Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Navigating New Federal, State Data Privacy Compliance Duties

By **Mark Krotoski and Jill Harris**
March 10, 2020, 4:30 PM EDT

Mark Krotoski

Jill Harris

Federal and state regulators continue to bring enforcement actions against companies and individuals following investigations of data breaches, cybersecurity incidents or consumer privacy violations. While many of these enforcement actions have common elements including significant fines, recent cases have highlighted new notification and reporting requirements, governance issues and compliance obligations.

This article reviews some of the common features in these enforcement actions and notes steps to prepare for, mitigate and respond to regulatory enforcement actions.

Multiple Federal and State Regulators and Overlapping Regulations

When a cybersecurity or data privacy incident occurs, a company typically launches its incident response plan, conducts an internal cybersecurity investigation (preferably under attorney-client privilege), restores security and safeguards information, resumes business operations and notifies consumers or others about the incident if necessary, among several other steps depending on the circumstances. Regulatory investigations may present another area of focus, including inquiries from multiple regulators at the federal and state levels.

Several federal agencies have brought recent cybersecurity enforcement actions, including the U.S. Securities and Exchange Commission; Federal Trade Commission; U.S. Department of Health and Human Services Office for Civil Rights; U.S. Commodity Futures Trading Commission; Consumer Financial Protection Bureau; and Federal Communications Commission.

The role of enforcement actions and orders was highlighted in early January when the FTC Bureau of Consumer Protection announced that it has focused on three primary changes to data security orders during the past year.

First, the “orders are more specific,” which “make the FTC’s expectations clearer to companies, but also improve order enforceability.”[1]

Second, the “orders increase third-party assessor accountability” in the review and report of the company’s data security program. The FTC expects documentation and support for the third-party conclusions and the opportunity to “access working papers and other materials.”

Third, the “orders elevate data security considerations to the C-Suite and Board level.” An annual certification of compliance under oath is increasingly required by senior company officers.

At the state level, 54 jurisdictions (all 50 states and the District of Columbia, Guam, Puerto Rico and the Virgin Islands) have enacted data breach notification statutes involving the access or acquisition of personal information.

New statutory privacy rights provide unique enforcement areas for some states. The landmark California Consumer Privacy Act, which took effect on Jan. 1, establishes new statutory privacy rights, including the rights to know what personal information is being collected, to opt out of the sale of personal information to third parties, to equal service and price and to request that a business delete personal information that has been collected.[2]

Other states, including Washington, Nevada and New York, are also considering comprehensive privacy statutes that allow consumers to request their personal information, opt out of having their personal information sold and exercise new privacy rights.[3]

The patchwork of federal and state statutes adopting different and conflicting standards creates an unnecessarily complex, cumbersome and costly system. The time has come for a uniform federal standard to promote effective cybersecurity, simplify the process and ensure consistent standards.[4] Until then, companies will continue to confront disparate enforcement standards from multiple enforcers.

Increasingly Broad Enforcement Terms

Most enforcement actions result in a consent or stipulated settlement or judgment. In assisting companies and individuals and in tracking federal and state enforcement actions, we have observed that many of the cybersecurity and privacy settlement actions, while still fact-specific, typically include some of the following elements:

- Fines and monetary judgments;
- Injunctions prohibiting certain conduct;

- New notification requirements to the agency based on new incidents;
- Governance and structural reforms;
- Comprehensive written information security program with specific safeguards;
- Monitoring requirements or third-party information security assessors;
- Third-party assessment, review and reporting on information security programs;
- Reporting to an enforcement agency on status and progress;
- Certification of compliance by executives with new settlement conditions;
- New record-keeping requirements;
- Whether the conduct is admitted or denied; and
- Term of jurisdiction with the agency (usually a few years, but up to 20 years).

The enforcement terms and conditions continue to be reviewed and scrutinized as they impact case resolutions. The FTC recently announced that it had modified its approach based on the U.S. Court of Appeals for the Eleventh Circuit's 2018 LabMD Inc. v. FTC decision, which struck down an FTC data security order as unenforceably vague.[5] In particular, the FTC noted that the orders should be more specific, increase third-party assessor accountability and elevate data security considerations to the C-Suite and board level.

Fines and Monetary Judgments

Many recent fines or monetary judgments have exceeded $1 million. For example, Facebook Inc. recently agreed to pay a $5 billion civil penalty along with other settlement terms to the FTC.[6] Also, in July 2019 consumer-reporting giant Equifax Inc. agreed to pay at least $575 million (and perhaps up to $700 million) to settle multiple investigations by the FTC, CFPB and states to resolve the enforcement actions related to its 2017 data breach.[7]

Injunction Prohibiting Certain Conduct

The resolution terms may enjoin certain activity related to the security issues or the handling of consumer information. For example, in the July Equifax stipulated order, Equifax was "permanently restrained and enjoined from misrepresenting, expressly or by implication, the extent to which Defendant maintains and protects the privacy, security, confidentiality, or integrity of any Personal Information."[8]

The injunction may also prohibit further violations of law. For example, the SEC administrative order in the Yahoo! Inc. data breach case ordered the company to "cease and desist from committing or causing any violations and any future violations of" the securities laws that were the subject of the enforcement action.[9]

Certification of Compliance with New Settlement Conditions

Increasingly, enforcement settlements include a requirement that the board of directors or a senior executive provide a certification of compliance with the cybersecurity settlement terms on an annual basis.[10]

In the Equifax case, the annual certification, which applies under the order for 20 years, requires the board of directors (or equivalent body) to certify that the company:

(1) has established, implemented, and maintained the requirements of this Order [for Permanent Injunction and Monetary Judgment]; (2) is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; (3) has cooperated with the [Third-Party Information Security] Assessor as required ... ; and (4) includes a brief description of any Covered Incident.[11]

Other recent orders have similar certification requirements.[12] As noted above, the FTC Bureau of Consumer Protection recently stated it is using company certifications by senior officials under oath to "force senior managers to gather detailed information about the company's information security program, so they can personally corroborate compliance with an order's key provisions each year."[13]

Governance and Structural Reforms

The settlement terms have increasingly addressed the company's governance over cybersecurity risks. In recent settlements, the board of directors (or a comparable governing body) is now required to receive the written information security programs and any material evaluations at least once every 12 months, as well as a report summarizing all covered incidents that occurred in that calendar quarter.[14] In addition, the FTC has imposed other remedies such as the creation of independent committees with removal authority over the designated expert privacy compliance officers.

Comprehensive Written Information Security Program

Many settlement terms include a requirement for a comprehensive written information security program with specific safeguards. In July 2019, Equifax was compelled to establish a comprehensive security program.[15]

The program must include documented risk assessments at least once every 12 months, documenting safeguards including policies and procedures concerning patch management, timely remediation, asset inventory, network intrusion protection, limiting unauthorized access, access controls, encryption, tokenization, security training programs and security vulnerability reports from third parties, among other security requirements.

The sufficiency of the safeguards must be assessed at least once every 12 months, including an evaluation of training and management, information systems and prevention, detection and response to security incidents. The effectiveness of the safeguards must be tested and monitored at least once every 12 months.

The written information security program usually contains specific safeguards based on the incident under investigation. The Equifax order addresses patch management issues that were a key vulnerability identified in the investigation.[16] Similarly, the Nationwide Mutual Insurance Co. settlement required the appointment of a “Patch Supervisor” to monitor and oversee security updates and security patch management.[17]

Third-Party Information Security Assessors

The settlement may impose a requirement for independent security assessments and reports. In the Equifax case, the company is required to obtain initial and biennial assessments from a third-party professional.[18] Some settlements have outlined specific assessor credentials. In the ClixSense.com matter, the defendant failed to utilize the latest security techniques to protect its users’ personal information, including encryption, firewalls, password management solutions and other cybersecurity detection tools.

To ensure compliance with its mandated information security program, the settlement requires the assessor to be a:

Certified Information System Security Professional (CISSP) or ... a Certified Information Systems Auditor (CISA); an individual holding Global Information Assurance Certification (GIAC) from the SANS Institute; or a qualified individual or entity approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.[19]

New Notification and Reporting Requirements

The settlement terms can include new reporting obligations to the enforcement agency or board for any new cybersecurity incidents. Companies have been required to submit a report to the FTC no later than 10 days after the date the defendant first notifies any U.S. federal, state or local government entity of the covered incident.[20] Additionally, a company must also provide the board of directors (or an equivalent body) with “a report summarizing all Covered incidents that occurred in that calendar quarter.”[21]

New Recordkeeping Requirements

The settlement terms may impose new recordkeeping obligations. As a result of the settlement, Equifax is required to create and retain certain records, including revenue, personnel, consumer complaints related to the subject matter of the order, security assessments and records demonstrating full compliance with each provision of the order.[22]

Whether the Conduct Is Admitted or Denied

Another consideration is whether the cybersecurity conduct under investigation is admitted by the company or remains as an allegation. For example, in the Yahoo! SEC resolution, “Yahoo neither admitted nor denied the findings in the SEC’s order.”[23] Some settlements do not require companies to admit or deny wrongdoing based on the collateral consequences from an admission, particularly if other enforcement actions or litigations are pending. Some settlements may solely admit limited facts to support an order and to establish jurisdiction.[24]

Term of Jurisdiction

Another key settlement element concerns the term of the agency jurisdiction under the conditions of the order. Many state or federal agencies generally use a term of three to five years. Traditionally, the FTC mandates a 20-year term.[25] The court may be asked to retain jurisdiction over the matter to address construction, modification and enforcement of the order.[26]

Recommendations: Steps Companies Can Take in Advance of a Regulatory Investigation

Regulators recognize that it is not possible to completely prevent a data breach or cybersecurity incident. While there is no way to mitigate all cyber risk or attacks, regulators expect companies to take reasonable steps to safeguard information and mitigate risks. Given the high-stakes consequences of enforcement actions and private litigation, there are a number of steps companies can take in advance of a regulatory investigation.

In its recent report, the SEC’s Office of Compliance Inspections and Examinations highlighted several best practices gleaned from its examination observations.[26] OCIE highlighted three elements of an effective cybersecurity program: (1) a risk assessment to identify, analyze and prioritize cybersecurity risks to the organization; (2) written cybersecurity policies and procedures to address those risks; and (3) the effective implementation and enforcement of those policies and procedures.[27]

Although each cybersecurity program is fact-specific, several steps are outlined below:

Tailored Written Cybersecurity Program

First, companies should be proactive in developing a strong, tailored written cybersecurity program based on risk assessments, designed to safeguard vital or sensitive information and address any unique circumstances. Mechanisms should be in place to prevent and detect incidents and respond and mitigate appropriately. Beyond simply establishing a comprehensive written policy, OCIE recently recognized the importance of testing, monitoring and continually evaluating an organization’s cybersecurity policy.[28]

Some information may require special protections such as trade secrets, which will require separate, tailored security protections, including trade secret protection plans.[29] As another category, credit card information is protected under the Payment Card Industry Data Security Standard.

The cybersecurity program should be based on established cybersecurity standards such as the National Institute of Standards and Technology Cybersecurity Framework; NIST special publications 800-171, 800-53 and 800-53A; the Center for Internet Security Critical Security Controls; or the International Organization for Standardization, among others.

Role of Attorney-Client Privilege and Work-Product Doctrine

Careful consideration should be given to the role of the attorney-client privilege and work-product doctrine at key stages in the cybersecurity process in which legal advice may be needed.[30] Legal guidance may be needed for the establishment of appropriate policies for incident response and anticipated litigation.

These legal protections will ensure that candid and frank communications are covered by the attorney-client privilege and work-product doctrine. For example, if forensic specialists are assisting in responding to an incident, the engagement terms should reflect that their work is at the direction of counsel and protected by the attorney-client privilege and work-product doctrine.

Governance

A key area of regulatory inquiry involves governance or how the cyber risk is managed. For example, the 2018 SEC Cybersecurity Guidance specifically notes that disclosure about how the board of directors oversees management's actions relating to cybersecurity risks is important to investors' assessment of risk oversight.[31]

Similarly, the recent OCIE cybersecurity report and a number of enforcement actions recognize the integral role of senior-level engagement in an effective cybersecurity program.[32] Enforcers want to be assured that an effective governance process is in place to manage the cyber risks.

Policies and Controls

Cybersecurity policies and controls are based on key security areas. For example, this may include patch management to ensure that software is up to date, encryption and two-level authentication to avoid potential theft, access rights and controls, data loss prevention, access management including for departing employees, data segmentation, ensuring backups are made and not accessible to perpetrators, disaster recovery, and the storage and removal of data.[33]

The policies should be reviewed on a regular basis to assess their effectiveness and identify potential risk factors. Regulators have held companies accountable based on their failure to have written policies and procedures in place to safeguard information.[34]

Establishing a Culture of Compliance

Ensure that your training, policies and program promote a culture of compliance, awareness and vigilance. Support from the board of directors and management has proven to be essential to establish a strong culture of compliance. Cyberincidents affect everyone in the company.

Third-Party Vendors

When information is shared with third parties, such as cloud providers, additional cybersecurity vulnerabilities may arise. The Target Corp. data breach was based on a stolen credential obtained from a third-party vendor.[35]

Vendor management processes should be in place to address risk issues. This will include due diligence in the selection of the vendor, contract provisions and measures to safeguard the information, periodic audits and assessments, notification requirements and clear procedures in the event of an incident, and other appropriate safeguards.

Incident Response Plan

Have an incident response plan in place, and test it to know that it will work when needed and the team is integrated. Ensure that the incident response plan is updated for new issues, such as the California Consumer Protection Act and other legislative or regulator developments. Further, it is important to assign staff with specific responsibilities in the event of a cyberincident.[36] In addition, companies should consider maintaining backup data in a different network and offline.[37]

Regulators

Identify your primary regulators at the federal and state levels, and understand their primary areas of cybersecurity focus and enforcement. For example, certain agencies (i.e., the SEC and New York Department of Financial Services) have emphasized particular cybersecurity standards. For public companies, the SEC has noted the importance of a strong insider trading program to avoid unauthorized conduct during an incident.

In order to avoid insider trading questions or investigations, strong insider trading policies should be implemented so companies should have "well designed policies and procedures to prevent trading on the basis of all types of material nonpublic information, including information relating to cybersecurity risks and incidents" and include measures to "protect against directors, officers, and other corporate insiders trading on the basis of material nonpublic information before public disclosure of the cybersecurity incident."[38]

Notifications

When an incident occurs, consider the timeliness of disclosure, who receives notification (customers and/or public agencies) and self-reporting to a potential regulator. Regulators are focusing on the timeliness and sufficiency of the disclosure.[39] Determining the scope of a data breach can take time. Some jurisdictions impose deadlines for requirements. Experienced counsel can work with the company to advise on these legal obligations.

Responding to Cybersecurity Investigations

When an incident occurs, use experienced counsel that has a track record in conducting cybersecurity investigations and responding to regulators. Due to the interest from multiple regulators and overlapping regulations, negotiating the issues that arise in cybersecurity matters is increasingly complex. We have had success in assisting companies and individuals subject to regulatory enforcement by federal and state authorities.

Conclusion

With the increasing focus of regulators on cybersecurity and privacy issues, companies can and should take meaningful steps in advance to prepare for enforcement inquiries. Once an enforcement action commences, companies will be put in a position to respond to legal process and inquiries from multiple regulators and provide documentation. Navigating this process requires coordination and anticipation of multiple issues that may arise.

Mark Krotoski is a partner and Jill Harris is an associate at Morgan Lewis & Bockius LLP.

[1] Andrew Smith, New and improved FTC data security orders: Better guidance for companies, better protection for consumers, (Jan 6, 2020), available at https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance?utm_source=govdelivery.

[2] See, e.g., California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq. (2018).

[3] See SB 6281, Washington Privacy Act (Jan. 2020), https://app.leg.wa.gov/committeeschedules/Home/Document/209620#toolbar=0&navpanes=0; S.B. 220, 2019 80th Sess. (Nev. 2019), available at https://www.leg.state.nv.us/Session/80th2019/Bills/SB/SB220.pdf; S.5642, Reg. Sess. (N.Y. 2019), available at https://legislation.nysenate.gov/pdf/bills/2019/S5642.

[4] See, e.g., Mark Krotoski, Lucy Wang, & Jennifer Rosen, The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze, BNA's Privacy & Security Law Report, 15 PVLR 271

(Feb. 8, 2016), available at https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bna-need-to-repair-data-breach-notification-maze-08feb16.ashx?la=.

[5] LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221 (11th Cir. 2018).

[6] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, United States v. Facebook, Inc., No. 19-cv-2184, at *3 (D.C. Cir. July 24, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

[7] See Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc., No. 1:19-cv-03297-TW (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc; see also Press Release, FTC, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), available at https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

[8] Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc., No. 1:19-cv-03297-TW, at *12 (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.

[9] See In the Matter of Altaba Inc., f/d/b/a Yahoo! Inc., Order Instituting Cease And Desist Proceedings, File No. 3-18448, § IV(A), at 9 (Apr. 24, 2018), available at http://www.sec.gov/litigation/admin/2018/33-10485.pdf; see also Decision and Order, In the Matter of Retina-X Studios, and James N. Johns, Jr., No. 1723118, ¶ III (Oct. 22, 2019) (enjoining violations of the Children's Privacy Protection Rule), available at https://www.ftc.gov/system/files/documents/cases/172_3118_-_retina-x_studios_agreement_containing_consent_order.pdf.

[10] See, e.g., Assurance of Voluntary Compliance, In re Nationwide Mutual Insurance Company and Allied Property & Casualty Insurance Company, ¶ 25 (Aug. 2017), available at https://www.law360.com/articles/952737/attachments/0.

[11] See Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc., No. 1:19-cv-03297-TW, § V, at *24-25 (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.

[12] See, e.g., Stipulated Order for Injunction and Judgment, FTC v. D-Link Systems, Inc., No. 3:17-cv-39-JD, at *10-11, (N.D. Cal. Aug. 6, 2019) (Doc. 276); Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief, United States v. Unixiz, Liu and Zhang, No. 5:19-cv-2222, at *15 (N.D. Cal. May 2, 2019) (Doc. 10); Decision and Order, In re Infotrax Systems, L.C., et al., Docket No. C-4696, ⁋ IV, at *6-7 (Dec. 30, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/162-3130/infotrax-systems-lc; Decision and Order, In re Lightyear Dealer Technologies, LLC d/b/a Dealerbuilt,

Docket No. C-4687, ⁋ IV, at *6 (Sept. 3, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3051/lightyear-dealer-technologies-llc-matter-0; Decision and Order, In re James V. Grago, Jr. d/b/a ClixSense.com, Docket No. C-4678, ⁋ V, at *5 (June 19, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3003/james-v-grago-jr-doing-business-clixsensecom.

[13] See, e.g., Smith, supra.

[14] See Stipulated Order for Injunction and Judgment, FTC v. D-Link Systems, Inc., No. 3:17-cv-39-JD, at *3-4 (N.D. Cal. Aug. 6, 2019) (Doc. 276); Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc., No. 1:19-cv-03297-TW, §§ II(B), V, VI(B), at *13, *24, *26 (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc; Decision and Order, In re Infotrax Systems, L.C., et al., Docket No. C-4696, ⁋ I.B, at *3 (Dec. 30, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/162-3130/infotrax-systems-lc; Decision and Order, In re Lightyear Dealer Technologies, LLC d/b/a Dealerbuilt, Docket No. C-4687, ⁋ I.B, at 3 (Sept. 3, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3051/lightyear-dealer-technologies-llc-matter-0.

[15] See Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc., No. 1:19-cv-03297-TW, § II, at *12-19 (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.

[16] See id. § II(E)(1), at *14 (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.

[17] See Assurance of Voluntary Compliance, In re Nationwide Mutual Insurance Company and Allied Property & Casualty Insurance Company, § 18, at *5 (Aug. 2017), available at https://www.law360.com/articles/952737/attachments/0.

[18] See Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc., No. 1:19-cv-03297-TW, § III, at *19-22 (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.

[19] Decision and Order, In re James V. Grago, Jr. d/b/a ClixSense.com, Docket No. C-4678, ⁋ III, at 4 (June 19, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3003/james-v-grago-jr-doing-business-clixsensecom.

[20] Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc., No. 1:19-cv-03297-TW, § VI, at *25-27 (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc; see also Decision and Order, In re Infotrax Systems, L.C., et al., Docket No. C-4696, ⁋ V, at *7 (Dec. 30, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/162-3130/infotrax-systems-lc.

[21] Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc., No. 1:19-cv-03297-TW, § VI(B), at *26 (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.

[22] See Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc., No. 1:19-cv-03297-TW, § XIX, at *59-60 (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc.

[23] See SEC Press Release, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million (Apr. 24, 2018), available at https://www.sec.gov/news/press-release/2018-71.

[24] See Agreement Containing Consent Order, In the Matter of Retina-X Studios and James N. Johns, Jr., No. 1723118, ¶ 2 (Oct. 22, 2019) ("Proposed Respondents neither admit nor deny any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Proposed Respondents admit the facts necessary to establish jurisdiction."), available at https://www.ftc.gov/system/files/documents/cases/172_3118_-_retina-x_studios_agreement_containing_consent_order.pdf.

[25] See, e.g., Stipulated Order for Injunction and Judgment, FTC v. D-Link Systems, Inc., No. 3:17-cv-39-JD, at 10-11, (N.D. Cal. Aug. 6, 2019) (Doc. 276); Stipulated Order for Permanent Injunction and Monetary Judgment, Federal Trade Commission v. Equifax Inc., No. 1:19-cv-03297-TW, § V, at *24-25 (N.D. Ga. July 23, 2019) (Doc. 6), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc; Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief, United States v. Unixiz, Liu and Zhang, No. 5:19-cv-2222, at 15 (N.D. Cal. May 2, 2019) (Doc. 10); Decision and Order, In re Infotrax Systems, L.C., et al., Docket No. C-4696, ⁋ IV, at *6-7 (Dec. 30, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/162-3130/infotrax-systems-lc; Decision and Order, In re Lightyear Dealer Technologies, LLC d/b/a Dealerbuilt, Docket No. C-4687, ⁋ IV, at *6 (Sept. 3, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3051/lightyear-dealer-technologies-llc-matter-0; Decision and Order, In re James V. Grago, Jr. d/b/a ClixSense.com, Docket No. C-4678, ⁋ V, at *5 (June 19, 2019), available at https://www.ftc.gov/enforcement/cases-proceedings/172-3003/james-v-grago-jr-doing-business-clixsensecom.

[26] See SEC Office of Compliance Inspections and Examinations Publishes Observations on Cybersecurity and Resiliency Practices (Jan. 27, 2020), available at https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[27] Id. at *2.

[28] Id. at *3.

[29] See, e.g., Mark Krotoski, Do You Know Whether Your Trade Secrets Are Adequately Protected?,

BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 181 (Nov. 21, 2014), available at https://www.morganlewis.com/-/media/files/publication/outside-publication/article/bloombergbna_patenttrademarkcopyrightjournal_21nov14.ashx.

[30] See, e.g., Upjohn Co. v. United States, 449 U.S. 383 (1981) (attorney-client privilege protecting corporate communications); Hickman v. Taylor, 329 U.S. 495 (1947) (holding that the work-product doctrine precludes access to materials prepared in anticipation of litigation by an opposing attorney).

[31] Mark Krotoski & Kurt Oldenburg, SEC Issues Guidance On Cybersecurity Disclosures (Feb. 28, 2018), available at https://www.morganlewis.com/pubs/sec-issues-guidance-on-cybersecurity-disclosures.

[32] See SEC Office of Compliance Inspections and Examinations Publishes Observations on Cybersecurity and Resiliency Practices, at *1 (Jan. 27, 2020), available at https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[33] See, e.g., id. at *2-5 (Jan. 27, 2020), available at https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[34] See, e.g., Press Release, SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach (Sept. 22, 2015) (noting violation of the SEC "safeguards rule" when a company "failed to adopt any written policies and procedures to ensure the security and confidentiality of PII and protect it from anticipated threats or unauthorized access"), available at https://www.sec.gov/news/pressrelease/2015-202.html.

[35] See Stephanie Mlot, HVAC Vendor Confirms Link to Target Data Breach, PC Magazine (Feb. 7, 2014), available at https://www.pcmag.com/news/320520/hvac-vendor-confirms-link-to-target-data-breach; see also Krebs on Security, Target Hackers Broke in Via HVAC Company (Feb. 14, 2014) (noting "the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor"), available at https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company.

[36] See SEC Office of Compliance Inspections and Examinations Publishes Observations on Cybersecurity and Resiliency Practices, at *7 (Jan. 27, 2020), available at https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf.

[37] Id. at *8.

[38] See Securities and Exchange Commission, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, at 22 (Feb. 26, 2018), available at https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[39] See id.