ALERTS | 09.14.2023

FTC Finalizes Order with Genetic Testing Company 1Health.io in Privacy and Security of Genetic Information Case

The FTC recently finalized an order with genetic testing company 1Health.io ("1Health" or "Vitagene"), settling claims that 1Health (1) failed to secure sensitive genetic and health data and misrepresented the adequacy of its storage and security practices, (2) deceived customers about the ability to have their data deleted, (3) failed to ensure DNA samples were destroyed, and (4) changed its privacy policy retroactively without adequately notifying and obtaining consent from consumers whose data had already been collected.

Among other things, the order:

- Imposes a $75,000 fine, which the FTC reports it plans to use for consumer refunds.
- Prohibits 1Health from disclosing health information to any third party without first receiving affirmative express consent from consumers.
- Requires 1Health to instruct any laboratories that collected physical DNA samples pursuant to a contract with 1Health to destroy any sample the laboratory has retained for more than 180 days.
- Mandates that 1Health notify the FTC within 10 days of discovery of unauthorized disclosures of consumers' individually identifiable health information.
- Requires iHealth to establish and maintain an information security program that addresses the security failures highlighted by the complaint, including by obtaining independent third-party information security assessments.

1Health operates under the trade name Vitagene and sells DNA health test kits to consumers. 1Health then uses customers' genetic data and information collected via health and lifestyle questionnaires to provide personalized reports about health, wellness, and ancestry. 1Health also sells products it claims to be customized to consumers' DNA results, including nutrition, fitness, beauty plans, and nutritional supplements.

The FTC's complaint alleges 1Health failed to live up to claims prominently featured in multiple sections of its website and advertising collateral about the strength of its privacy and security practices, including claims that DNA would be stored separately from other identifying information and claims that customers were free to delete their information from 1Health's servers at any time. The complaint also alleges that, despite stating on its website that it would destroy all DNA samples after they had been analyzed, 1Health lacked measures to ensure those samples were in fact destroyed. Furthermore, the complaint asserts that in 2020, 1Health updated its privacy policy to significantly expand the ways in which it may share consumers' personal information (including information belonging to consumers who purchased products and services before the updated policy went into place) and failed to specifically notify consumers of or obtain their specific consent for the changes.

As a result of these allegedly deceptive practices, according to the FTC, consumers' sensitive genetic and individually identifiable health data were put at risk of public disclosure. The complaint states that 1Health uses Amazon Web Services' Simple Storage Service (the "Amazon S3 Datastore") in order to store and retrieve data. The complaint alleges that, despite receiving at least three warnings over a two-year period, individually identifiable unencrypted health reports and raw genetic data were available to the

public, 1Health failed to implement any access controls on these data, resulting in public exposure of the health and genetic information of more than 2,600 consumers. 1Health notified consumers about this breach in 2019, but because 1Health did not log or monitor access to the data, or maintain a data inventory, it could not determine exactly when or how the data had been accessed and could not comply with consumers' requests that 1Health delete their data.

This is the FTC's first enforcement action focused on both the privacy and security of genetic information. This enforcement action highlights the FTC's continued focus on protecting consumers' genetic and biometric information. In May, the FTC issued a policy statement noting that "the increasing use of consumers' biometric information and related marketing of technologies that use or purport to use biometric information ('biometric information technologies') raise significant concerns with respect to consumer privacy, data security, and the potential for bias and discrimination." With a focus on the increasing use of facial recognition technology and the risk that biometric information can be used to create counterfeit videos or voice recordings (known as "deepfakes"), the policy statement laid out a non-exhaustive list of examples of practices that the FTC will scrutinize in determining whether companies are complying with Section 5 of the FTC Act. These practices include:

- False or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information.
- Deceptive statements about the collection and use of biometric information.
- Failing to assess foreseeable harms to consumers before collecting biometric information.
- Failing to promptly address known or foreseeable risks of particular biometric information technologies.
- Engaging in surreptitious and unexpected collection or use of biometric information.
- Failing to evaluate the practices and capabilities of third parties.
- Failing to provide appropriate trainings for employees and contractors.
- Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale, or uses in connection with biometric information.

The FTC's 1Health order highlights an ongoing trend of active enforcement related to the privacy and security of health information, especially sensitive health information. This order also highlights the fact that the FTC's enforcement authority goes beyond traditional healthcare providers and includes a focus on consumer-facing apps and websites.

Printable version.

Christine G. Savage
Co-Chair, Government Enforcement & Compliance

Sara K. Frank
Principal