Use of OFAC Data in Spotlight: Consumer Reporting Agency Sued Again for False Positive Terrorist Watch List Data in Consumer Reports

Article By
Katherine A. Spicer
Glenn A. Brown
Squire Patton Boggs (US) LLP
Consumer Privacy World

- Administrative & Regulatory
- Criminal Law / Business Crimes
- Corporate & Business Organizations
- Financial Institutions & Banking
- Litigation / Trial Practice
- Pennsylvania

Tuesday, September 1, 2020

The U.S. Department of the Treasury’s Office of Foreign Assets Control ("OFAC") maintains the Specially Designated Nationals ("SDN") list, which is published to identify suspected terrorists and other bad actors. US persons are generally prohibited from dealing with anyone on the list, so companies and governments regularly run checks against the SDN list and other “terrorist watch list” data to ensure that they are not doing business with such bad actors. Some consumer reporting agencies ("CRAs") provide these checks to alert users of a possible terrorist in order to prevent prohibited transactions with such individuals. Often these users are legally required to run such checks.

Such terrorist watch lists, however, often contain very little personal information about the individuals on the list—sometimes the list only discloses a name and country of birth. Compounding the issue, some CRAs report a match or potential match if the name of the subject simply matches a name on the list even if other
information, such as a date of birth, does not match the subject. Did you catch that? A name can match with little to no other corroborating personally identifiable information and that terrorist alert can land squarely on an innocent consumer’s credit report just for having the same or similar name as a suspected terrorist. Indeed, as we have seen in the courts in recent years, false positive results from these checks are not uncommon.

This creates issues for CRAs that include terrorist watch list data in consumer reports, given the Fair Credit Reporting Act’s (“FCRA”) mandate that reasonable procedures must be used to ensure the “maximum possible accuracy” of information included in credit reports. If a CRA only has a name and country of birth from a terrorist watch list, or is not even attempting to use information in the terrorist watch list other than the name to match the consumer, how will it accurately attribute the record to the correct individual’s file? Well, recent high-stakes litigation on this issue suggests that complacent inclusion of terrorist watch list data in consumer reports violates the FCRA, and plaintiffs brought the issue back to federal court again this week in Pennsylvania.

Earlier this week, one of the “big three” credit bureaus was sued in the Eastern District of Pennsylvania over an alleged practice that the Ninth Circuit and the Third Circuit had previously determined violated the FCRA in unrelated class action litigation against the same credit bureau.[1] The class action complaint alleges that TransUnion, LLC (“TransUnion”) included information found on terrorist watch lists in its consumer reports in violation of the FCRA.

This is not the first time TransUnion has had to defend these practices. In 2010, the Third Circuit affirmed a jury award of compensatory and punitive damages against TransUnion and in favor of a class. The lead plaintiff was initially refused an auto loan because TransUnion included an “alert” on her credit report flagging her as being a possible match for an individual on the OFAC’s watch list.[2] Indeed, even though the individual on the OFAC list had a different date of birth than the plaintiff, TransUnion’s product flagged the plaintiff’s report because it only considered the name in determining a match. When the plaintiff disputed the information, TransUnion refused to conduct a reexamination on the basis that the information was not part of her credit file. She sued on behalf of the class and was awarded compensatory and punitive damages by a jury as a result of TransUnion’s failure to ensure the maximum possible accuracy of consumer reports, among other FCRA violations. On appeal, the Third Circuit found that the FCRA’s accuracy standard “requires more than merely allowing for the possibility of accuracy,” meaning that CRAs do not meet that standard by flagging certain consumers as “possible” matches for individuals on the OFAC’s watch list. The court also found that TransUnion’s failure to use a date of birth where available in the matching process was “reprehensible” and warranted punitive damages.

In 2011, a husband and wife also attempted to purchase an auto but were also initially refused because the husband’s name was flagged by the same TransUnion product involved in the Cortez case. Again, the husband brought class action litigation against TransUnion and the jury returned a verdict in favor of the class and awarded statutory and punitive damages.[3] On appeal, the Ninth Circuit reduced the amount of the punitive damages, but upheld the lower court’s finding of
willfulness, holding that “TransUnion was provided with much of the guidance it
needed to interpret its obligations under the FCRA with respect to OFAC Alerts in
2010 when Cortez was decided. Despite this warning, TransUnion continued to use
problematic matching technology and to treat OFAC information as separate from
other types of information on consumer report.”

The complaint in the instant case is therefore the third time that TransUnion is
having to defend a product and process that it has unsuccessfully defended thus far.
The lead plaintiff in this case was denied a mortgage loan based on being flagged
by the same TransUnion product involved in the Cortez and Ramirez cases. Plaintiff
contends that his personal information does not match the individual on the OFAC
watch list and that he is not a terrorist, but a law-abiding US citizen. TransUnion
continues to market the OFAC watch list data as a “credit report add-on” on its
website. TransUnion has apparently made no substantive changes to its procedures
for associating consumers with information from these watch lists- it continued to
use only first and last names, and did not consider dates of birth where available. It
also allegedly continues to present these alerts as “potential” matches despite the
results of the previous litigation. It should be no surprise that the law firm
representing the plaintiffs in this case also represented the plaintiffs
in Cortez and Ramirez. This is a case to watch, and we will do so here on CPW.


© Copyright 2020 Squire Patton Boggs (US) LLP

National Law Review, Volume X, Number 245

Source URL: https://www.natlawreview.com/article/use-ofac-data-spotlight-
consumer-reporting-agency-sued-again-false-positive