoms.

Return to Table of Contents

Coloring Book App Companies Settle FTC COPPA Claims

The operators of a coloring book app have settled Federal Trade Commission (FTC) allegations that they violated the Children's Online Privacy Protection Act (COPPA).

On July 1, 2021, the FTC announced that it had entered into a settlement agreement with Kuuhuub Inc., Kuu Hubb Oy and Recolor Oy, the operators of Recolor, a coloring book app. The FTC had alleged that the app collected the personal information of children and allowed third-party advertisers to misuse children's personal information for behavioral advertising, all in violation of COPPA.

The Recolor app allows users to digitally color different images on their mobile devices and generates revenue from paid subscriptions and advertisements. While Recolor is marketed as an app for adults, the FTC argued that a portion of the app's coloring categories are directed toward children.

In addition to the coloring book, Recolor also contains social media features that allow users to upload, comment on and "like" images, as well as follow other users' accounts. In order to access the social media features, users are required to create an account using their email address and a screen name, along

with an optional user description and profile picture. According to several parents who complained, children were utilizing the social media features and engaging with adults on the app.

FTC Allegations

COPPA and its enabling regulations forbid the collection, use or disclosure of personal information from visitors who identify themselves as under age 13 without providing notice to parents and obtaining parental consent.[3] The FTC alleged that children under the age of 13 had created Recolor accounts and were utilizing the app's social media features. According to the FTC, not only had Recolor allegedly collected personal information from children under the age of 13 without parental notice and consent, but it also allowed third-party advertising networks to collect children's personal information, in the form of persistent identifiers, without instructing the advertising networks not to use these persistent identifiers for targeted ads.

Settlement Terms

Under the settlement agreement, the operators of Recolor must delete all information obtained without parental consent from children under the age of 13. Additionally, the companies must offer Recolor's current paid subscribers a refund if they were under the age of 18 when they signed up. Further, the app's parent companies were assessed a $3 million penalty, though as they are unable to pay the full amount, the penalty will be suspended upon a $100,000 payment. Finally, the companies are required to inform their users of the allegations and actions users can take in response to the settlement.

The Recolor settlement is noteworthy for a number of reasons. Firstly, this is the first time a COPPA settlement requires refunds to be issued to paid subscribers who created accounts while under the age of 18, which may reflect the unique facts of the case. Secondly, this is the first time a COPPA settlement requires defendants to notify users of the allegations, which reflect a renewed desire by the FTC to alert consumers of alleged misuse of their information. Finally, while the agency's usual practice in these types of situations has been to assume all information collected by a service (or a portion of the service) originated from a child, in this case the FTC required the operators to try to parse out the children's data from other data collected by the service. This requirement likely reflects the nature of the service itself, rather than a change in the FTC's approach overall.

Key Takeaways

The Recolor settlement is a reminder that, for websites or apps that primarily target adults, operators must also be aware of COPPA obligations if portions of the website or app are directed at children under the age of 13.

Return to Table of Contents

CISA Unveils Website Listing 'Bad Practices' for Cybersecurity

The Cybersecurity and Infrastructure Security Agency (CISA) has unveiled a website listing cybersecurity "bad practices" for companies and individuals.

The latest ransomware attack on oil pipeline company Colonial Pipeline demonstrates how cyber threats can affect U.S. government functions and the private sector. On June 24, 2021, CISA released a website[4] that identifies "Bad Practices" that outlines "exceptionally risky" cybersecurity practices.

Background

CISA is a government agency tasked with managing risks to America's critical infrastructure, including cybersecurity risks. The agency releases periodic guidelines and insights to update the critical infrastructure community on evolving cyber threats and shifting cybersecurity standards. Although the target audience for these guidelines and insights is key stakeholders in the critical infrastructure community, the agency's guidance often applies to the broader community as well. Moreover, CISA encourages all organizations to follow its guidelines, including by avoiding practices that the agency deems to be "bad practices."

CISA's List of Bad Practices

In CISA's view, the presence of these bad practices in organizations that support critical infrastructure is "exceptionally dangerous." Currently, there are only two practices highlighted as bad practices on the CISA site, but the agency intends to update and expand the list over time. The two bad practices currently listed will be familiar to cybersecurity professionals:

- use of unsupported (or end-of-life) software; and
- use of known/fixed/default passwords and credentials.

[3] 16 C.F.R. § 312.2 (2021)

[4] Available here.

In CISA's view, each of these practices, when used in service of critical infrastructure, are dangerous and significantly elevate risk to national security, national economic security, and national public health and safety. CISA describes the dangers as "especially egregious" in internet-accessible technologies.

Potential Impact

CISA's identification of these practices as "bad practices" and its description of them as "exceptionally risky" and "exceptionally dangerous" puts the cybersecurity community on notice that organizations need to avoid these activities. If an organization engages in these practices and experiences a cybersecurity incident, it may be difficult — though not impossible — for the organization to defend itself against claims that it took appropriate steps to protect its systems.

Key Takeaways

The CISA Bad Practices website identifies what the agency believes are particularly egregious examples of bad cybersecurity practices. Companies should periodically review CISA's list and verify whether their own organizations engage in the identified practices. Continuing to engage in a particular practice after CISA has warned of its risks could put organizations in danger of being unable to defend against potential enforcement or litigation.

Return to Table of Contents

California Attorney General Seeks to Automate CCPA Compliance and Reporting

California Attorney General Rob Bonta has taken measures to facilitate automating certain compliance and reporting aspects of the California Consumer Privacy Act (CCPA).

Among the measures taken by the attorney general, the state has updated its CCPA FAQ[5] to confirm that companies subject to the CCPA must honor consumer requests not to sell their information that are automatically generated by the Global Privacy Control (GPC) browser protocol. Secondly, the attorney general's office released an online tool for consumers to report violations of their CCPA rights to companies.

Automated Do-Not-Sell Requests Through Global Privacy Control

GPC is a technology initiative that enables users to automatically opt out of sales of their information. The technology is being developed by an informal consortium of organizations, including the National Science Foundation, *The New York Times*, Mozilla and the Electronic Frontier Foundation. In some internet browsers, users can configure their browser settings to turn on GPC, while other browsers require users to install a browser extension to do so.

GPC has not been made available in all browsers, and has yet to be recognized by all organizations collecting information online.

Recognition Under CCPA

The CCPA requires companies subject to the its regulations to provide consumers with at least two methods to opt out of having personal information sold to third parties. The CCPA's implementing regulations elaborate on that requirement, stating that "if a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer." In effect, though some commentators have argued that the FAQ overstates companies' obligation to comply with GPC, many have understood the FAQ update as a clearer confirmation of what the regulations already require.[6]

Automated Noncompliance Reporting Tool

Separately, on July 17, 2021, the attorney general's office also released an online tool for reporting CCPA noncompliance to companies.[7] Currently, the tool only allows for the reporting of a failure to provide the CCPA-required "Do Not Sell My Personal Information" link on a company's website, which provide consumers with a way to request to opt out of the sale of their personal information. The attorney general's office has indicated, however, that it intends to update the tool over time to include other potential CCPA violations.

The tool guides users through a series of questions and, based on the answers provided, offers information about the CCPA and a draft notice to the business that the consumer can copy into an email asserting that the consumer believes the company has violated the CCPA.

[5] The attorney general's updated CCPA FAQ is available here.

[6] See, for example, International Association of Privacy Professionals' July 15, 2021, article "Update by the California Attorney General Could Be a Game-Changer. "

[7] The new tool is available here.

CCPA enforcement is generally left to the attorney general's office, and the law allows the attorney general to sue businesses that violate the regulations if they do not cure any violation(s) within 30 days of being notified of noncompliance. The attorney general's office has stated that it will use information gathered through the online tool, which will include data about the business and the consumer involved, to aid in its enforcement of the CCPA. According to the Mr. Bonta's office, the notice generated by the tool and sent to the business may satisfy the CCPA's 30-day notice prerequisite.

Effect of Automation

The attorney general's decisions to require companies to comply with GPC requests not to sell consumer information and to provide automated tools for generating notices of noncompliance are intended to simplify the process for consumers to exercise their rights under the CCPA. These decisions may encourage other jurisdictions to follow suit. California has long been viewed as a leader in state-level legislation related to the protection of personal information, and other states with laws modeled in part on the CCPA (including Colorado) may decide to follow California's lead in this area as well.

Key Takeaways

- Companies that are subject to CCPA should determine whether they accept and honor GPC requests, as it seems likely that the use of this technology — or similar technologies that have the same effects — will grow as consumers become aware of its availability.
- Companies should, as a standard practice, be sure to review CCPA noncompliance notices received from consumers. In particular, however, companies should be aware that information on noncompliance that is processed through the attorney general's noncompliance reporting tool also is being provided to the attorney general's office, which may give rise to a greater threat of an enforcement action.

Return to Table of Contents

EDPB Publishes Draft Guidelines on Codes of Conduct as a Tool for Data Transfers

The European Data Protection Board (EDPB) published draft guidelines relating to the use of codes of conduct as appropriate safeguards for the transfer of Europeans' personal data to third countries.

On July 7, 2021, the EDPB released draft guidelines on the use of codes of conduct to permit transfers of personal data outside of the EU under the General Data Protection Regulation 2016/679 (GDPR). The guidelines aim to provide organizations with practical guidance regarding the content of such codes of conduct, the process for adopting such codes and the relevant actors involved in the process. The guidelines also aim to act as a reference point for European supervisory authorities to ensure that codes of conduct are evaluated in a consistent manner and in accordance with a streamlined assessment process.

Background

The topic of international data transfers from the European Economic Area (EEA) has been in a state of flux for the past several years. Under the GDPR, the default position under Article 44 is that organizations cannot transfer personal data to third countries that lack adequate data protection laws unless appropriate safeguards have been implemented or a specific derogation applies. Specific derogations apply only where the data transfer is not repetitive (*i.e.*, such data transfers are "one-offs"). For data transfers that are repetitive, organizations must implement appropriate safeguards. Following the Court of Justice of the European Union's (CJEU) July 2020 decision in *Schrems II* to invalidate the EU-U.S. Privacy Shield as an appropriate safeguard,[8] most organizations have chosen to rely on the European Commission's standard contractual clauses (SCCs) to legitimize their data transfers to the U.S. However, the CJEU's ruling in *Schrems II* and subsequent recommendations from the EDPB have imposed an "enhanced due diligence" standard regarding the use of SCCs.

The use of codes of conduct as appropriate safeguards for international data transfers, as permitted by Article 46(2)(e) of the GDPR, has, until now, seldom been explored. This is consistent with the low uptake of the use of codes of conduct under the GDPR more generally, beyond the transfer context. However, given the uncertainty surrounding data transfers from the EEA to third countries (particularly to the U.S.), there has been increased interest in the use of codes of conduct as an appropriate safeguard.

The guidelines are open for comments until October 1, 2021.

Guideline Details

- **What are codes of conduct as a tool for data transfers?** Per Article 40 of the GDPR, codes of conduct are intended to "contribute to the proper application" of the GDPR and must contain mechanisms that enable accredited bodies to monitor compliance with such codes. In relation to data transfers, a code of conduct requires controllers and processors in third countries to make binding and enforceable commitments

[8] See Skadden's July 17, 2020, client alert "*Schrems II*: EU-US Privacy Shield Struck Down, but European Commission Standard Contractual Clauses Survive."

to apply the appropriate safeguards provided by the code. According to the EDPB, the benefit of codes of conduct in this context is that they can be more specific to particular sectors or processing activities. For a code of conduct to be determined as an appropriate safeguard, it first needs to be approved by a competent supervisory authority in the EEA and then officially implemented by the European Commission. Previous guidelines published by the EDPB provide that code owners can choose the competent EEA supervisory authority, taking into account factors such as the location of the processing activity or sector, the location of the code owner's headquarters and the location of the proposed monitoring body's headquarters.

- **Who puts together the codes of conduct?** Codes of conduct are generally drafted by associations or other bodies representing categories of controllers or processors within a given sector or industry, such as trade and representative associations, sectoral organizations, academic organizations and interest groups.
- **What should a code of conduct for data transfers contain?** The guidelines set out a checklist of 16 elements that should be reflected in any code of conduct, including, among others:
  - a description of the in-scope transfers (*e.g.*, nature of data transferred, categories of data subjects, countries involved);
  - a list of accountability measures to be undertaken in relation to any transfer;
  - the monitoring of the transfers through appropriate governance that is independent from the oversight to be performed by the third-party monitoring body (*e.g.*, internal data protection officers or other privacy-related staff in charge of ensuring compliance with the relevant data protection obligations);
  - the criteria for selecting the third-party monitoring body for the code (to demonstrate that the monitoring body has the requisite level of expertise to carry out its role);
  - the conduct of a data protection audit carried out either internally or externally to verify compliance with the code; and
  - a warranty that the third country controller/processor has no reason to believe that the laws in the third country prevent it from fulfilling its obligations under the code.
- **Who are the main actors involved?** The guidelines distinguish between the "code owner" and the "monitoring body." The code owner is the organization that prepares the code and submits it to the relevant supervisory authority for approval. The monitoring body must be independent from the code owner and must be approved by the relevant supervisory authority that approves the code. Monitoring bodies must also be free to act from external influence to ensure that no conflict of interest arises and have the required knowledge and expertise.

We will be watching this space to see whether the guidelines prompt the creation of new monitoring bodies and code owners in the context of international data transfers.

Key Takeaways

- Data transfer options are limited for organizations transferring personal data from the EEA to third countries that lack adequate data protection laws. Codes of conduct offer an alternative to the much-discussed SCCs and the accompanying enhanced due diligence, and could be particularly useful for data transfers at a sectoral level as the code and its accountability mechanisms can be made bespoke to the nature of the data.
- A less tangible, but equally important, potential benefit of codes of conduct is the message that they send and the impact they may have within a given sector or industry. For example, adherence to a particularly stringent code of conduct for data transfers may be perceived favorably by the market, enhance customers' trust in organizations abiding by the code, and contribute to the further development of that sector or industry.

Return to Table of Contents

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

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

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

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

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

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

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

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

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