The FCRA

A Double-Edged Sword for Consumer Data Sellers

By James A. Francis

It has been more than 40 years since Congress passed the Fair Credit Reporting Act (FCRA) out of concern for the growing use and potential misuse of consumer credit history, but its relevance as a consumer privacy statute has never been greater.

Given the electronic age in which we live, it should come as little surprise that the consumer data and reporting industry is larger and more robust than ever. The "Big Three" alone—TransUnion, Equifax, and Experian—issue more than 3 billion consumer reports a year and maintain files on 200 million Americans. But that is just a segment of the industry. A whole host of other companies known as specialty consumer reporting agencies, including the Big Three themselves, now sell consumer information relating to employment background checks, medical records and payments, insurance claim history and underwriting, and tenant rental history.

Masterfile

In addition, the types of consumer data products sold are greater and more varied than ever. As reported by the *Wall Street Journal* in November 2010, data brokers and consumer reporting agencies are selling far more than just the traditional credit report and score. They now sell products related to a consumer's bank deposit behavior and scores, income estimation, home value history, assets, and marketing demographics, as well as "collection trigger" data to lenders and collections agencies, which measure changes in a consumer's ability to repay existing or future debts. Lenders, insurers, employers, and landlords want faster and more efficient analytics and demographics tools for assessing a consumer's background, predicting risk, and maximizing profitability. In turn, the consumer data industry that services them is responding by inventing products that are more customized and detailed than ever before. Practically every aspect of consumers' transactional lives is now subject to scrutiny and sale—what they buy, what they sell, how much they make, how much they save, how much they owe, who they buy from, and whether those behaviors have changed in the last 90 days to six months. The consumer data industry is exploding.

Practically every aspect of consumers' transactional lives is now subject to scrutiny and sale.

FCRA AND CONSUMER PRIVACY

As a result of these trends, the consumer reporting and data industry is an increasing threat to consumer privacy and, consequently, is also the target of a new wave of FCRA litigation. When most practitioners think of the FCRA and the litigation surrounding it, they usually think of cases involving disputes over the accuracy of traditional credit reports. This is natural, as a sizable segment of past and current FCRA litigation arises from an individual consumer's dispute with a credit reporting agency (CRA) and/or bank concerning a credit report's inaccuracy.

However, in a significant fashion, the FCRA governs not just traditional credit reports and the Big Three but all information broadly defined as "consumer reports" and the companies that sell them. Though representatives of the consumer data industry would probably disagree with me, in my view practically any and all information about a consumer will constitute a consumer report if it provides useful information about a consumer's background, history, or habits and is used in connection with a credit or loan application, job, insurance underwriting, marketing, or collection purposes. And the Big Three are not the only players. ADP, LexisNexis, CoreLogic, Acxiom—these are just a few of the Goliaths selling consumer report data whose activities are subject to the FCRA.

Although much of the FCRA is oriented toward guarding against inaccuracies in the reporting of consumer data, a significant if not equal goal of the statute relates to protecting consumer privacy. This is introduced by Congress' fourth finding, which states: "There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to *privacy*."

The way the FCRA protects consumer privacy is twofold. The first way is direct. The FCRA restricts the sale and access of consumer report data to a handful of enumerated purposes (known in FCRA parlance as "permissible purposes"), such as credit, insurance and job applications, licenses, or review of an account. Any sale of consumer information for a non-permissible purpose subjects that reporting agency and user to liability for the mere sale and/or use of the information.

The second way the FCRA protects consumer privacy is indirect but very practical. The FCRA makes CRAs who sell consumer report data accountable to the consumer in a whole host of ways. It requires that CRAs observe a standard of "maximum possible accuracy" regarding the information they sell. It also imposes a wide range of duties on CRAs that are designed to make them and their activities transparent to consumers. It requires CRAs to set up toll-free numbers, provide consumers with a free copy of their consumer report annually, and provide consumers with *all* the information they sell about a consumer; the FCRA also affords consumers the right to dispute errors in the information and have the CRA investigate and correct any inaccuracies. In addition, the FCRA requires CRAs to provide consumers with the names and contact information of the parties to whom they sell this information and from whom they receive it.

These FCRA duties function to make CRAs' activities and their use of consumer information fair, open, and challengeable. When coupled with the FCRA's private right of action and mandatory fee shifting for proof of a violation, these "inspect and correct" duties (as they are known in litigator parlance) make CRAs wholly accountable for the misuse and/or mishandling of consumer report information. In this way, the FCRA acts as a double-edged sword for the consumer reporting industry. If companies want to sell consumer data, they must open themselves and the data they sell up to scrutiny by the consumer, the FTC, and the new Consumer Financial Protection Bureau (created through the recently enacted Dodd-Frank Wall Street Reform and Consumer Protection Act). Moreover, they expose themselves to potentially costly litigation, including class actions.

LOOKING FOR A LOOPHOLE

Needless to say, these FCRA duties impose significant costs to the CRA in the form of staff and infrastructure that cannot be passed onto the consumer or the CRAs' customers. CRAs must hire employees to handle and oversee consumer inquiries and disputes—which can be quite voluminous given the high error rates of consumer data—must adopt training and education programs, and must implement procedures for carrying out all their duties in a compliant manner.

As a result, there is a huge incentive for companies selling new and previously unvetted consumer data products to view these products as outside of the reach of the FCRA. After all, they are not traditional credit reports, right? Moreover, no case or FTC letter or regulation has held that such a product constitutes a consumer report. Similarly, there is the same incentive for new and specialized consumer data companies and "data brokers" to consider themselves as something different than a consumer reporting agency and outside the reach of the FCRA. And if the FCRA does not apply, then consumers need not be told about the data that is being sold about them, meaning these consumers will not be alerted to any errors in the data, will not submit disputes, and thus there will be no litigation. You get the message.

The current reality is that there is a whole world of consumer information and data selling that is carried on in an invisible fashion owing to the industry's self-serving belief that nontraditional credit report products fall outside the FCRA's reach. Being under the FCRA radar would have *many* advantages for a company, if only the statute permitted such a loophole.

THE LOOPHOLE IN ACTION: *CORTEZ V. TRANSUNION*

My law firm's recent case of *Cortez v. TransUnion, LLC*, 617 F.3d 688 (3d. Cir. 2010), is indicative of this current reality and the threat it poses to consumer privacy. *Cortez* arose from TransUnion's gross misreporting of what was a relatively new consumer information product, termed an "OFAC alert," on one of our client's credit reports. An OFAC alert is a message on a credit report that communicates to a lender or other user (e.g., a landlord) that the consumer applicant's name matches a name on the U.S. Department of Treasury's OFAC (Office of Foreign Assets Control) list. OFAC administers and enforces economic and trade sanctions against individuals and regimes considered as threats to national security. The OFAC list is a list of foreign terrorists and narcotics traffickers compiled by the U.S. Department of Transportation. Although the OFAC list had been around for years, the passage of USA Patriot Act regulations following 9/11 subjected creditors doing business with anyone on the OFAC list (whether knowingly or not) to serious civil and criminal penalties and fines including imprisonment. In response to their lending industry clients' new obligations, the credit reporting industry invented OFAC alerts as an add-on product to credit reports that would provide them with a simple and automatic method for complying with the USA Patriot Act. The purpose of an OFAC alert is simply to prevent the extension of credit to an applicant whose name is on the list, a hallmark of an FCRA consumer report. Prior to our agreeing to represent Sandra Cortez, our firm had never heard of OFAC credit report alerts, and no reported case had ever addressed them.

Notwithstanding the fact that Cortez had never been out of the country, had no criminal background, and had never been on the OFAC list, TransUnion reported an OFAC alert on her credit report in connection with her attempt to buy a car. Though unknown to Cortez and the dealership at the time, TransUnion was reporting the OFAC alert belonging to a completely different individual named Sandra Cortes Quintero, who was listed as a narcotics trafficker from Colombia and who had a date of birth almost 30 years younger. As a result, and among other things, Sandra Cortez was subjected to a harrowing ordeal at the dealership that included the dealership keeping her there against her will, stating that it would have to call the FBI. Hours later, and only after the dealership showed her a copy of the TransUnion credit report that enabled her to finally prove the mix-up, Cortez left astounded, scared, and determined to immediately clear up the error with TransUnion.

But that is where her problem got worse, not better. Each time she communicated with TransUnion to dispute the error, TransUnion denied that it was reporting any OFAC information about her. The credit reports TransUnion sent her never contained the OFAC alert reported to the dealership. Moreover, although she made four separate disputes to TransUnion, TransUnion informed her that her disputes were frivolous and that it was not reporting the OFAC information about her. Left with no option or remedy, Cortez filed suit.

The report sent to the car dealership claimed that my client was a narcotics trafficker from Colombia.

Discovery finally revealed the reason behind TransUnion's inexplicable conduct in denying that it was reporting the incorrect OFAC alert information about her and failing to respond to her disputes. TransUnion's legal view was that the OFAC alerts it reported about Cortez were separate products from the credit report it sold to the dealership—even though they appeared right in the middle of the report—and thus were not subject to the FCRA. As a result, TransUnion

argued that it did not have to disclose the alerts to Cortez when she requested copies of her personal credit report and had no obligation to investigate her dispute and remove the alerts from her file. Even during the litigation, TransUnion again reported the OFAC alert about Cortez to a prospective landlord in connection with an apartment she was seeking to rent.

At trial, the jury found that TransUnion willfully violated the FCRA and awarded Cortez $50,000 in actual damages and $750,000 in punitive damages. Notably, the jury's punitive damages award related to TransUnion's failure to disclose the OFAC alert information to her and investigate her disputes, not its initial erroneous reporting. The district court remitted the punitive damages post-verdict but otherwise denied TransUnion's post-trial motions.

Upon appeal to the Third Circuit, TransUnion argued that judgment should have been entered in its favor because the OFAC alerts it reported about Cortez were not FCRA-regulated information but an add-on, separate product that it had obtained from a third-party company; further, the OFAC alert did not contain traditional credit report information (e.g., credit accounts, loan repayment history, etc.). As a result, it argued the OFAC information was not part of her "file," and thus that it had no obligation to disclose it to her with her credit report or investigate her disputes of them. In addition, TransUnion asserted that even if OFAC alert information was covered under the FCRA, it could not have willfully violated the statute because no court or interpretative agency had ever found OFAC information to be covered FCRA information. The Third Circuit rejected every one of TransUnion's arguments.

In rejecting TransUnion's coverage argument, the Third Circuit noted the extraordinary breadth of the FCRA in that it does not just apply to traditional credit reports but covers "*any* communication of *any* information by a consumer reporting agency" that bears upon a consumer's character, general reputation, and/or numerous other features. In addition, the court held that the mere fact that TransUnion chose to use a third party to obtain its OFAC information, and did not keep such information in its credit history database, did not excuse it from disclosing the information to Cortez. Finally, the court held that the mere fact that no court or agency had ever found OFAC alerts to be FCRA-covered information did not excuse it from willfully violating the law. In essence, the court found that TransUnion knew or should have known better.

Either a company has no right to sell the information, or it is subject to the FCRA.

LESSONS FOR CONSUMER PROTECTION

Cortez is instructive for numerous reasons. First, it demonstrates one of the many types of new consumer data and background products that consumer reporting agencies and data brokers are selling "under the radar" or "off the books" of the FCRA. OFAC alerts are just one of many screening products sold by the consumer data industry in conjunction with or as an add-on to a traditional credit report. Each of these products presents implications to consumer privacy.

Cortez also demonstrates the disturbing perspective of at least a segment of the consumer data industry that considers some of the consumer data it sells to be off-limits to regulation and consumer scrutiny. The most surprising and puzzling thing about the *Cortez* litigation was TransUnion's recalcitrance. Even after Cortez's ordeal, a lawsuit, and a trial (and a ridiculous legal theory, in my view), it resolutely maintained its position that it was entitled to sell OFAC information because of its unilateral legal position that OFAC information was not FCRA-covered. TransUnion's approach raises the question of how many other products are being sold behind the scenes pursuant to an arrogant legal attitude that such products are outside the realm of the FCRA, and thus none of a consumer's (or a court's) business.

Finally, *Cortez* solidly addresses what should be (but is obviously not) a clear question about the relationship among a company's right to sell consumer information, a consumer's right to privacy, and the FCRA. That is, contrary to TransUnion's view of the world in *Cortez*, the FCRA does not permit some large gap between the right to sell consumer information and the obligation to do it in an FCRA-complaint manner. The FCRA does simply does not permit consumer data sellers to have their cake and eat it too by selling consumer data yet avoiding legal accountability. Either a company has no right to sell the information in the first place, in which case the mere sale is actionable, or the information is permissible information that must be transparent to the consumer and subject to the FCRA's protections. Although TransUnion is certainly not the only company deluding itself at the temporary expense of consumer privacy, the future of FCRA litigation will only tell how many other consumer data companies are engaging in this same fantasy. ■

James A. Francis (jfrancis@consumerlawfirm.com) is a shareholder with Francis & Mailman, P.C., a law firm based in Philadelphia, Pennsylvania, that concentrates on consumer protection litigation.