FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Buying or selling debts? Steps for keeping data secure

For savvy companies, keeping data secure is a day-to-day part of their business. They reduce the amount of sensitive information they collect in the first place, keep it secure if there's a legitimate business need to maintain it, and dispose of it safely when they no longer need it.

If you're in the business of buying or selling debts, many of the documents in your files or on your network contain confidential information that shouldn't be made publicly available. It's your obligation to take reasonable steps to keep sensitive information secure.

Why should appropriate security practices be important to your industry? First, consider what's at stake for consumers. Information of this nature is particularly sensitive because the public disclosure of debts can result in job loss and family turmoil – and that's just for starters. It also raises the risk of identity theft and financial fraud, including exploitation by phantom debt collectors, scammers who try to collect on debts they don't have authority to collect.

What's more, slipshod security practices can spell trouble industry-wide. When a portfolio is compromised, it makes collection more difficult for the true owner of the debt. That, in turn, reduces the value of the portfolio for sale. Given how fraudsters like phantom debt collectors erode confidence in the entire process, legitimate industry members have a financial stake in adopting and encouraging reasonable security practices.

The Federal Trade Commission (FTC) has common-sense suggestions for debt buyers and sellers to help reduce the risk of unauthorized disclosure.

Don't disclose data publicly

The data in your possession – account numbers, Social Security numbers, information about debt amounts, creditors, charge-offs, etc. – is the financial equivalent of plutonium. Powerful when used with proper safeguards in place, but hazardous in the wrong hands. That's why there is simply no legitimate business reason for publicly posting your portfolios or making consumer information publicly available in any other way. You can advertise by mentioning specific categories of information you have, but don't disclose the individual's information. Period.

Store your portfolios securely

Keep paper copies in a locked room or in a secure cabinet. Limit employee access on a need-to-know basis. Electronic data needs fortification, too. Consider keeping portfolios in password-protected files and make sure all devices with access to the information have reasonable security measures in place – updated antivirus software, firewalls, and the like.

Minimize the amount of consumer information you share with prospective buyers

Potential buyers may need access to some of the sensitive data in a portfolio to evaluate whether they want to buy it, but keep it to a minimum. Provide only the data the prospective buyer needs and explain why sound security is in their best interest, too. Furthermore, don't sell sensitive information to just anyone. Make sure they are who they say they are, and contractually require them to maintain reasonable safeguards.

Transfer data securely

When transferring data to a potential or final buyer, keep it secure. For example, encrypt the file or password-protect the portfolio. If you're sending the file via email, don't include the password in the same message.

Dispose of data safely

When you no longer need sensitive consumer information, get rid of it securely, using strategies to thwart dumpster divers and hackers. Don't just throw away hard copies. Burn, pulverize, or shred them. For electronic files, just clicking the delete button may not be enough. Take advantage of free and low-cost tools that will reduce the risk that a computer criminal can recreate a deleted file.

Have a plan in place in case there's a breach

Whether it's a misplaced file, a lost laptop, or a hack attack, the worst time to start thinking about a data breach is after you've experienced one. One key step in a compliance check-up is to put together an up-to- date file of "just in case" resources. For example, if there's a breach, how will you contact affected consumers, businesses, and law enforcement? Most states have data breach laws with specific requirements. Be sure to consult all relevant laws.

Take advantage of free resources from the FTC

Evaluating your company's practices doesn't have to be a start-from-scratch process. The FTC has a to-the-point publication, *Protecting Personal Information: A Guide for Business*, with practical tips on securing sensitive data. Watch a 20-minute online tutorial that outlines the basics. *Information Compromise and the Risk of Identity Theft* includes steps to consider if you've experienced a data breach.

Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to sba.gov/ombudsman.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace and to provide information to businesses to help them comply with the law. For free information, visit the Business Center, business.ftc.gov.