Bloomberg BNA

Privacy and Security Law Report®

A Primer on FTC Expectations for Your Partner and Vendor Relationships: Enforcement Shows You *Are* Your Brother's Keeper

BY D. REED FREEMAN JR. AND MAURY RIGGAN

With all of the privacy and data security enforcement actions brought by the Federal Trade Commission in recent years, and with all of the guidance distributed by the FTC in that time frame, it is easy to get caught up in making sure your privacy and data security practices are in order and compliant with Section 5 of the FTC Act. But even if you do that, there is a blind spot that can result in a data breach, a privacy violation and a resulting investigation and possible FTC order: the use of data by your vendors and business partners. The purpose of this primer is to call your attention to that blind spot and provide guidance on how you can address it before it causes big problems for you.

The FTC has made its position clear on vendor oversight requirements when it comes to privacy and cybersecurity: companies can and will be held responsible for their vendors' failures. Over the course of the past decade, the FTC has effectively announced a position that a company can be held legally responsible for privacy violations, or data breaches occurring as a result of its vendors' unreasonable security practices, if the company failed to perform adequate due diligence, implement appropriate contract provisions or exercise sufficient oversight.

D. Reed Freeman Jr. is a partner and co-chair of the Cybersecurity, Privacy and Communications practice at Wilmer Cutler Pickering Hale and Dorr LLP in Washington.

Maury Riggan is an associate at WilmerHale in Washington.

In the eyes of the FTC, an effective vendor oversight program is a key component of a company's reasonable and appropriate privacy or security program.[1] The FTC first signaled its expectations of vendor management in the data security context 10 years ago when it alleged in its complaint against Superior Mortgage Corp. that the respondent failed to oversee a third-party service provider responsible for hosting the company's website on a server outside of the company's internal network.[2] Although the respondent employed secure sockets layer (SSL) encryption for information transmitted from a visitor's Web browser to the external server whenever the company's website was accessed, that precaution was rendered moot when the service provider allegedly decrypted secure consumer information and forwarded it to the respondent's headquarters via e-mail in clear, readable text, resulting in a data breach. This failure to oversee a vendor's security practices was one of many findings alleged to have amounted to an unreasonable security practice by the respondent, but the FTC's message was unmistakable: the company was accountable for its vendors' practices.

Since 2005, the FTC has taken a number of opportunities to flesh out these expectations further in both the security and privacy contexts by alleging numerous ways in which a company could be said to have failed to exercise adequate vendor oversight. We address them in turn in the sections that follow.

Due Diligence Failure

As Jessica Rich, director of the FTC's Bureau of Consumer Protection, pointed out in a speech at the January AdExchanger conference, it is important to know with whom you are dealing and to make sure that they are an appropriate partner.[3] For example, in *FTC v. Si-*

[1] The FTC has relied on its power under Section 5 of the FTC Act to prohibit ''unfair or deceptive acts or practices in or affecting commerce'' for the majority of its data security enforcement actions. 15 U.S.C. § 45(a)(2). However, the FTC has also asserted violations of other laws in these data security actions, including the Gramm-Leach-Bliley Act, Fair Credit Reporting Act and Children's Online Privacy Protection Act.

[2] Complaint, *In re Superior Mortg. Corp.*, File No. 052-3136 (F.T.C. Dec. 14, 2005) (4 PVLR 1209, 10/3/05).

[3] Jessica Rich, Director, FTC Bureau of Consumer Protection, Beyond Cookies: Privacy Lessons for Online Advertising, Remarks Delivered at AdExchanger Industry Preview 2015 (Jan. 21, 2015), *available at* https://www.ftc.gov/system/files/

 ISSN 1538-3423

tesearch Corp. d/b/a LeapLab, **the FTC alleged that the respondent bought payday loan applications from data brokers and sold them to telemarketers.[4] Any amount of thoughtful due diligence, the commission suggested, would have revealed that consumers would likely be surprised by this, and avoiding consumer surprise is the touchstone of a good privacy program.[5]**

In 2014, the FTC put this principle into practice, in *In re Snapchat, Inc.*, wherein it ordered the company to establish, implement and maintain a ''privacy by design'' program, which included a requirement to develop and use ''reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order.''[6] This privacy by design template borrows heavily from the ''data security by design'' principle, thus signaling the FTC's expectation that companies perform reasonable due diligence on both their privacy and data security vendors prior to engagement of services.

Contractual Failure

In two of the earliest data-security-focused complaints, the FTC alleged that respondents' failure to require *by contract* that third-party service providers protect the security and confidentiality of personal information contributed to eventual data breaches. First, the FTC held Gregory Navone, a mortgage broker, liable for both his failure, and the failure of two service providers, to properly dispose of consumer data (the data were physically dumped into publicly accessible dumpsters).[7] Second, Goal Financial LLC suffered a data breach in 2008 when employees exploited security failures, one of which was ''fail[ing] in a number of instances to require third-party service providers by contract to protect the security and confidentiality of personal information,'' removed without authorization more than 7,000 consumer files containing sensitive information and transferred them to third parties.[8] In these instances, the FTC focus was on the failure to implement proper contractual terms governing the vendor's use of the data at issue.

Similarly, in *FTC v. GeneLink, Inc.*, the FTC held the respondent liable for inadequate vendor practices, even though a breach had not occurred.[9] GeneLink Inc. and its former subsidiary foru International Corp. marketed nutritional supplements and a skin care product that were purportedly customized to each customer's genetic profile, based on a DNA assessment performed on a cheek swab provided by the customer. In the complaint, the FTC alleged that GeneLink did not take reasonable and appropriate security measures to safeguard its customer personal information. GeneLink allegedly failed to require by contract that service providers implement and maintain appropriate data security safeguards and failed to provide reasonable oversight of service providers, by, for example, mandating implementation of simple, low-cost and readily available defenses to protect consumers' personal information. The FTC also alleged that GeneLink *failed to restrict by contract the personal information provided to service providers by business need*. As a result, every service provider was allegedly able to access the personal information of every GeneLink customer in the respondent's database, which included names, addresses, e-mail addresses, telephone numbers, dates of birth and Social Security numbers.

Monitoring Failure

In a 2012 data security complaint, the FTC made clear that it expected companies not only to contractually require third-party servicers to observe sound data security practices, but also to actually ensure these service providers properly implement these agreed-upon practices. Wyndham Worldwide Corp., a global operator and franchisor of hotels, suffered three computer hacking attacks that over a two-year period that allegedly compromised the information of over 619,000 consumer payment cards.[10] The FTC alleged that Wyndham's failure to ensure that the hotels and third-party service providers *implemented adequate information security policies and procedures* prior to connecting to Wyndham's global network contributed to the breaches. The FTC further alleged that this enabled hackers to gain unauthorized access to the hotel group's network through Wyndham-branded hotels' computers and through service providers' administrator accounts.

In two similarly reasoned complaints, the FTC alleged that respondents failed to adequately supervise and oversee service providers' security practices on an ongoing basis.[11] In both instances, it was allegedly the vendor's mistake or unsafe security practice that contributed to and enabled an eventual breach. However, it was the companies, and not the vendors, that were left with the liability. This monitoring principle was further elaborated in the case of *In re GMR Transcription Servs., Inc.*, wherein the FTC held the respondent liable for a vendor's inadequate security practice, even though the respondent was unaware of the unsafe

---

documents/public_statements/620061/150121beyondcookies.pdf.

[4] Complaint, *FTC v. Sitesearch Corp.*, No. 2:14-cv-02750-NVW (D. Ariz. Dec. 22, 2014), *available at* http://www.bloomberglaw.com/public/document/Federal_Trade_Commission_v_Sitesearch_Corporation_et_al_Docket_No (14 PVLR 23, 1/5/15).

[5] Office of the Attorney General of California, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (Jan. 2013) (discussing the importance of ''surprise minimization''), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf (12 PVLR 80, 1/14/13).

[6] Decision and Order, *In re Snapchat, Inc.*, Docket No. C-4501, at Section II.D (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf (14 PVLR 69, 1/12/15).

[7] Complaint, *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 29, 2008); *see also* Stipulated Final Order for Payment of Civil Penalties, Permanent Injunction, and Other Equitable Relief, *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 29, 2009) (9 PVLR 134, 1/25/10).

[8] Complaint, *In re Goal Fin., LLC*, File No. 072-3013 (F.T.C. Apr. 9, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2008/04/080415complaint_0.pdf; *see also* Decision and Order, *In re Goal Fin., LLC*, File No. 072-3013 (F.T.C. Apr. 9, 2008) (7 PVLR 581, 4/21/08).

[9] Complaint, *In re GeneLink, Inc.*, File No. 112-3095 (F.T.C. May 8, 2014); *see also* Decision and Order, *In re GeneLink, Inc.*, File No. 112-3095 (F.T.C. May 8, 2014) (13 PVLR 879, 5/19/14).

[10] Complaint, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. June 26, 2012) (11 PVLR 1069, 7/2/12).

[11] Complaint, *In re CBR Sys., Inc.*, File No. 112-3120 (F.T.C. May 3, 2013) (12 PVLR 195, 2/4/13); Complaint, *In re Credit Karma, Inc.*, File No. 132-3091 (F.T.C. Aug. 19, 2014) (13 PVLR 1500, 9/1/14).

  PVLR ISSN 1538-3423

third-party practice.[12] This case unequivocally announced that ignorance is no excuse in the eyes of the FTC.

The FTC has also used its settlement terms to force good vendor and affiliate oversight behavior from certain companies. For example, in 2007, DirectRevenue LLC, a large adware distributor, agreed to settle charges that it used unfair and deceptive methods to download adware onto consumers' computers and then obstruct them from removing it.[13] In addition to a number of other stipulations, the settlement requires that DirectRevenue monitor its affiliates to ensure that both the affiliates and their sub-affiliates comply with the FTC order.

In 2005, the FTC reached a settlement with GlobalNet, alleged to have sent millions of illegal e-mail messages.[14] This settlement also contained an affiliate monitoring requirement, requiring the defendants to collect certain information about an e-mail campaign, as well as identification information about the affiliates, before they can begin the campaign. Once the e-mails are sent, the defendants are required to sample new subscribers to their website to make sure the affiliates are complying with the settlement order when sending out marketing e-mails.

The allegations in these complaints cover the: failure to contractually require third-party service providers to protect the security and confidentiality of personal information; failure to monitor, supervise and assess vendor practices with regard to sensitive data; and failure to ensure that third parties maintain and adhere to adequate security policies and procedures. The facts giving rise to the claims varied from case to case, but, in each, vendor practices found to be unreasonable in the eyes of the FTC contributed to a security or privacy breach or a potential breach of the same for which the company was held responsible.

Secondary Liability: Not a New Horizon

As noted above, this principle of holding companies liable for the practices of their business partners should not be viewed as a departure from or a radical development in FTC enforcement trends. Indeed, the FTC has been applying this principle of holding companies liable for the practices of affiliates and entities with whom they contract in a wide variety of contexts. Key examples of areas where the FTC has applied this theory of liability include telemarketing and advertising.

The FTC has articulated clear expectations for companies engaging in telemarketing: due diligence is a must. As Rich has stated: ''Companies that use lead generators must exercise due diligence when they buy lists of phone numbers or else they can be on the hook for illegal telemarketing.''[15] In a 2014 case, the FTC alleged that Versatile Marketing Solutions Inc. (VMS) called millions of consumers whose names and phone numbers VMS bought from lead generators.[16] The lead generators asserted that these consumers had given VMS permission to contact them about the installation of a free home security system, but in fact, they had not. The FTC held VMS liable for not exercising adequate due diligence on the lead generators, which would have uncovered that the majority of the consumers were on the National Do Not Call Registry, and that the lead generator's statements to the contrary were false.

The FTC has also held companies liable for their business partners' marketing practices. ''Whether they advertise directly or through affiliates, companies have an obligation to ensure that the advertising for their products is not deceptive,'' said David Vladeck, former director of the FTC's Bureau of Consumer Protection.[17] Through public statements like this and a number of enforcement actions, the FTC has made it clear that companies are liable for their affiliates' and third-party servicers' marketing practices.

In *In re Coleadium, Inc.*, the FTC alleged that the respondent's affiliate marketers made deceptive claims on fake news sites to promote acai berry supplements, and so-called ''colon cleansers,'' as weight-loss products.[18] In addition to misleading consumers about the effectiveness of the supposed weight-loss products, these marketers recruited by the defendants allegedly also promoted ''free trials'' of the products, a ''service'' for which consumers were billed monthly. Coleadium was held liable for the marketing practices of its affiliates, and under the agreed-upon settlement, the defendants will be required to monitor affiliate marketers in their network to ensure that their statements are truthful and in compliance with federal advertising law.

Likewise, in *In re Legacy Learning Sys., Inc.*, the FTC alleged that the respondent deceptively advertised its products through online affiliate marketers who falsely posed as ordinary consumers or independent reviewers.[19] Under the proposed administrative settlement, in addition to paying a fine, Legacy Learning will be required to monitor and submit monthly reports about their top 50 revenue-generating affiliate marketers, and to ensure that these marketers are disclosing that they earn commissions for sales and are not misrepresenting themselves as independent users or ordinary consum-

[12] Complaint, *In re GMR Transcription Servs., Inc.*, File No. 122-3095 (F.T.C. Aug. 14, 2014) (The FTC alleged that the respondent failed to adequately verify that their service provider implemented reasonable and appropriate security measures to protect personal information in files on the service provider's network and computers; did not take adequate measures to monitor and assess whether the service provider employed measures to protect personal information; and did not request or review relevant information about the service provider's security practice.) (13 PVLR 1500, 9/1/14).

[13] Decision and Order, *In re Direct Revenue, LLC*, File No. 052-3131 (F.T.C. June 26, 2007) (6 PVLR 312, 2/26/07).

[14] Stipulated Order for Permanent Injunction and Monetary Judgment, *FTC v. Global Net Solutions, Inc.*, No. CV-S-05-0002-PMP-LRL (D. Nev. Aug. 4, 2005) (4 PVLR 1433, 11/21/05).

[15] Press Release, FTC, FTC Reaches Settlement With Home Security Company That Called Millions of Consumers on the National Do Not Call Registry (Mar. 12, 2014), *available at* https://www.ftc.gov/news-events/press-releases/2014/03/ftc-reaches-settlement-home-security-company-called-millions.

[16] Complaint, *United States v. Versatile Mktg. Solutions, Inc.*, No. 1:14-cv-10612-PBS (D. Mass. Mar. 10, 2014) (13 PVLR 455, 3/17/14).

[17] Press Release, FTC Firm to Pay FTC $250,000 to Settle Charges That It Used Misleading Online ''Consumer'' and ''Independent'' Reviews (Mar. 15, 2011), *available at* https://www.ftc.gov/news-events/press-releases/2011/03/firm-pay-ftc-250000-settle-charges-it-used-misleading-online.

[18] Complaint, *In re Coleadium, Inc.*, File No. 102-3239 (F.T.C. Aug. 30, 2012).

[19] Complaint, *In re Legacy Learning Sys., Inc.*, File No. 102-3055 (F.T.C. June 1, 2011).

ers.[20] Legacy Learning must also monitor a random sampling of another 50 of its affiliate marketers and submit monthly reports to the FTC about the same criteria.

Vendor and Business Partner Oversight: Lessons Learned

Through its enforcement actions, the FTC has laid out a framework for an effective vendor relationship. First, it is important to consider your vendor's privacy and data security at the beginning of the vendor relationship. Indeed, companies should add to their vendor due diligence routines a review of vendor privacy and cybersecurity policies and procedures. In the cybersecurity context, this review should confirm not only that the vendor in fact *has* data security policies in place, but also that these practices reasonably protect potentially sensitive data. In the privacy context, the review should determine how and where the data were originally collected and what representations (direct or implied) were made regarding how the data would be used and disseminated.

Next, contract terms matter: service-level agreements should require that vendors adhere to certain practices designed to safeguard sensitive information and to maintain the privacy of consumers' information in accordance with any representations made when it was collected. Companies should also, of course, require by contract that vendors use the data they receive only for purposes specified by the principal, and that they securely dispose of the information when it is no longer needed for those purposes.

But a company's oversight responsibilities do not end once the contracts are signed. Rather, once the vendor or business partner has been brought on board, the company must continue to oversee and supervise its vendor or business partner on a reasonable and appropriate basis by regularly monitoring and assessing whether the vendor or business partner is adhering to the agreed-upon practices. In the data security context, mandated practices must also be continually reviewed and updated in light of the shifting and evolving threats of the digital age to ensure the vendor is keeping current with reasonable security upgrades.

As the number of enforcement cases brought against companies for privacy and data security violations continues to increase, failing to meet the FTC's expectations for vendor oversight will only become more indefensible. Keeping these simple principles in mind: due diligence, effective contract provisions and ongoing monitoring will greatly reduce the likelihood of investigations or enforcement actions stemming from the activities of vendors and business partners.

---

[20] Decision and Order, *In re Legacy Learning Sys., Inc.*, File No. 102-3055 (F.T.C. June 1, 2011).

  PVLR ISSN 1538-3423