INFORMATION BULLETIN:

SHARING OF GUN OWNER DATA PURSUANT TO AB 173

DECEMBER 13, 2021

The California Rifle & Pistol Association is dedicated to protecting, defending, and promoting the Constitution of the United States and the rights of individuals to keep and bear arms in public and in private. In direct furtherance of that mission, CRPA will work to ensure the privacy of tis members and all California gun owners from unconstitutional and illegal disclosures of their personal information.

Many of CRPA's members have raised legitimate concern over a recently passed bill, Assembly Bill No. 173 ("AB 173"), which beginning January 1, 2022, requires the California Department of Justice ("DOJ") to share data collected in connection with firearm purchases and transfers here in California. While CRPA attorneys continue to analyze AB 173 for potential legal challenges, the following information has been prepared to inform members and concerned gun owners of its effects and what immediate steps can be taken to protect your privacy.

I. RIGHT OF PRIVACY AND CALIFORNIA'S INFORMATION PRACTICES ACT

Although not expressly recognized in the United States Constitution, California's Constitution recognizes an inalienable right to privacy.[1] Fearing the indiscriminate collection, maintenance, and dissemination of personal information by various government entities, the California Legislature enacted the Information Practices Act of 1977 ("IPA") to address these issues and the lack of effective laws and legal remedies. The IPA specifically sought to protect the privacy of individuals as a result of an increase in the use of computers to store and disseminate personal information.

In general, the IPA prohibits California state agencies from disclosing any personal information in a manner that would link the information to the individual to whom it pertains absent limited circumstances.[2] Once such exception is to provide the information to the University of California or another nonprofit entity conducting scientific research, but only if the request for the information satisfies the following requirements:

[1] Cal Const, Art. I § 1.

[2] Cal. Civ. Code § 1798.24.

1) The researcher has provided a plan sufficient to protect personal information from improper use and disclosures;
2) The researcher has provided a sufficient plan to destroy or return all personal information when no longer needed; and,
3) The researcher has provided sufficient written assurances that the personal information will not be reused or disclosed to any other person or entity, or used in any manner not approved, except as by law or for authorized oversight of the research project.[3]

Notably absent from the provisions of the IPA is a mandate that personal information be disclosed should the above requirements be satisfied. In other words, a state agency is not **required** to disclose any personal information for scientific research purposes.

II. ASSEMBLY BILL NO. 173

AB 173 does not change California's IPA directly with regards to firearm purchase and transaction data. Instead, AB 173 amends the applicable Penal Codes regarding the collection of data by DOJ pertaining Dealer Record of Sale ("DROS") data, stating in part:

> *All information collected pursuant to this section shall be maintained by the department and shall be available to researchers affiliated with the California Firearm Violence Research Center at UC Davis for academic and policy research purposes upon proper request and following approval by the center's governing institutional review board when required*.[4]

Given use of the phrase "shall be available," AB 173 ***requires*** DOJ to provide the information to the California Firearm Violence Research Center if a proper request is made. However, the IPA's restrictions appear to remain in effect. What's more, DOJ retains discretion to release the same data to "any other nonprofit bona fide research institution accredited by the United States Department of Education or the Council for Higher Education Accreditation" subject to the IPA's restrictions, just as it did prior to the enactment of AB 173.[5]

Any DROS information provided, whether to the California Firearm Violence Research Center or any other nonprofit institution, is only to be used for research or statistical activities and "shall not be transferred, revealed, or used for purposes other than research or statistical activities, and reports or publications derived therefrom shall not identify specific individuals."[6] **In other words, UC Davis and any other non-profit provided access to DROS information cannot disclose a person's personal information in any reports or publications generated from the information provided by DOJ.**

[3] Cal. Civ. Code § 1798.24(t).

[4] Cal. Pen. Code § 11106(d) (eff. Jan. 1, 2022).

[5] *Id.*

[6] *Id.*

In addition to DROS data, UC Davis will also be provided with information regarding restraining orders "or any other data relating to prohibition on firearm ownership.[7] But as with the above, any information identifying individuals "shall not be revealed or used for purposes other than research or statistical activities.[8]

a. Required DOJ Procedures

AB 173 requires DOJ to establish procedures implementing the restrictions of the IPA as applied to the disclosure of information to the California Firearm Violence Research Center, as well as any nonprofit education institution, or other specific entities. Specifically, the procedures must include, but are not limited to, "requests for data and timely review of requests."[9] Regardless of what the procedures may be, any material identifying individuals "shall only be provided for research or statistical activities and shall not be revealed or used for purposes other than research or statistical activities."[10] And any reports or publications derived therefrom cannot disclose a person's personal information. [11]

III. POTENTIAL LEGAL CLAIMS FOR VIOLATIONS OF THE IPA

Should either DOJ or the California Firearm Violence Research Center fail to comply with the requirements of either the IPA or the restrictions imposed by AB 173 regarding the use of personal information, individuals affected may be able to pursue legal action. But to be successful on such a claim, plaintiffs must be able to prove both liability and resulting damages.

a. Establishing Damages

The IPA generally allows plaintiffs to seek statutory damages of up to $2,500 per violation in addition to actual damages suffered, but only if the defendant is a private entity. Because DOJ and the California Firearm Violence Research Center are government entities, *this $2,500 statutory damages provision does not apply*, leaving only actual damages as an available remedy, and one that each individual plaintiff must be able to prove in any civil suit. But if the violation is the result of a nonprofit private entity, then the statutory damages provision may still apply.

To prove actual damages, a plaintiff must show that the disclosure of his or her personal information resulted in a tangible injury, e.g., misuse of their private information by a third party to engage in identity theft. Identity theft or other economic harm would need to be proved on a case-by-case basis, making a class action lawsuit very difficult or impossible due to a lack of commonality of injury among victims. For example, where some victims may suffer identity theft as a result of the release and illicit use of personal information, and such injury results in a victim paying for ongoing credit monitoring or causes a loss of credit worthiness or imposes on a victim the burden of fees and costs associated with fraudulent charges on that person's revolving credit

[7] Cal. Pen. Code § 14231.5(a).

[8] Cal. Pen. Code § 14231.5(b).

[9] Cal. Pen. Code § 14240(a).

[10] Cal. Pen. Code § 14240(b).

[11] *Id.*

accounts, other victims of the release of personal information may never suffer any resultant identity theft or tangible loss.

In each circumstance, to prevail on a claim that a violation caused harm/damages to a victim, that victim would have to show individualized and material injury from the release of the personal information. While the possibility exists that the reasonable emotional distress aspect of victims' learning of the unlawful release of their personal information might be shown by an individual victim to have been suffered, each such injury would be evaluated on a case-by-case basis by a court to determine whether such an injury was actual and significant enough to award such a victim damages.

In conclusion, individuals whose personal information is improperly released may have a viable liability claim against DOJ, the California Firearm Violence Research Center, or any other non-profit entity for violating, inter alia, the IPA. All such claims, however, will be subject to proving actual and individualized damages arising out of the improper release.

b. Administrative Claim Requirement

As this is a generalized conclusion not specific to any one victim and provided solely for the purposes of providing public information, any victim should act quickly to have a personalized legal consultation regarding whether he or she has grounds for a viable legal action. This of course requires the victim to be made aware of the breach somehow. But there are other considerations one must account for when suing a state agency for damages.

Generally, before a lawsuit can be filed against a government entity, an administrative claim must be submitted. Victims desiring to pursue a claim or lawsuit against DOJ or other government entity should be mindful of general requirements under state law of a prerequisite requirement of "claims presentment" to government agencies. This generally requires that an administrative claim against a government entity such as DOJ *must be filed no more than six months after the date of the injury*. Failure to submit a timely claim can result in loss of a "right to sue" that government agency.

For information on the steps involved in the government claim process, visit the Government Claims Program website.

c. Statute of Limitations

As stated above, individuals who had their information improperly disclosed by a government entity have six months to file an administrative claim. If you are the victim of your personal information being improperly disclosed, you should consult with an experienced attorney to accurately determine any deadlines based off your individual claims.

IV. Protecting Your Identity and Credit Rating

In addition to understanding what legal remedies you may have should your personal information be improperly disclosed, you may wish to take additional steps to protect your identity and credit profile. Several companies offer monitoring services to customers allowing them to monitor their credit reports to determine whether any personal information is or has been used to engage in fraudulent credit transactions in their name.

You can learn more about how to monitor credit reports by contacting any of three credit reporting agencies identified below:

EQUIFAX - www.equifax.com
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111

EXPERIAN - www.experian.com
P.O. Box 2104
Allen, TX 75013-0949
1-888-EXPERIAN (397-3742)

TRANSUNION - www.transunion.com
P.O. Box 1000
Chester, PA 19022
1-800-916-8800

The CRPA legal team makes no warranties about the efficacy of such services, but such services purport to regularly monitor their members' credit and alert their members to any unusual activity.

Individuals who have not obtained a free credit report from any one of the three agencies within the past 12 months are entitled to request a copy of their credit report(s) free of charge from the website www.annualcreditreport.com. Please note, there are websites with similar names that will nonetheless attempt to charge for copies of credit reports or otherwise attempt to sell credit monitoring services. www.annualcreditreport.com is a free service run by the three credit-reporting agencies that is obligated under state and federal law to provide an annual free-of-charge credit report.

Individuals who are concerned about unauthorized revolving credit and other accounts being opened in their name using improperly disclosed information can also have a security freeze put on the credit profiles for maintained by all three credit monitoring agencies. Information about how to place a security freeze with any of the three reporting agencies can be found here and here.

Individuals can also request that those reporting agencies place a consumer statement in their credit file identifying that they have had personal information disseminated, or if actual identity theft occurs, that they have been the victim of identity theft. Please note, that absent evidence of actual identity theft occurring, credit reporting agencies are allowed to charge $10 per occurrence every time a request is made to have a credit profile frozen or unfrozen.

If it is discovered that personal information was used to engage in fraudulent credit transactions, victims should contact their credit card companies to alert them of the theft of their personal information. Some of them will allow credit account holders to set up text-based or phone-based alert systems for unusual activity on those account holders credit card accounts, or will allow account holders to add additional layers of security to their account to include additional personal information that would not be found with the type of personal information disseminated, e.g., some credit card companies will allow account holders to add a PIN or password

to their account as an additional security measure against anyone attempting to access the account who is also in possession of other personal information.

Individuals should also monitor any bank accounts, mutual fund accounts, IRAs, and 401k or other retirement accounts, to ensure that none of their personal information has been used to access funds in these accounts. While most issuers of revolving credit accounts are required by law to hold their account holders responsible for no more than $50 of any fraudulent charges made on an account, these rules do not apply to other types of accounts such as retirement or savings accounts.

Additionally, you should consult with a tax specialist about the need for and desirability of alerting the federal Internal Revenue Service about the breach of any personal information. Criminals with access to individuals' Social Security Number and other private data can file false tax returns in those victim's names to seek a refund of tax withholdings to which victims may actually be entitled. Information on how to file an affidavit of identity theft with the IRS can be found at https://www.irs.gov/uac/taxpayer-guide-to-identity-theft.

The Federal Trade Commission maintains a website where victims of identity theft can report and register the circumstances of the theft of personal information, to the extent that any victim discovers that the dissemination of personal information has led to actual identity theft. Information about this process can be learned by visiting https://www.ftc.gov/faq/consumer-protection/report-identity-theft. Regardless of what steps a person may take to protect their identity and credit profile, should it be discovered that personal information has been stolen, a criminal complaint should be filed with the victim's local police or sheriff's department or with the local authorities in the jurisdiction where the theft occurred.

V. CONCLUSION

CRPA attorneys are working to bring all possible legal challenges to AB 173. In the meantime, should you be made aware of your personal information being improperly disclosed as a result of AB 173, please contact the CRPA legal team immediately by calling (562) 216-4444 or by sending an email to helpdesk@michellawyers.com. It is important for any individual who has had their personal information improperly disclosed to consult with qualified legal counsel as soon as practicable to determine if they have suffered actual damages, and what legal remedies they can or should pursue, and the time limits for seeking those remedies.

Victims of improper disclosure can also contact their local bar association's lawyer referral service or visit the State Bar of California website to locate qualified counsel. Regardless of whether your personal information has been improperly disclosed, you should take steps to monitor your credit and use other identity theft prevention tools and resources to the extent you know or reasonably believe you are or may become the victim of identity theft as a result of any improper disclosure of your personal information.

Be sure to subscribe to CRPA email alerts to stay informed about AB 173 and any future legal challenges by visiting www.CRPA.org