

Identity **THEFT** in the rent-to-own world

These days, businesses are being held more accountable for the records they keep and the safeguards they use to protect them. Should your customers' personal and financial information fall into the hands of thieves, you might be liable for the damages caused.

By Ed Winn III

Rarely a day goes by without news headlines declaring the loss of private, sensitive financial information from consumer files by the thousands, or even millions. Laptops get lost or stolen; CDs go missing; sensitive paper files are tossed into dumpsters behind stores. Retail giants such as Radio Shack, CVS Pharmacy, TJ Maxx, Marshall's and EZ Pawn have all suffered such losses.¹ If no rent-to-own store has yet made the news, it's probably only a matter of time. The reason for the headlines is the fear that the loss of this information will give rise to identity theft, one of the fastest growing, most pernicious crimes in the country. Rent-to-own stores do, after all, regularly collect the kind of financial information from current and future customers that can give rise to identity theft.

Of course, if thieves were logical, they would steal the identities of people with impressive credit, since the whole idea behind identity theft is to pretend to be someone else in order to buy things using that person's name and good credit, empty that person's bank accounts and otherwise profit from that person's station in life. If you are going to steal someone's identity, you want to steal an identity that has assets and credit from which to profit.



But the law does not draw a distinction between stealing the identity from a rich man or from a poor man. The Texas attorney general recently filed a suit against CNG Finance Corp. and its subsidiary, EZ Pawn, for violations of the *Texas Identity Theft Enforcement and Protection Act* (2005), which provides penalties of up to \$50,000 per violation. The attorney general also cited CNG for violations of another Texas statute concerning the businesses' retention and disposal procedures for customer information; it provides a \$500 penalty for each abandoned record. The allegation in the lawsuit is that the company failed to safeguard the private financial information of its customers when it threw boxes of customer files into dumpsters behind several stores.

One might suppose that the pawn shop customers were credit constrained, but that detail did not trouble the attorney general, nor is that distinction acknowledged in any of the laws that the attorney general is seeking to enforce. Nor is there any evidence that any thieves went dumpster diving behind the pawn shops. There need not be any such evidence. No records need actually to be stolen and used for liability to attach to a business that fails to destroy its records properly. It is the mere failure to dispose of customer records in accordance with the law that gives rise to liability—regardless of any identities actually been stolen.

There is an assortment of statutes and regulations that affect how businesses must deal with the personal and financial information that they have on consumers. The *Fair and Accurate Credit Transactions Act* (2003), or FACTA, is the federal government's response to the identity theft problem. FACTA is a multi-faceted statute that amends the *Consumer Reporting Act* and regulates consumer reporting agencies—Equifax, TransUnion and Experian—and the

companies that do business with them. FACTA rules provide that credit card receipts can display no more than the last five digits of a card number. The statute also gives consumers enhanced rights regarding their access to information in their credit reports and what they can do if they become—or fear that they *might* become—victims of identity theft.

Recent rules promulgated by the Federal Trade Commission under the authority of FACTA concern the disposal of consumer information by certain businesses.² The rule applies to companies that get information directly from, or derived from, consumer

new rules from the FTC regulate how customer files must be destroyed or deleted.

Once again, few RTO companies are covered by these rules because the information they are collecting is coming directly from consumers themselves and not from consumer reporting agencies. However, as a practical matter, there are state statutes already in place or pending that will cover any businesses exempt under FACTA, such as rent-to-own companies. The state statutes cover private financial information, however derived. Therefore, rental dealers are going to have to take steps to safeguard the information

No records need actually to be stolen and used for liability to attach to a business that fails to destroy its records properly. It is the mere failure to dispose of customer records in accordance with the law that gives rise to liability.



credit reports. Rent-to-own companies do not generally run credit reports on customer applicants and so the specifics of the new FTC rule do not apply to them. However, dealers who use Teletrack or other subprime reporting services may be covered by the rule. Chris Kelleher, writing about FACTA for Entrepreneur.com³ suggests that if you are not sure whether you are covered by the FACTA rules for safeguarding consumer financial data, be on the safe side and assume that you are.

FACTA rules generally require businesses to design and implement “reasonable” plans to safeguard consumer information. The plan need not be foolproof and companies can implement plans commensurate with the risk. Some companies deal with more consumer information and must have more comprehensive plans in place. The plans must identify “material internal and external” risks to security and then control for those risks. The plan must have contingencies in place if a breach occurs—notice to affected consumers and the like. Relatively

they collect on their customers or suffer painful, perhaps catastrophic, consequences under these state statutes; the Texas attorney general is using state law to go after the pawn shops. The statutes vary from state to state, but generally require proper destruction of consumer records and impose notice requirements if the company becomes aware of a breach in consumer information security.

So, what should rent-to-own companies do?

① Think about the information that you are collecting from your customers. How important is a customer's Social Security number to the success of your business? This is an important question to answer because a Social Security number is a keystone to identity and, therefore, identity theft. This number is carved out for separate treatment in a number of state statutes. See, for example, the Texas Business & Commerce Code, section 501.001: “Confidentiality of Social Security Numbers;” or California Civil Code, section 1789-85-89.

There is a certain amount of information you need from a customer in order to be able to rent and collect successfully. You need the customer's name, address, telephone number and work information. You need references and his or her contact information. You may not need the customer's bank account number unless you are setting up a direct-debit account with that customer. Copying a driver's license number is probably a good idea. If you have not reviewed your rental application/order form in this century, now is a good time to review it, line by line.

② Review your current policies and procedures concerning customer information. This will require more than pulling out the manual. You will need to talk to employees and get the truth about what is really happening in the store(s). Who has access to customer files? When can the hard copies of those files leave the store? Who is in charge of checking those files in and out of the system? What are the rules about credit/debit card numbers? Do your delivery or collection colleagues have their own notebooks with customer information, including credit/debit card numbers in them? You need a frank assessment of where sensitive customer information is located in the company in order to begin to corral it.

③ Review any applicable state laws concerning how you have to treat customer information. The National Conference of State Legislatures' Web site is a good place to start.⁴ Then contact your local chamber of commerce and Better Business Bureau for more information.

④ Develop and implement a written plan to safeguard customer information. There are currently more than 2,000 companies offering identity theft prevention services, document destruction services and consulting services, and they all have written plans for retail companies. Any good plan will have one person in charge of the program, limit access to customer information to those who need it, have employee management and training

provisions, encourage regular audits, demand accountability for adherence to the plan all the way up to the governing board of the company, have sign-offs for employees to acknowledge understanding of and commitment to the plan, have systems for detecting and managing breaches of customer security, have implementation of an information security control framework that is tested and enhanced continuously and have rules for the proper destruction of customer information.

There are useful outlines for plans that are available online from the Federal Trade Commission and/or the California Office of Information Security & Privacy Protection.⁵

⑤ Review existing customer information eligible for destruction. Shred with a cross hatch shredder, hammer into pieces or erase, as appropriate.

⑥ Create a plan that will keep pace with the rules in this rapidly developing area of the law.

The federal government and state legislatures have all gotten very serious about the crime of identity theft. They are pursuing identity thieves with a vengeance. They are also making it possible for private citizens, together as a class, to pursue businesses that fail to do everything possible to safeguard private consumer information that falls into the wrong hands. As sure as I am penning this article, sadly, we will all live to read about a rent-to-own company brought low, not because it charged customers too much, used a bad rental agreement or abused collection practices, but because private customer information leaked out of a store and hundreds or thousands of customers got together and used these new identity theft laws to sue the company out of existence. Make sure that lawsuit does not have your company's name on it. *

Ed Winn III is APRO's general counsel. His e-mail address is edwinn@muvmlaw.com.

LINKS to more INFORMATION

¹ Current identity theft cases:

www.privacyrights.org

www.reclamere.com/headlines/index.php

www.bbbonline.org/update/issue.asp?id=48

² The Federal Trade Commission's guidelines for disposing of customer information:

www.ftc.gov/bcp/online/pubs/alerts/disposalart.shtm

³ Entrepreneur.com's information regarding the Fair and Accurate Credit Transactions Act:

www.entrepreneur.com/management/legalissues/article76976.html

⁴ National Conference of State Legislatures' state-by-state security breach notification laws:

www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

⁵ Plans to safeguard customer information—outlines provided by the Federal Trade Commission and the California Office of Information Security & Privacy Protection:

www.ftc.gov/bcp/online/pub/buspubs/safeguards.shtm

www.oispp.ca.gov/consumer_privacy/business/default.asp