Advisory

JANUARY 2013

If you have any questions about this Advisory, please contact:

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

Lost Backup Tape Puts Blood Bank Under the FTC's Microscope

In an all-too familiar fact pattern, a San Francisco-based employee of a California-based cord blood bank put four company back-up tapes -- filled with personal data on 300,000 pregnant mothers, expectant fathers and newborns -- into a backpack and then set out by car to deliver the tapes to the company headquarters in San Bruno, 13 miles away. The backpack also contained a company laptop, an external hard drive and a USB drive; these devices contained network information including user passwords and access protocols. Somewhere along the way, the employee's car was broken into by an intruder, and the tapes and hardware devices –all unencrypted--were stolen. Once again, a simple business errand gone awry led a company on a trip to the Federal Trade Commission ("FTC").

THE PERSONAL DATA SPILL

The settlement with CBR Systems, Inc. ("CBR") this week [1] follows the established pattern of FTC enforcement actions targeting inadequate data security practices. CBR routinely collects personal data from expectant families, who permit CBR to store umbilical cord blood and tissue for possible medical use. Data typically collected includes name, address, Social Security number, driver's license number, credit card numbers, medical history profile, blood type and infectious disease marker results – a trove of information of the kind that can facilitate identity theft and expose sensitive medical data. The lost tapes included all these kinds of data but were unencrypted and therefore technically accessible to an unauthorized person with the means to access the tapes. There is no mention in the FTC settlement documents of any actual or suspected misuse of the personal data on the CBR tapes.

LOSS OF UNENCRYPTED NETWORK PASSWORDS

The FTC's concern over the loss of the laptop and other storage devices was not limited to the unencrypted consumer data. It also focused on the loss of unencrypted passwords and other network access information for CBR's systems and its website (where the company also maintains a "Gift Registry" to cover CBR's costs in collecting and storing a pregnant woman's umbilical cord blood and collects data on donors). Loss of this system access data effectively handed over the keys to CBR's information assets to anyone with the wherewithal to exploit the data. Again, the FTC documents do not indicate whether CBR actually experienced any hacks of its systems following the loss of the devices.

THE FTC'S INVESTIGATION OF CBR'S DATA SECURITY PRACTICES

The loss of the tapes and the storage devices in late 2010 was just the beginning of the FTC's issues with CBR. Once an inquiry of this kind commences, the FTC takes a long, hard look under the hood of a company's data security policies and practices. As the consent decree suggests, CBR's shortfall in data security measures was not confined to transporting unencrypted tapes in an employee's car

CONTINUED ON NEXT PAGE

Lost Backup Tape Puts Blood Bank Under the FTC's Microscope CONTINUED

through a rough neighborhood. The ensuing investigation brought to light a number of other data security practices that the FTC has repeatedly found fault within prior actions. In the case of CBR, these practices were alleged to include:

- Not adequately supervising an outside service provider that managed a legacy CBR database containing personal information in a "vulnerable format" on its network;
- Failing to take reasonable steps to render any personal information on the lost tapes and devices "unusable, unreadable, or indecipherable" to anyone gaining unauthorized access;
- Failing to implement adequate controls in CBR's databases to limit access to personal information to only those personnel with a "need to know";
- Failing to destroy consumers' personal information after it was no longer needed for business purposes; and
- Failing to deploy "sufficient measures" to protect against unauthorized access to the company's computer networks, such as (i) monitoring traffic on the company's web site, (ii) confirming that anti-virus software was distributed, (iii) using an automated network intrusion detection system and (iv) retaining system logs and systematically reviewing these logs for threats.

Finally, in light of the above alleged security deficiencies, the FTC complaint also charged that CBR had misled consumers, singling out the following statement in CBR's privacy policies:

". . . CBR takes steps to ensure that your information is treated securely and in accordance with the relevant Terms of Service and this Privacy Policy. . . . Once we receive your transmission, we make our best effort to ensure its security on our systems."

It was this "deceptive practice" on which the FTC based its authority under Section 5(a) of the FTC Act.[2]

TERMS OF THE CONSENT ORDER

The draft consent order imposes the standard litany of remedies for businesses that allegedly fail to maintain "reasonable and adequate" information security measures. The terms include (i) a prohibition on misrepresentations about the security of customer data, (ii) a requirement to establish a comprehensive information security program consistent with the FTC Safeguards Rule[3], (ii) biennial third party compliance audits of this security program for the next twenty years and (iv) various reporting and compliance requirements, including notification of any change in corporate status (e.g., a sale or merger). As is also customary in these settlements, the draft order stipulates that CBR does not admit any violation of law or the truth of the factual allegations in the FTC's complaint.

IMPLICATIONS OF THE CBR MATTER

CBR's new twenty-year relationship with the FTC, and the attendant costs of being under the FTC's microscope, might have been avoided had the company deployed certain basic measures, such as having a written information security program containing industry standard terms consistent with the Safeguards Rule and a practice of encrypting personal information on storage tapes before they leave company premises (something that the 2010 Massachusetts data security regulation specifically mandates[4] and the FTC now seems to expect). Without such measures, companies that make even bland and innocuous statements about their data security practices –such as the assurances cited by the FTC in CBR's policies – may be setting themselves up for extra trouble on that day when the messenger calls with a shaky voice to say that her car has been broken into and the tapes are gone.

[1] http://ftc.gov/oscaselist/1123120/130128cbragree.pdf . The settlement, announced on January 28, 2013, is not final pending a public comment period that ends on February 28th.

[2] 15 U.S.C. 45(a)

[3] 16 C.F.R. Part 314; http://www.ftc.gov/os/2002/05/67fr36585.pdf

[4] 201 C.M.R. 17.00; http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf