Proskauer

Standing to Sue: Is Theft of Drivers' License Numbers Sufficient to Allege Imminent Threat of Future Harm?

Proskauer on Privacy Blog on **December 16, 2022**

Judge Jeffrey White of the Northern District of California recently dismissed a putative class action lawsuit in which plaintiffs claimed they faced an imminent threat of future of harm in the form of identity theft and fraud because their personal information, specifically their driver's license numbers, may have been compromised in a data breach. In doing so, the court determined that driver's license numbers "are not as sensitive as social security numbers," and that they don't rise to the level of sensitive personal information "needed to establish a credible and imminent threat of future harm" for Article III standing. *Greenstein et al v. Noblr Reciprocal Exchange, No. 4:2021cv04537 (N.D. Cal. 2022)*.

Noblr is one of a growing number of data breach-related cases in which courts must determine whether the theft or exposure of specific types (and combinations) of personal data establishes a credible threat of real and immediate harm sufficient to confer standing. In making this determination, courts consider whether that type (or combination) of data is more or less likely to subject plaintiffs to risk of identity theft or fraud as well as the ability of the consumer to take action to reduce or eliminate the risk of harm caused by the theft.

There are a variety of opinions in this area, but, as an example, courts have generally found the theft or exposure of social security numbers to be more likely to subject plaintiffs to a credible threat of imminent harm, than theft of credit or debit card information, because a social security number derives its value in that it is "immutable" and can be used to commit identity theft and open new accounts without the need for much additional information. Driver's license numbers, however, appear to be treated differently. While driver's license numbers, like social security numbers, are difficult to change and derive value from their immutability, plaintiffs have not always been able to convince courts that without more there is a credible risk of identity theft or fraud that risks imminent injury.

Similar to the *Noblr* court, other federal courts in California have distinguished driver's license numbers from social security numbers and dismissed claims at an early stage when limited personal information in the form of a driver's license number is alleged to have been exposed. For example, in *In re Uber Technologies., Inc., Data Sec. Breach Litigation*, a Central District of California court in 2019 dismissed a proposed data-breach class action, with leave to amend, because the plaintiff failed to explain how a hack of basic contact information and driver's license numbers, unlike social security numbers, create a credible threat of fraud or identity theft sufficient to allege injury in fact. Similarly, in *Antman v. Uber Technologies, Inc.*, a Northern District of California court held that the theft of Uber drivers' names and driver's license numbers, even combined with bank account and routing numbers, without more (like social security numbers), did "not plausibly amount to a credible threat of identity theft that risks real, immediate injury."

However, not all Courts within the Ninth Circuit have subscribed to this reasoning: A District of Nevada court, in *Stallone v. Farmers Group, Inc.*, determined that a data breach that compromised plaintiff's driver's license number and address was sufficient to establish a credible risk of immediate harm where the breach was part of a concerted campaign by hackers to "pharm" and accumulate the personally identifiable information of plaintiff and other victims, and the information would likely be used to fraudulently apply for unemployment benefits, cultivate a fraudulent synthetic identity, or gain access to victim's bank accounts and other personal information.

In sum, while opinions from California federal courts suggest they are becoming less sympathetic to future, unrealized harm stemming from data breaches, especially where social security numbers aren't involved, other courts still seem willing to find the theft of less sensitive information, such as driver's license numbers, sufficient to confer standing. This is especially true when the plaintiff is able to convince the court that the exposed information can be used for identity theft, to rack up fraudulent charges, or gain access to additional personal information.

We will be watching this space for further developments, as the Ninth Circuit will likely need to weigh in on this issue to ensure that the circuit uses a single, unified approach. It is also important to note that these evolving court decisions focus on standing and harm associated with data breaches. These decisions do not eliminate a company's privacy and cybersecurity compliance obligations, including the requirements to provide privacy notices, to be transparent and accurate regarding the company's collection, use, disclosure and storage of personal information and a company's requirement to respond to consumer requests under certain state privacy laws such as the California Consumer Privacy Act of 2018.

View original.

Related Professionals

- **Margaret A. Dale**
  Partner
- **Nolan M. Goldberg**
  Partner
- **Amy B. Gordon**
  Associate