FUNKHOUSER VEGOSEN LIEBMAN & DUNN LTD.

Legal Update

May 2011

FTC: Digital Copiers Pose Data Security Risks

By Seth A. Stern

Today's technologically inclined businesses may believe that the last thing they have to worry about in terms of data privacy compliance is their copy machines. The Federal Trade Commission (FTC), though, is reminding companies that digital copiers – which preserve electronic records of documents they scan, copy, and fax – can land them in as much trouble as social media sites, P2P sharing, or unsecured networks.

Like computers, digital copiers have hard drives that may store information from copied documents, including customers' and employees' social security numbers, health data, account numbers, trade secrets and financial data. If not protected, this information can fall into the hands of anyone from spam e-mailers to identity thieves, especially when leased copiers are returned. This can lead to liability under the FTC Act and similar state laws, as well as numerous state and federal computer privacy statutes. Healthcare providers and financial institutions may also face liability for leaked data under the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act, respectively. Consumer reporting records must be disposed of in accordance with the Fair and Accurate Credit Transactions Act and the Fair Credit Reporting Act and related rules and regulations.

Affinity Health Plan, a New York non-profit managed healthcare plan, learned about the data privacy risks posed by copiers the hard way last year when CBS News revealed that a copier previously owned by Affinity allegedly contained numerous individuals' medical and other personal records. Affinity had to notify over 400,000 customers that their personal information may have been at risk due to the breach pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Recommendations

The FTC recently issued Guidelines intended to help businesses prevent mishaps like the Affinity incident. Among the FTC's recommendations are for businesses to:

- Include digital copiers in their information security policies.
- Explore security options including encryption (or scrambling) of data.
- Securely overwrite a data digital copier's hard drive at least once a month.
- Consider implementing password protection of data stored on copiers.
- Ensure that copiers connected to networks are securely integrated.

FVLD®

- Ensure that they contract to either keep hard drives at the end of any copier lease or require the company providing the copier to scrub the hard drive.
- Place a warning sticker on the copier to inform users of data security risks and procedures.

Companies should also ensure that any assurances they make regarding the privacy of data they store are accurate to avoid further liability for misrepresentations under the FTC Act and other statutes.

Companies unsure of their data privacy obligations in regard to data stored on copiers as well as that stored on computers should consult with counsel.

FVLD publishes updates on legal issues and summaries of legal topics for its clients and friends. They are merely informational and do not constitute legal advice. We welcome comments or questions. If we can be of assistance, please call or write Jon Vegosen 312.701.6860 jvegosen@fvldlaw.com, Glenn Rice, 312.701.6895 grice@fvldlaw.com, Seth A. Stern 312.701.6837 sstern@fvldlaw.com, or your regular FVLD contact.

FVLD®