FAQ

1. **Have all the victims been notified?**

It appears that the Department of Justice is at least claiming they have. In a letter to various California State Senators dated July 21, 2022, Chief Deputy Attorney General Venus D. Johnson writes:

"We are working to address concerns regarding any impacts on individuals whose data was exposed. We have sent letters to those individuals who we believe may have been impacted by the CCW data exposure and have established a call center for anyone who believes they may have been impacted. The call center is open from 6 a.m. to 6 p.m. PST and can be reached at 1-833-909-4419. Additionally, we are offering one year of complimentary credit monitoring services to impacted individuals through IDX. Impacted individuals may enroll in these services at https://response.idx.us/dojca/, using the enrollment code provided in the notification letter. We also continue to communicate with law enforcement partners throughout the state and will collaborate with them to assist any affected individuals."

Whether or not everyone affected has actually received a letter likely depends on how up-to-date the DOJ's information is on where that person lives. If you did not receive a letter but believe you may have been affected, CRPA recommends placing a call with the call center referenced above.

2. **What information was contained in the leak?**

For a full description of what was leaked to CRPA's knowledge, click here.

3. **Can the government be held liable for losses, damages, injury, or death that directly resulted from this leak?**

If someone can prove they were harmed by the leak, there are a few legal theories which they could pursue to attempt to recover damages. While this FAQ is not intended to be a comprehensive legal analysis, CRPA will attempt to briefly describe the three of the main legal theories and their relative odds of success.

- Federal Right to Privacy: 14th Amendment to the U.S. Constitution & 42 U.S.C. § 1983

A claim brought based on the federal right to privacy is a tenuous theory of liability. Unless more information as to the reason for the leak is revealed which shows the leak to have been an intentional act (i.e., the person or persons at the DOJ who caused or facilitated the leak did so with the intent to publish gun owners' personal information), a Section 1983 action based on a *negligent* leak of the data would likely be unsuccessful. This is because "negligent conduct by a state official, even though causing injury" is not grounds for finding the deprivation of a constitutional right." *Daniels v. Williams*, 474 U.S. 327, 331 (1986). If evidence comes to light which shows the leak was intentional, we will update this portion accordingly.

- Right to Privacy Under Article I, Section 1 of the California Constitution

The California right of privacy protects the individual's reasonable expectation of privacy against a serious invasion and it is "much broader than its federal analog". *American Academy of Pediatrics v.*

Lungren, 16 Cal. 4th 307, 325–26 (Cal. 1997). California courts recognize a constitutionally protected interest in a person's name, address, and phone number.

To establish a violation of privacy rights in California, a plaintiff needs to establish three things: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy. In this circumstance, people with conceal carry permits do have a legally protected privacy interest under California law, and they also have a reasonable expectation that their data will not be accidentally leaked out for no reason. Whether the invasion of privacy is "serious" or not in a legal sense will likely vary based on the individual.

Such a claim may thus be viable, and if you believe you have been harmed by the leak you should seek to consult an attorney as you may need to file what is called a government claim to preserve your right to sue in state court. That said, whether or not money damages are available remains an open question. While one case has said that "courts, exercising their authority over the common law, may, in appropriate circumstances, recognize a tort action for damages to remedy a constitutional violation", *Katzberg v. Regents of University of California,* 29 Cal.4th 300, 325 (2002), what constitutes an "appropriate circumstance" is up for debate, and it would be quite risky to assume money damages are available from the government in such a lawsuit.

-The Information Practices Act (California Civil Code section 1798, *et seq*.)

California's Information Practices Act (IPA) broadly protects people's interest in the confidential and private information stored in government files. While an extensive analysis of the IPA is outside the scope of this FAQ, whether a claim for the DOJ's data leak is viable likely depends on whose privacy interest is being pursued. An IPA claim will require arguing that a plaintiffs' privacy interest is greater than the public's right to know, even though the leak was not intentional (as far as we know). In addition to actual damages as well as attorney's fees and costs, a successful plaintiff under the IPA can recover $2,500 in exemplary damages if they prove the leak was intentional.

4. Does accepting the DOJ's complimentary credit monitoring service waive claims against them?

No. There is no waiver of claims or release if you use the free credit monitoring.