

Stop Faxing



David Smyth

May 11, 2016

Topics: [Data Security](#)

I've long thought that sending faxes was a pretty silly means of communication. Don't send me a fax. I don't want it. At some point I'm hoping that even my kids' doctor's office will get dragged into the 20th century and drop their insistence on faxing. In the meantime a pdf will be fine, thanks. In addition to the many reasons faxes are antiquated and annoying, the SEC has just provided us another reason to avoid them: they encourage violations of Reg. S-P!

The Rule

Reg. S-P's Safeguards Rule requires that every broker-dealer registered with the SEC adopt policies and procedures reasonably designed to:

1. insure the security and confidentiality of customer records and information;
2. protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
3. protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The Allegations

Craig Scott Capital, LLC, a broker-dealer in Uniondale, New York, had written supervisory procedures that purported to describe the manner in which the firm complied with the Safeguards Rule. But those procedures allegedly had some problems. For example, the procedures said the "Designated Supervisor" was responsible for ensuring compliance, but did not identify the Designated Supervisor. Also, the procedures allegedly contained blanks to be filled in later, such as: "[The Firm] has adopted procedures to protect customer information, including the following: [methods]."

But let's get to the faxes. As last month's [administrative order](#) sanctioning Craig Scott Capital says:

From January 20, 2012 until approximately June 2014 (the "Relevant Period"), CSC used email addresses other than those with the Firm's domain name--@craigscottcapital.com – to electronically receive more than 4,000 faxes from customers and other third parties. These faxes routinely included sensitive customer records and information, such as

BLOG ARCHIVE

TOPICS

About This Blog
 About Us
 Access to Court Dockets
 Access to Courtrooms
 Access to Search Warrants
 Anti
 Anti-SLAPP Statutes
 Contact
 Cyberattack
 Data Breach
 Data Security
 Defamation
 Digital Media and Data Privacy
 Law
 Disclaimer
 Drone Law
 Fair Report Privilege
 FCC Matters
 First Amendment
 First Amendment Retaliation
 FOIA
 HIPAA
 Indecency
 Internet
 Intrusion
 Miscellaneous
 Mobile Privacy
 Newsroom Search Warrants
 Newsroom Subpoenas
 Political Advertising
 Prior Restraints
 Privacy
 Privacy Policies
 Privacy Policy
 Public Records

customer names, addresses, social security numbers, bank and brokerage account numbers, copies of driver's licenses and passports, and other customer financial information. During the Relevant Period, Taddonio and Porges, CSC's principals, as well as other CSC employees and registered representatives, also used their personal (i.e., non-Firm) email addresses for matters relating to the business of CSC. CSC did not maintain and preserve either these faxes or this email correspondence as required by Section 17(a) of the Exchange Act and Rule 17a-4 thereunder.

The problem was the same as with all faxes: nobody wants them. They want emails instead. So when the firm set up an electronic faxing service, they added an extra step in the communication chain, and routed the faxes to email addresses. While they should have sent those faxes to email addresses with the firm's domain name, thousands went to personal email addresses instead. Those personal email addresses were outside the firm's communication management system, and the data in the faxes was unprotected.

The violations of Reg. S-P and Rule 17a-4 have cost Craig Scott Capital a \$100,000 penalty and left the firms' principals subject to cease-and-desist orders.

A Three-Step Data Security Plan^[1] for Your Business

1. Have a good reason for the communication methods your firm uses. Do you have a plan for your faxes? Can you protect the integrity of the data they contain? If not, quit it with the faxes.
2. Keep your business in front, and party in the back. Are you using personal emails for your business? Can you protect the integrity of the data they contain? If not, quit it with the personal emails and save them for your fantasy jai alai league. They are a terrible idea.
3. Re-read your data security procedures. Do they have actual blank spaces that will leave you exposed later? Fill those, and then look for your other problems, which you surely have.

Reporters Privilege
Services
Shield Laws
Wiretapping

LINKS

International Association of Privacy Professionals
National Association of Broadcasters
North Carolina Cable
Telecommunications Association
North Carolina Press Association
North Carolina Association of Broadcasters
Radio-Television News Directors Association of the Carolinas
Media Law Resource Center
The Reporters Committee for Freedom of the Press
Society of Professional Journalists
The Journalist's Toolbox - American Press Institute
Law Blog - WSJ.com
Legal Blog Watch
North Carolina Business Litigation Report

^[1] This is an incomplete plan. You need way more than this plan.