November 7, 2019

California DMV exposed drivers' SSN details to federal gov't officials

Bradley Barth

Follow @bbb1216bbb

For at least the last four years, the California Department of Motor Vehicles had mistakenly given seven government entities access to Social Security number information pertaining to roughly 3,200 drivers and license applicants, the state agency has admitted in a data breach notification.

"You are being sent the attached Notice regarding the disclosure of Social Security number information to another government agency, because state law requires that it be sent when there is an 'unauthorized acquisition of computerized data that compromises… the confidentiality… of personal information,' reads a notification letter that that the DMV mailed out to affected individuals. "The California Department of Motor Vehicles (DMV) considers the sharing of information regarding your Social Security number with a government entity that is not authorized to access it under the law to fall within this notice requirement."

According to an L.A. Times report, the government agencies and individuals who incorrectly had access to the SSN information included the Internal Revenue Service, the Small Business Administration, and district attorneys in San Diego and Santa Clara counties.

The data, which included whether or not a license holder had a verified Social Security card or was ineligible to be registered with Social Security, was accessed as a result of investigations into criminal activity or tax law compliance, reported the Times, citing officials. The Times also noted that the breach may have allowed federal government officials to look up information on illegal immigrants who applied for driver's licenses. (California allows them to apply if they can provide proof of identity and California residency.)

The DMV, which reportedly discovered the error on Aug. 2, emphasized that no hacking was involved in the incident, and information was not shared with any private individuals or organizations.

"Protection of personal information is important to the DMV, and we have taken additional steps to correct this error, protect this information and reaffirm our serious commitment to protect the privacy rights of all license holders," said an official statement from the Anita Gore, the DMV's deputy director of communications. "That's why the DMV immediately began correcting the access error following a legal compliance review, ensured that no additional confidential information was disclosed to these entities, and has implemented several additional layers of review – including review and signoff by DMV Chief Legal Counsel – for any requester seeking new access to SSN information."

Although the breach does not appear to have been caused by a purposefully malicious act, incidents like these can still have significant ramifications, experts reminded SC Media.

"Breaches aren't always the result of malicious attacks. In fact, they're often a consequence of misconfigurations. In these cases, there's no stereotypical bad guy to arrest, but often a group of well-meaning, but overworked and under-skilled staff that either couldn't keep up or just didn't know any better," said Tim Erlin, VP of product management and strategy at Tripwire, in emailed comments. "Finding and addressing misconfigurations can be automated, but you have to start with an understanding of how the systems should be configured in order to measure how they differ from that desired state."

"Sensitive data exposure creates consequences, regardless of the means of exposure – targeted attacks, unauthorized access, or employee negligence," added Emily Wilson, VP of research at Terbium Labs, in her own comments. "While targeted attacks provide a clearer measure of intent… unauthorized access can have the same fallout, even if on a different scale. Fraud, identity theft, account

takeover and new account fraud can still result from the data exposure, creating a host of issues for consumers who feel the impact of the exploits one way or another."

TOPICS: GOVERNMENT | NETWORK SECURITY | PRIVACY & COMPLIANCE

Leave a Reply

You must be logged in to post a comment.

Back to Top ↑

OTHER SC SITES

RiskSec Conference

SC Resource Library

SC Online Events

SC Awards