Published on *The National Law Review* https://natlawreview.com

FTC Decision with Global Tel*Link Signals Expectations for Use of Testing Environments

Article By:

Liisa M. Thomas

Wynter L. Deagle

Dane C. Brody Chanove

The FTC recently announced a settlement with Global Tel*Link, a telecommunications company that contracts with prisons and jails to provide communication services to incarcerated individuals and their families. Those who use their services create accounts with the company and are required to provide not only usernames and passwords but also Social Security numbers and government ID numbers. The company also collects financial account information as well as names and addresses. The company included in its marketing materials promises about security, including that it was the "cornerstone of what we do." The company also made promises about its security in RFPs to prisons and jails.

An August 2020 data breach, according to the FTC, exposed the personal information users' had submitted. This included information of both incarcerated individuals as well as that of their family members. The breach, the FTC alleged, resulted from the company's failure to take appropriate safeguards during a software upgrade. Namely, during the upgrade, the company copied users'

personal information from its regular work environment into a test environment that did not include encryption, automated monitoring, a perimeter firewall, or log monitoring. All things that existed in its regular working environment.

The alleged lack of security existed for three days, and during that time almost 650,000 users' information was in the test environment. And, according to the FTC, the company's forensic investigation showed both access to the test environment as well as data exfiltration during that three day window. The company also, the FTC indicated, received consumer complaints saying their information had been misused. However the company made statements to the press that "no medical data, passwords or consumer payment information" was impacted.

The company did notify a subset of individuals (45,000), but as of the date of the settlement, had not notified the remainder of people whose information was in the test environment.

As part of the settlement, GTL has agreed to both implement things that are standard for an FTC settlement (put in place a security program, have the program assessed by a third party) as well as some that are less usual. These include steps that can signal what the FTC might view as "appropriate" security measures, such as:

- Implementing specific security measures that would impact security of test environments. These include security practices for in-house developed applications and having procedures in place to protect personal information when changes to systems to networks occur that might affect risk. (On this latter point the settlement provides for very specific requirements, rather than more general "appropriate measures" that it has called for in past settlements.)

- Not only ensuring that those who were impacted by this incident receive notice (and credit monitoring), but also if the company suffers a breach in the future it has agreed to provide notice within 30 days to impacted individuals and the relevant prisons and/or jails. While these requirements may mirror what exists under state breach notification laws, the company has also agreed to notify the FTC in such cases as well.
- Providing the board (or equivalent) a written report of compliance with its security program at least annually, and within 30 days after on breach that requires notice under breach notification laws. Related to this is assessing compliance with the program annually.
- Having all employees take security awareness training annually. InfoSec personnel are also required to take additional training "sufficient to address relevant security risks." The settlement also calls for developers and engineers to receive appropriate training.

Putting It into Practice: The detailed requirements imposed in this settlement not only combine state law requirements around breach notification and data security, but go beyond them as well. Reviewing the details can be helpful in understanding what the FTC expects of companies, not only in normal environments, but others -like test environments- where sensitive data may be housed.

National Law Review, Volumess XIII, Number 333