THE CYBER INVESTIGATIONS GUIDE

THIRD EDITION

Editors
Benjamin Powell and Shannon Togawa Mercer

The Cyber Investigations Guide

Third Edition

Editors

Benjamin A Powell

Shannon Togawa Mercer

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-253-6

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

Anderson Mōri & Tomotsune

BCL Solicitors LLP

Clifford Chance US LLP

Cravath, Swaine & Moore LLP

Jones Day

K&L Gates LLP

Nyman Gibson Miralis

Ropes & Gray LLP

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher's Note

The Cyber Investigations Guide is published by Global Investigations Review (GIR), the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature by providing an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its seventh edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation from discovery to resolution.

The Cyber Investigations Guide takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Cyber Investigations Guide* as the close-up.

The Cyber Investigations Guide is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

David Samuels
Publisher
May 2023

CHAPTER 7

FTC Investigations and Multistate AG Investigations

Benjamin A Powell, Kirk Nahra and Ariel E Dobkin[1]

Introduction

Significant data breaches and privacy mistakes are likely to draw the attention of many regulators, including the Federal Trade Commission (FTC) and the state attorneys general (state AGs), which view themselves as the consumer protection watchdogs when it comes to privacy and data security issues.

Both the FTC and state AGs have remained remarkably active in this space. In spring 2022, FTC Chair Lina Khan stated her intent to 'approach data privacy and security protections by considering substantive limits rather than just procedural protections', noting that the '"notice and consent" paradigm may be "outdated and insufficient"'.[2] Chair Khan has been extraordinarily forward-leaning in this space; the FTC has engaged in numerous enforcement actions for several years, some of which have expanded beyond the FTC's historical approach by alleging

1 Benjamin A Powell and Kirk Nahra are partners and Ariel E Dobkin is a senior associate at Wilmer Cutler Pickering Hale and Dorr LLP.

2 'Remarks of Chair Lina M. Khan as Prepared for Delivery, IAPP Global Privacy Summit, Washington D.C.' (11 April 2022) (https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf (last accessed 4 April 2023)).

substantive unfairness claims.[3] The Commission has also issued a policy statement on unfairness,[4] and it is undergoing a rule-making to address commercial surveillance and lax data security practices.[5]

State AGs, likewise, continue to focus on data security enforcement, and privacy actions are becoming more prevalent. These settlements can involve hundreds of millions of dollars and onerous injunctive terms.[6]

This chapter seeks to provide an overview of practical considerations when defending a client in an FTC or state AG privacy or data security investigation while highlighting key distinctions between the two that may affect counsel's strategy. As a starting point, FTC investigations often can be more procedurally formal by virtue of their voluminous regulations and guidance, and well-developed

---

3 For example, in February 2023, the Federal Trade Commission (FTC) and the Department of Justice announced a settlement with GoodRx Holdings Inc, based on allegations that the company misrepresented the ways in which it used and protected users' data; the settlement imposes a number of requirements on GoodRx relating to not only its disclosures but also its actual practices with regard to user data (e.g., it may not disclose health information for advertising purposes). See Compl. For Perm. Injunction, Civil Penalties, and Other Relief, *United States v. GoodRx Holdings, Inc.*, No. 3:23-cv-460, ECF No. 1 (N.D. Cal. Feb. 1, 2023) (https://www.ftc.gov/system/files/ftc_gov/pdf/goodrx_complaint_for_permanent_injunction_civil_penalties_and_other_relief.pdf (last accessed 4 April 2023)); Stip. Order for Perm. Injunction, Civil Penalty Judgment, and Other Relief, *United States v. GoodRx Holdings, Inc.*, No. 3:23-cv-460, ECF No. 3-1 (N.D. Cal. Feb. 1, 2023). In addition, in March 2023, the FTC banned BetterHelp, Inc from sharing health data for advertising; it also took its first action ever in which it returned funds to consumers whose health data was compromised when it was shared with third parties. See Compl., *In re BetterHelp, Inc.*, FTC No. 2023169 (https://www.ftc.gov/system/files/ftc_gov/pdf/2023169-betterhelp-complaint_.pdf (last accessed 4 April 2023)); Agreement Containing Consent Order, *In re BetterHelp, Inc.*, FTC No. 2023169 (https://www.ftc.gov/system/files/ftc_gov/pdf/202_3169-betterhelp-consent.pdf (last accessed 4 April 2023)).

4 FTC, Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act, Commission File No. P221202 (10 November 2022) (https://www.ftc.gov/system/files/ftc_gov/pdf/p221202sec5enforcementpolicystatement_002.pdf (last accessed 4 April 2023)).

5 FTC, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed on 22 August 2022) (https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security (last accessed 4 April 2023)).

6 See, e.g., *Commonwealth of Pennsylvania v. Google, LLC*, Assurance of Voluntary Compliance (2022) (https://www.attorneygeneral.gov/wp-content/uploads/2022/11/2022-11-14-PA-v.-Google-LLC-AVC-efile.pdf (last accessed 4 April 2023)); *Commonwealth of Pennsylvania v. Intuit Inc.*, Assurance of Voluntary Compliance (2022) (https://www.attorneygeneral.gov/wp-content/uploads/2022/05/2022-05-04-PA-Intuit-AVC-accepted-efiling.pdf (last accessed 4 April 2023)).

administrative and federal case law. Conversely, state AG investigations can be more informal in light of their comparatively brief statutory authority and scant case law.

Key differences

Structure

The FTC is an independent agency headed by five commissioners, nominated by the President and confirmed by the Senate, each serving a seven-year term. No more than three commissioners can be of the same political party. The President chooses one commissioner to act as chairman. State attorneys general are elected by popular vote or appointed by the governor.[7] Many state AGs have subsequently been elected to the US Senate, governorships and other higher government offices.

Authority

The FTC relies on its authority under Section 5(a) of the Federal Trade Commission Act (FTC Act) to investigate privacy and data security matters, using its general authority to regulate 'unfair or deceptive' practices. By contrast, all 50 state AGs are empowered to investigate suspected violations of similar, state-level unfair and deceptive practices laws, and they also have the ability to enforce under state data breach notification statutes. These statutes allow the AGs to investigate and enforce against companies that are found not to have notified affected individuals or the proper authorities of a breach within the required statutory period.

External counsel

The FTC does not work with private external counsel to investigate or bring consumer protection cases.[8] State AGs may retain law firms to represent their states in consumer protection matters, including data security cases.[9]

---

7 Except Maine, where the state AG is elected by a secret ballot of the legislature, and in Tennessee, where election is by the state supreme court.

8 An executive order even bars federal agencies, including the FTC, from hiring outside lawyers on a contingency-fee basis. See Exec. Order No. 13,433, Protecting American Taxpayers from Payment of Contingency Fees, 72 Fed. Reg. 28441 (18 May 2007).

9 See Eric Lipton, 'Lawyers Create Big Paydays by Coaxing Attorneys General to Sue', *The New York Times* (18 December 2014) (www.nytimes.com/2014/12/19/us/politics/lawyers-create-big-paydays-by-coaxing-attorneys-general-to-sue-.html (last accessed 4 April 2023)).

Confidentiality

FTC investigations are confidential and the information and materials produced to the FTC during the course of an investigation are generally protected from disclosure under the Freedom of Information Act,[10] with limited exceptions. By contrast, state AGs' offices frequently publicly announce the initiation of an investigation, and protections from third-party disclosure vary greatly by state statute.[11] Typically, FTC closures of investigation without enforcement activity are not public.

Civil penalties

The FTC can only impose civil penalties if a company has violated a consent order or a trade regulation rule promulgated by the Commission. Most state statutes allow state AGs to immediately seek civil penalties of around US$5,000 per violation.

Introduction to the Federal Trade Commission

Authority

The FTC enforces the FTC Act, Section 5(a) of which prohibits 'unfair or deceptive acts or practices in or affecting commerce'.[12] This language serves as the basis for the FTC's jurisdiction over consumer protection matters, including those relating to consumer privacy and data security. Since the early 2000s, the FTC has brought more than 80 general privacy lawsuits and 80 cases alleging inadequate data security.[13] These have generally ended in settlements imposing injunctive terms, such as comprehensive security or privacy programmes. These settlements, as noted above, allow the Commission to bring a later suit for civil penalties if it believes the company has violated the injunctive terms.

This authority has been affirmed by federal courts, perhaps most notably in *FTC v. Wyndham Worldwide Corp*, in which the Third Circuit held that certain data security practices could be considered 'unfair' under Section 45(a), and that, in this instance, the relevant provision provided Wyndham fair notice that its practices opened it up to liability under the Act.[14]

---

10 5 U.S.C. § 552.

11 Compare Fla. Stat. §§ 119.071 to 19.0715 with Tex. Gov't Code Ann. §§ 552.101 to 552.162.

12 15 U.S.C. § 45.

13 *FTC Report to Congress on Privacy and Security* (13 September 2021) (https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf (last accessed 4 April 2023)).

14 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir 2015).

Initiation of an investigation

The FTC has broad statutory authority to 'gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce'.[15] Although FTC staff do not typically disclose the catalyst of an investigation, investigations may be initiated in response to consumer or industry complaints, blog posts by advocates or security researchers, other government agency requests, court referrals or independent investigations by the Commission. FTC investigations are also typically confidential[16] but there are several exemptions to this rule, including disclosure to a congressional committee or to other law enforcement agencies.[17]

The FTC typically initiates an investigation by serving on the target either a hold letter, with an access letter (otherwise known as a 'demand for information'), or a civil investigative demand (CID).[18] A hold letter typically only requires the recipient to preserve certain documents or information (see following paragraph for a discussion of document holds). Access letters are informal requests for information or testimony (oral or written). Similar to an access letter, a CID requests information or testimony (oral or written); however, the Director of the FTC's Bureau of Consumer Protection and one commissioner's office must approve the issuance of the CID. In the event a target does not comply with a CID, the FTC may seek enforcement in court through the Department of Justice under Section 16 of the FTC Act.[19]

Another tool in the FTC's investigative belt is Section 6 of the FTC Act, which permits the Commission to require the filing of 'annual or special reports or answers in writing to specific questions' for the purpose of obtaining information about 'the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals' of the entities to whom the enquiry is addressed.[20] These reports do not necessarily have a law enforcement purpose.

---

15 15 U.S.C. § 46(a).

16 15 U.S.C. § 57b-2.

17 See, e.g., 16 C.F.R. § 4.11.

18 Subpoenas are not available in consumer protection matters. 15 U.S.C. § 57b-1.

19 15 U.S.C. § 57(b)1(e).

20 Federal Trade Commission Act (FTC Act), Section 46 (Sec. 6) para. (b). As with subpoenas and CIDs, the recipient of a 6(b) order may file a petition to limit or quash, and the Commission may seek a court order requiring compliance.

On receipt of a letter or CID from the FTC, a target should first put in place a document hold to preserve any relevant documents and information. The letter or CID may reflect specific topics or documents of concern; however, the target should consider whether to broaden the hold to cover any documents or custodians with potentially relevant documents. For many clients, a document hold involves both (1) notifying and requesting acknowledgement from custodians of the hold and (2) placing a technical hold on the back end of any systems that may roll over, including email and other data storage.

Meet-and-confer

After reviewing the letter or CID (or both), counsel should reach out to the FTC staff handling the case to acknowledge receipt and schedule a meeting to discuss a response timeline. Although it is prudent to reach out early in the investigation to staff in any event, if a target receives a CID, the company is required to schedule a meet-and-confer within 14 days of receipt.[21]

To prepare for the meeting, it is important to understand the basic facts of the case and identify the employees with relevant knowledge or involvement and key documents. In addition, counsel will need to understand the scope of the letter or CID requests and the burden on the client in responding to these requests. Some documents and information may be easy to provide quickly to the FTC, while other information sought may not be kept in the normal course of business and require vast amounts of time and resources to compile. For other requests, the volume of documents alone may be nearly impossible to produce by the return date stated in the letter or CID.

Negotiating the timing and scope of the productions is the main objective at the meet-and-confer, but it also provides an opportunity to converse with the FTC staff about the focus of the investigation. This focus will guide the discussion and help the parties to identify priorities and agree on a reasonable production schedule. The FTC staff may agree to modify the timeline and scope of the production; however, it is typically without prejudice to come back and request full compliance, especially in the case of a CID.

Timing

Letters and CIDs typically include a deadline that is impossible to meet. Often, the FTC staff will agree to a rolling production of materials if the target can provide cogent explanations as to why the deadline included in the letter is not

21 16 C.F.R. § 2.7(k).

realistic, and further provide that the target make an initial production by the return date on the CID or access letter. Here, it can be helpful to understand which requests are of greatest priority to the FTC staff and schedule accordingly.

Scope

Often, the FTC will seek 'any and all' documents or 'any and all' information relating to a specific topic. Consider alternative proposals such as (1) providing documents 'sufficient to show', (2) limiting the number of custodians, (3) limiting the document by agreed search terms, (4) providing a narrative response in lieu of documents and (5) limiting the response time limit. Providing a convincing argument why the FTC staff should accept your proposal is critical, considering arguments such as 'this custodian is most likely to have the documents of interest' or 'this few month period is the most relevant one' or 'we will simply drown in the millions of documents responsive to these requests over the multi-year period it will take for [the company] to produce them'. While the burden to your client in producing the materials can be considered, the FTC staff are more likely to be amenable to proposals designed to provide the most relevant materials as quickly as possible, without prejudice to seek more later.

The FTC staff will typically record the production schedule in writing after the meeting. This mitigates the likelihood of a misunderstanding regarding timelines and makes the company accountable. If an agreement regarding the timing or scope of a subpoena cannot be reached, the target can move to quash the CID. The target must file the motion to quash with the Commission before the sooner of 20 days after service of the CID or the return date of the CID.[22]

Understanding the investigation

Once the recipient understands the focus of the investigation, it is advisable to conduct a privileged, internal investigation led by counsel to understand the conduct of potential interest. This will assist in understanding potential liability, developing defensive and advocacy strategy, and, if warranted, take advance corrective action if an issue is identified. See the chapter on the art of investigating for additional considerations in an internal investigation.

22 16 C.F.R. § 2.10.

Document production

Once a production schedule is agreed, document collection should begin, if it has not already. Depending on the scope of the production, it may require conducting collection interviews, during which the custodians discuss with counsel leading e-discovery each of the places the individual may have stored responsive documents, including those stored locally, in the cloud and on shared drives; certain requests may extend to chats or other client-specific means of communication (e.g., Slack or Signal). Counsel should confirm with custodians whether they use personal forms of communication (e.g., personal email or text messaging) for work purposes; if so, those communications should also be collected.

Counsel should review all documents before production to the FTC staff. In addition to confirming responsiveness and screening for privilege, this review can help inform the company's internal investigation and gain insight into potential theories of liability the FTC staff may develop. If a client is concerned about cost, consider developing ways to review a sample of the documents, use artificial intelligence to identify certain categories for review, or craft search terms for documents that are most likely to give rise to liability for the client.

Many clients are very concerned about keeping their documents confidential. This is particularly true in a data security context if requested materials may reflect sensitive security documents, such as incident response plans, threat assessments or network diagrams. The FTC Act prohibits disclosure of confidential information, testimony and materials submitted pursuant to a CID, and materials otherwise marked confidential.[23] It is required to label sensitive documents and information as confidential, and you should request that these documents and information be returned or destroyed by the FTC at the conclusion of the investigation.

Counsel should only agree to production deadlines that are realistic, but of course, unanticipated issues arise to delay production. Reaching out to the FTC staff as soon as reasonably practicable about a potential delay (preferably not the day the production is due), with a clear explanation and a new deadline, can help maintain goodwill and credibility with FTC staff.

23 15 U.S.C. § 46(f); ibid. § 57b-2(b); ibid. § 57b-2(c).

Written and oral testimony

FTC staff may request written responses to interrogatories or accept a written response in lieu of document production. Written responses should seek first to answer the question posed but should also be viewed as an opportunity for affirmative advocacy. You can include information designed to allay staff concerns, providing an overview of added protections or industry comparisons.

Consider whether to include materials supporting the authority of the written statements. If relying on employee statements, provide information about why that employee knows the most about the topics and should be trusted. If speaking to general practices, consider the submission of ordinary course of business documents that support the proposition. In some cases, documents alone may be more persuasive than a written submission, and the rules of practice dictate that you may submit documents in lieu of a written response if the documents meet the substance of the interrogatory specifications.[24]

The FTC may also take oral testimony during investigative hearings; however, this is an infrequent practice, most often seen in fraud and national advertising cases.[25]

Advocacy

Advocacy is intentionally included after document production and written and oral testimony in this chapter. Each interaction with the FTC staff is an opportunity for advocacy to explain and contextualise issues; however, FTC staff may be unwilling to fully engage with white papers and presentations (or other materials that are solely advocacy-focused) until they have received responses to their questions and at a least a large number of the requested documents. Launching into advocacy before the FTC staff feel that they understand the facts is likely to undercut its efficacy, and perhaps even annoy them.

In addition to conversations with FTC staff, looking to recent FTC enforcement actions and staff speeches may help to identify the focus of the investigation and place it in the context of the FTC's enforcement priorities. Understanding these priorities should inform negotiation and advocacy tactics.

24 16 C.F.R. § 3.35.

25 These hearings are similar to depositions, except counsel is not allowed to object to lines of questioning. However, time-outs with the witness are permitted.

The form of the advocacy will depend on the facts of the matter and the preferences of the FTC staff. While a long-form white paper with witness declarations and expert reports can provide greater detail on a subject, a presentation with visuals may have greater impact.

Resolution

At the conclusion of an investigation, and based on the recommendation of the FTC staff, the Commission may vote to (1) close the investigation, (2) seek a consent order, (3) file a complaint in administrative court or (4) authorise the FTC staff to file a complaint and litigate in federal court. Before an enforcement recommendation is presented to the Commission, the FTC staff typically present the company with a draft complaint or consent decree, providing the company an opportunity to advocate to the FTC staff and, if needed, escalate to the Director of the Bureau of Consumer Protection and demonstrate that enforcement is unwarranted or to negotiate more favourable terms of the proposed consent decree.

Voluntary closure

The FTC may close the case if it finds there was no violation of law, an enforcement action would not further the public interest, or it would be likely to lose if the matter proceeded to litigation. If the investigation was initiated with an access letter, no formal vote is required to close. Instead, discretion to close is left to the FTC staff. The FTC may also recommend that the company take certain corrective action in connection with the closure, but without a formal consent decree (and, thus, formal enforcement mechanism).

A company may request a formal closing letter; note, however, that such a letter goes on the public record.[26] If your client wishes the investigation to remain confidential, you can also request that the FTC staff forgo issuing a closing letter.

Consent agreements

A consent agreement may be negotiated between the FTC staff and the company to conclude the investigation. These agreements provide relief similar to a cease-and-desist order, and include a proposed complaint, and decision and order. An admission of liability is not required. Agreements typically impose an injunction prohibiting the practices alleged in the draft complaint, a privacy-by-design or security-by-design programme, biannual audits by a qualified independent

26 16 C.F.R. § 14.9(b)(4)(ii).

third party for 20 years, a compliance report, and standard record-keeping and reporting requirements. These agreements may also include 'fencing in' provisions, designed to prevent the company from engaging in similar misconduct.

Once drafted, a proposed agreement is reviewed by the FTC and, if accepted, the proposed order, complaint and consent agreement are put on the public record for a 30-day comment period.[27] Following this period, the Commission may issue the complaint and order, withdraw its acceptance of the agreement or modify the order. Orders are considered final 60 days after issuance.[28]

Consent agreements can help clients avoid the cost and potential embarrassment associated with a protracted litigation. Depending on the conduct at issue and the goodwill and credibility built up with the FTC staff, you may be able to help craft the complaint. You may also negotiate the language of the agreement although much of the privacy and data security agreements is standardised. Fruitful considerations for negotiating a consent include:

- the scope of the injunction;
- definitions;
- the frequency and scope of the reporting requirements;
- the duration of the record-keeping requirements; and
- the entities covered.

Administration hearing (Part 3 adjudication)

If, by a majority vote, the FTC determines that it has reason to believe that the law has been violated and that a proceeding would be in the public interest, it may issue a complaint to be litigated by FTC staff before an administrative law judge (ALJ), according to the FTC's Rules of Practice for Adjudicative Proceedings.[29] At the conclusion of the hearing, the ALJ will issue an initial decision with findings of facts and conclusion of law and will recommend either an entry of a cease-and-desist order or dismissal of the complaint. Cease-and-desist orders are

27 16 C.F.R. § 2.34(c). This is also true for consent agreements resolving cases filed in administrative court; however, it does not apply to order files in federal court under Section 13(b).

28 FTC, 'A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority' (July 2008, revised May 2021) (www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last accessed 4 April 2023)).

29 16 C.F.R. §§ 3.1 to 3.83.

substantively similar to consent agreements and typically include the same types of provisions, including a 20-year sunset period. Civil penalties are not available in first instance administrative proceedings.[30]

The ALJ's decision, if appealed, is reviewed *de novo* by the FTC.[31] The respondent may appeal the Commission's final order to a federal circuit court, which will review the Commission's legal conclusions *de novo*.[32] Critics of the Part 3 adjudication proceedings argue that because the FTC effectively serves as investigator, prosecutor and arbitrator, the proceedings are inherently unfair.[33]

Federal court (Section 13(b))

The FTC may also file a complaint and seek an order in federal court.[34] Pursuant to Section 13(b), the FTC may seek preliminary and permanent injunctions and other equitable relief if a violation of the FTC Act is ongoing or likely to occur.[35] According to the FTC, most consumer protection enforcement is now conducted directly in court under Section 13(b) rather than by means of administrative adjudication because 'in such a suit, the court may award both prohibitory

30 15 U.S.C. § 45(1) authorises penalties for violations of an administrative order, such a consent decree or cease-and-desist order.

31 16 C.F.R. § 3.52.

32 Courts review the FTC's legal decisions *de novo* but give 'some deference to [its] informed judgment that a particular commercial practice is to be condemned as "unfair"'. *FTC v. Ind. Fed'n of Dentists*, 476 U.S. 447, 454 (1986).

33 Maureen K Ohlhausen, 'Administrative Litigation at the FTC: Effective Tool for Developing the Law or Rubber Stamp', *J. Comp. L. & Econ.*, 1–37 (2016), at 3 (https://www.ftc.gov/system/files/documents/public_statements/1005443/ohlhausen_-_administrative_litigation_at_the_ftc_effective_tool_for_developing_the_law_or_rubber.pdf (last accessed 4 April 2023)) ('Nevertheless, the FTC's administrative litigation process, examined in Part III.A, stands accused of being a rigged system. In a Part 3 proceeding, the FTC serves prosecutorial and adjudicative roles.').

34 FTC, Brief Overview (op. cit. note 28). (Section 16 of the FTC Act, 15 U.S.C. Section 56, authorises the FTC to represent itself by its own attorneys in five categories of cases: (1) suits for injunctive relief under Section 13 of the FTC Act, 15 U.S.C. Section 53; (2) suits for consumer redress under Section 19 of the FTC Act, 15 U.S.C. Section 57b; (3) petitions for judicial review of FTC rules or orders or a cease-and-desist order issued under Section 5 of the FTC Act, 15 U.S.C. Section 45; (4) suits to enforce compulsory process under Sections 6 and 9 of the FTC Act, 15 U.S.C. Sections 46 and 49.3; and (5) suits to prohibit recipients of compulsory process from disclosing the existence of the process in certain situations, Section 21a of the FTC Act, 15 U.S.C. Section 57b-2a.)

35 *U.S. Oil & Gas Corp.*, 748 F.2d 1431, 1434 (11th Cir 1984) (quoting *H. N. Singer, Inc.*, 668 F.2d 1107, 1113 (9th Cir 1982)).

and monetary equitable relief in one step'.[36] Although the resulting orders from such litigation may be substantively similar to an administrative cease-and-desist order, they do not typically include the 20-year sunset provision.

Limits on authority

The FTC's authority to impose requirements in an order is not without limits. The US Court of Appeals for the Eleventh Circuit vacated a cease-and-desist order by the FTC issued against LabMD, Inc arising from an FTC enforcement action alleging that LabMD's data security programme was unreasonable and, therefore, constituted an unfair act or practice under Section 5 of the FTC Act.[37] The Court found that it 'mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished' and in turn held that 'the prohibitions contained in cease and desist orders . . . must be specific'.[38] Counsel should cite to this ruling when negotiating a settlement or order that is overly broad and not specific to the conduct at issue.

In April 2021, the US Supreme Court held that Section 13(b) of the FTC Act does not authorise the Commission to pursue equitable monetary relief.[39] The Court held, based on the Act's language and structure, that Section 13(b) authorises the FTC to seek injunctions but makes no mention of monetary relief. The Court emphasised that other FTC Act sections – notably Sections 5(l) and 19 – do authorise the FTC to pursue monetary remedies, subject to identified limitations.

State AG investigations

Authority

State attorneys are given authority to investigate businesses or individuals suspected of engaging in unfair, deceptive or abusive practices (UDAP). These provisions are sometimes referred to as 'little FTC Acts'[40] and the dearth of

---

36 FTC, Brief Overview (op. cit. note 28); see, also, *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1024–28 (7th Cir 1988); *U.S. Oil & Gas*, 748 F.2d at 1432–35 (*per curiam*); *H. N. Singer, Inc.*, 668 F.2d at 1110–13.

37 *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir 2018); see, also, Kim Phan et al., 'Eleventh Circuit Concludes FTC Data Security Order Unenforceable Because Standards Not Specific Enough', WilmerHale (12 June 2018) (www.wilmerhale.com/en/insights/client-alerts/20180612-eleventh-circuit-concludes-ftc-data-security-order-unenforceable-because-standards-not-specific-enough (last accessed 4 April 2023)).

38 *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir 2018).

39 *AMG Cap. Mgmt., LLC v. FTC*, 593 U.S.__, 141 S. Ct. 1341, 1344 (2021).

40 Jack E Karns, 'State Regulation of Deceptive Trade Practices Under "Little FTC Acts": Should Federal Standards Control?', 94 *Dick. L. Rev.* 373, 374 (1989–1990).

regulations and case law provides substantial power to the state AGs on how they can be interpreted.[41] In the data security context, AGs bring UDAP claims on a similar theory to the FTC; namely that by suffering a breach, a company has failed to keep its promises to consumers to keep their data safe, which is an unfair and deceptive practice. In addition to this UDAP authority, 50 states and Washington, DC, have laws requiring entities to notify individuals of breaches involving personally identifiable information; more than 30 states require entities to notify the AG of a breach, in at least some circumstances. AGs can investigate and bring a claim against companies for failing to notify under these state statutes.

Initiation of an investigation

State AGs are empowered, among other things, to investigate and enforce the consumer protection laws of their respective state.[42] As such, their investigatory powers are broad and they are generally authorised to demand production of information and materials that are 'reasonably related' to their investigation.[43] State AG investigations can be triggered by media coverage, consumer complaints, whistleblowers, or even a perceived risk to consumers. In the data security context, an AG's office may see media coverage of an incident or, if the state requires AG notification in the event of a breach, receive a letter from a company notifying them of an incident.

---

41 See, for example, Cal. Bus. & Prof. Code Section 17500, which makes it unlawful 'for any person, . . . corporation . . . or any employee thereof with intent directly or indirectly to dispose of real or personal property or to perform services . . . or to induce the public to enter into any obligation relating thereto, to make or disseminate . . . before the public in this state, . . . in any newspaper or other publication . . . or in any other manner or means whatever . . . any statement, concerning that real or personal property or those services . . . which is untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading'; see also Massachusetts Section 2 of Chapter 93A, which declares unlawful any '[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce'; N.Y. Gen. Bus. Law, §§ 349, 350.

42 See, e.g., N.Y. Gen. Bus. Law, §§ 349, 350.

43 See, e.g., *Fielder v. Berkeley Props. Co.*, 23 Cal. App. 3d 30, 38–39, 99 Cal. Rptr. 791, 796–97 (Ct App 1972) ('Insofar as the prohibition against unreasonable searches and seizures can be said to apply at all it requires only that the inquiry be one which the agency demanding production is authorized to make, that the demand be not too indefinite, and that the information sought be reasonably relevant.').

A state AG may initiate an investigation by sending a litigation hold, an informal letter, a CID, or a subpoena for information and documents. Immediately upon notice of receipt, the company should place a hold on relevant custodial documents. (See FTC subsection titled 'Initiation of an investigation', above, for considerations in drafting and executing a document hold.)

Confidentiality protections are weaker in state AG investigations than FTC investigations. As mentioned above, an AG's office may announce publicly it is investigating a company or incident.[44] Additionally, materials produced to a state AG's office may not be protected from disclosure. State open records laws, also known as 'sunshine laws', vary greatly, and it is important to determine whether there are any applicable exemptions shielding documents from disclosure, including for investigatory materials provided in response to a subpoena.[45] Some states, however, will only exempt trade secret or other confidential business material from public disclosure.[46]

Counsel should discuss with the AG office staff handling the matter whether they would consider entering into a confidentiality agreement before the company produces any documents. This agreement should include provisions contemplating whether documents may be shared with other government entities or AG offices, notice in the event that the AG receives an open records request, and how to handle the documents at the conclusion of the investigation. Some offices will decline to enter into an agreement, citing sufficient protection from the state statutes, while others may decline simply as a matter of practice. Note that no matter

44 See, e.g., Dan M Clark, 'NY AG Announces Probe of Marriott Data Breach and Its Failure to Report Incident', *New York Law Journal* (30 November 2018) (https://www.law.com/newyorklawjournal/2018/11/30/ny-ag-announces-probe-of-marriott-data-breach-and-its-failure-to-report-incident/ (last accessed 4 April 2023)); Reuters, 'US attorneys general investigating Google data breach', *New York Post* (9 October 2018), https://nypost.com/2018/10/09/us-attorneys-general-investigating-google-data-breach/ (last accessed 4 April 2023)).

45 See, e.g., Mass. Gen. Laws ch. 93A, Section 6.

46 See, e.g., Fla. Stat. § 815.045.

what confidentiality protection has been negotiated in the agreement, case law may prohibit the offices from entering into confidentiality agreements that would override or supersede these open record statutes.[47]

Multistate investigations

AGs can also leverage resources by working together and forming multistate investigations, with an executive committee typically consisting of two to eight states taking the investigatory lead. Multistate investigations are most common in large-scale data breaches that affect large numbers of consumers in multiple states.[48] However, some AG offices have expressed their dissatisfaction with the multistate model, pointing to delays in investigations or settlements resulting from coordination issues.

If possible, negotiate so that the company is producing materials only to the executive committee to decrease the risk of a document leak or successful open records request. Relatedly, confidentiality agreements are particularly important

47 See, e.g., *Nat'l Collegiate Athletic Ass'n v. Associated Press*, 18 So. 3d 1201, 1207 (Fla Dist Ct App 2009), review denied, 37 So. 3d 848 (Fla 2010), in which the court held that a confidentiality agreement entered into by a private law firm on behalf of a state university with the National Collegiate Athletic Association (NCAA) that allowed access to records contained on the NCAA's secure custodial website that were used by the university in preparing a response to possible NCAA sanctions, had no effect on whether these were public records, stating that a 'public record cannot be transformed into a private record merely because an agent of the government has promised that it will be kept private'. See, also, *City of Pinellas Park v. Times Publ'g Co.*, No. 00-008234CI-19 (Fla 6th Cir Ct 3 January 2001) ('there is absolutely no doubt that promises of confidentiality [given to employees who were asked to respond to a survey] do not empower the Court to depart from the public records law').

48 Press release, Office of AG Maura Healey, 'AG Healey Leads Multistate Coalition in Reaching $148 Million Settlement With Uber Over Nationwide Data Breach', (26 September 2018) (https://www.mass.gov/news/ag-healey-leads-multistate-coalition-in-reaching-148-million-settlement-with-uber-over (last accessed 4 April 2023)); see, also, B Colby Hamilton, 'Nationwide reaches $5.5M data breach settlement with 33AGs', Property Casualty 360° (11 August 2017) (www.propertycasualty360.com/2017/08/11/nationwide-reaches-5-5m-data-breach-settlement-wit/?slreturn=20190212205913 (last accessed 4 April 2023)); News release, Office of AG Ken Paxton, 'AG Patton Announces $1.5 Million Settlement with Neiman Marcus over Data Breach' (8 January 2019) (www.texasattorneygeneral.gov/news/releases/ag-paxton-announces-15-million-settlement-neiman-marcus-over-data-breach (last accessed 4 April 2023)); Press release, Office of AG Letitia James, 'A.G. Schneiderman Announces $18.5 Million Multi-State Settlement With Target Corporation Over 2013 Data Breach' (23 May 2017) (https://ag.ny.gov/press-release/2017/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation (last accessed 4 April 2023)).

in multistate investigations where the state laws will vary widely. AGs are typically more willing to enter into confidentiality agreements in the multistate context, and some AG offices will agree to apply the confidentiality obligations of the state from which they are receiving the documents if their own state laws provide less protection.

Initial response and document production

There is no requirement to meet-and-confer with AG staff within a set number of days. However, CIDs and subpoenas typically include a response date (generally 30 or 45 days), by which a company should make at least an initial, good faith production. To produce all the required documents to the AG within the time limit, it is advisable to reach out to the AG's office to negotiate scope a few weeks before the deadline. (See FTC subsection titled 'Meet-and-confer', above, for tips on negotiating the scope of a letter, CID or subpoena.) AG offices may be more willing than FTC staff to have a flexible, rolling production schedule.

Document requests will frequently seek 'any and all documents' concerning a certain topic, but the office may agree to reduce the requirements based on reasonable search terms and custodians most likely to have the relevant documents. The AG office may not request the search terms and custodian list itself; however, any cover letters accompanying the production should make clear you are providing relevant documents identified by running search terms over certain custodial documents.

As with FTC productions, counsel should ensure all potentially relevant documents are collected, review the documents before they are submitted to the AG, label confidential documents as such, and meet any agreed production deadlines.

If an agreement on a production schedule cannot be reached with the office, counsel should review local practice and civil procedure to determine whether it would be appropriate to file a motion to quash the subpoena. Most state civil procedure requires AG offices to file a motion to compel before a motion to quash may be filed, but it is important not to miss the window.[49]

Strategy and advocacy

As in FTC investigations, each interaction with the AG's office is an opportunity to advocate for your client. Assess whether a white paper or presentation (or both, perhaps) most effectively lays out your clients' defences. Generally, it is advisable to find time to have a meeting with the AG's office to discuss any

49 See, e.g., Cal. Gov't Code, §§ 11187, 11188.

potential concerns in the case after the bulk of information or documents have been produced and a written advocacy piece has been submitted. Hearing from the AG's office directly what is of most concern provides counsel with an opportunity to provide immediate feedback.

In multistate investigations, it can be difficult because of scheduling conflicts and budget constraints to meet all the states, or even just the executive committee, in person. However, these in-person discussions with the AGs are invaluable and offer counsel an opportunity to efficiently address any concerns and make sure the different offices are on the same page.

Resolution

State AG data security investigations are typically voluntarily closed or resolved with a settlement (although state AGs often do not indicate as a formal matter that an investigation is closed – the target just may not hear from them again). The AG's office may close the investigation if it finds there is no violation of law or the company has voluntarily made modifications to its data security programme to rectify any perceived failures or deficiencies.

The majority of state AG settlements are formal legal documents, filed in state court and typically styled as an assurance of discontinuance, an assurance of voluntary compliance or a stipulated judgment.[50] Stipulated judgments typically differ from assurances of discontinuance and assurances of voluntary compliance only in that they typically include findings of fact and violation of law. In multistate AG investigations, the document may also be styled as a 'consent decree', which is then filed in various state courts as a stipulated judgment. These settlements are not considered an admission of guilt (and many such agreements have 'neither admit nor deny' provisions) but, if violated, the agreements have the same force of law as an injunction, judgment or final court order.

State AG settlements typically reflect similar provisions as FTC settlements, including prohibiting the company from making misrepresentations regarding the extent to which the company protects the privacy, confidentiality, security or integrity of personal information, and requiring the company to cease any violative conduct, implement privacy and security programmes and perform regular independent assessments of the company's data practices, to be reported to the AGs at regular intervals. Notably, these settlements typically include fines ranging from US$20,000 to much higher numbers, as in the *Google*, *Intuit*, *Uber* and *Equifax* matters.

50 See, e.g., VCPA, § 59.1-202; D.C. Code, § 28-4512; R.C.W., § 19.16.480.

State AG data security cases rarely proceed to litigation. To bring a UDAP claim, many state AGs do not have to show that the unfair or deceptive conduct resulted in actual harm or injury to receive injunctive relief and do not have to demonstrate monetary harm to consumers to receive civil penalties.[51] These statutes typically authorise the AGs to bring damages of up to US$5,000 per violation – and how a 'violation' is defined is open to interpretation.[52] Moreover, state AG privacy or data security cases generally cannot be consolidated across states, relegating a company to responding to suits in several state courts at once. The relatively low bar for bringing a successful claim, coupled with the potentially high civil penalties available, make many clients reluctant to litigate, even if they believe they have a good case.

Practice points

Rising cost of compliance

Compliance with a request from the FTC or an AG can be extremely expensive for a client, even if the matter results in a voluntary closure. The advent of e-discovery makes it easy for the FTC or AG staff to ingest hundreds of thousands of documents and search for those of greatest interest using key words, instead of paging through hard copies. Conversely, it is expensive for a client to dedicate the resources necessary to identifying the right documents, collecting the

---

51 See, e.g., D.C. Code Ann., § 28-3904 (West 2015) (stating that a person violates the law 'whether or not any consumer is in fact misled, deceived or damaged thereby'); Md. Code Ann., Com. Law §§ 13-301(1), 13-302 (West 2013) (providing that the capacity or tendency to deceive establishes a violation 'whether or not any consumer in fact has been misled, deceived, or damaged as a result of that practice'); *People ex rel. Lockyer v. Fremont Life Ins. Co.*, 128 Cal. Rptr. 2d 463, 470–71 (Cal Ct App 2002) (finding the test is 'whether the public is likely to be deceived . . . even if no one was actually deceived, relied upon the fraudulent practice, or sustained any damage') (citing *State Farm Fire & Cas. Co. v. Super. Ct.*, 53 Cal. Rptr. 2d 229, 235 (Cal Ct App 1996)); *State ex rel. McLeod v. Brown*, 294 S.E.2d 781, 783 (SC 1982) (finding a tendency to deceive and mislead without proof of actual deception is sufficient to establish liability); *Goshen v. Mutual Life Ins. Co. of N.Y.*, 98 N.Y.2d 314, 324 (NY 2002) ('Unlike private plaintiffs, the Attorney General may, for example, seek injunctive relief without a showing of injury . . . On its face, General Business Law § 349(a) declares deceptive conduct unlawful without reference to whether it has actually caused specific pecuniary harm to consumers in general . . . [T]he deception itself is the harm that the statute seeks to remedy[.]'); *Rule v. Fort Dodge Animal Health, Inc.*, 607 F.3d 250, 255 (1st Cir 2010) (noting that Mass. Gen. Laws ch. 93A, Section 2(a) claim brought by consumer requires injury, although ch. 93A claim brought by the Commonwealth does not).

52 Mass. Gen. Laws, ch. 93A, § 4; N.Y. Gen. Bus. Law, § 350-d.

documents and having counsel review them prior to production. Accordingly, in recent years, the strategy for defending an investigation has become increasingly focused on alleviating the burden on the client.

Importance of compliance planning

Because of these high costs, companies should pay careful attention to their compliance programmes and decision-making in respect of privacy and data security. Effective legal advice (and advice from privacy and compliance officers) often will raise issues of concern before business decisions are made, to avoid situations that are likely to be of interest to these enforcement officials.

Beware collateral consequences

In determining whether to proceed to litigation if parties are unable to come to an agreement, the client should be aware of potential collateral consequences, including bad press coverage and private litigants. Class action follow-on lawsuits are becoming increasingly common in the data security context.

Importance of building rapport, credibility and goodwill

Keeping in mind the staff's constrained time and resources, it is generally advisable to overcommunicate with them at the outset of an investigation to build rapport and underscore that the company is taking the investigation seriously. Responding quickly to concerns raised by staff, including taking efforts or steps to correct potentially problematic processes or behaviour, can further build credibility. A good relationship with the staff can go a long way towards reaching a favourable outcome for your client.