CRPA INFORMATION BULLETIN:

UPDATE ON DOJ'S IMPROPER DISCLOSURE OF CERTIFIED FIREARM SAFETY INSTRUCTOR PERSONAL INFORMATION

CRPA's legal team has prepared the following information regarding the California Department of Justice's ("DOJ") improper disclosure of personal information of DOJ Certified Firearm Safety Certificate ("FSC") instructors. Be advised, this memorandum is for general information purposes only and does not constitute legal advice or create an attorney client relationship. Victims of DOJ's improper disclosure of personal information should consult with an attorney to determine their rights as based on their individual circumstances.

I. FACTUAL BACKGROUND

DOJ began mailing Release of Personal Information letters to FSC instructors in December 2016. DOJ's letter admitted that in October 2016, DOJ had inadvertently released the name, date of birth, and California Driver's License and/or Identification Card numbers of FSC instructors to a third-party in responding to a public records request.

The party to whom this information was released was not immediately identified. Through Public Records Act Requests, it was later determined that the person to whom FSC instructors' personal information was disclosed is a reporter for Southern California Public Radio (KPCC), Aaron Mendelson. DOJ claims that it discovered the data breach a few days after the disclosure of the data, and immediately contacted the reporter to ask that the information be destroyed and not be disseminated further. Although we have reached out to the reporter directly, we have been referred to KPCC's legal department and are still awaiting an official response regarding the status of the information in KPCC's possession. For its part, DOJ has not confirmed or otherwise further commented on whether it was able to get Mr. Mendelson to comply with its request. So to date, we have not been able to confirm whether any of the FSC instructors' personal information released by DOJ has been destroyed, is still in Mr. Mendelson's possession, or may have been disseminated to other parties.

II. POTENTIAL LEGAL CLAIMS

As discussed below, DOJ's failure to comply with the requirements of the Information Practices Act of 1977 ("IPA") and general negligence almost certainly makes DOJ liable for their actions and potentially constitutes grounds for a civil law suit against the State of California. But in

order to be successful on such a claim, plaintiffs must be able to prove both liability and resulting damages.

a. Basis for Liability

By disclosing private FSC instructor information, DOJ violated the privacy rights of FSC instructors. Because DOJ is the agency responsible for the private information of every registered gun owner and FSC instructor, DOJ has a legal duty to use due care in protecting that information. By disclosing the personal information of FSC instructors to a reporter, DOJ's actions violated this duty and makes DOJ potentially liable for a negligence claim.[1]

DOJ is also subject to the requirements set forth under the IPA. Fearing the indiscriminate collection, maintenance, and dissemination of personal information, and the lack of effective laws and legal remedies, California created the IPA to protect the privacy of individuals as a result of an increase in the use of computers to store and disseminate personal information.

In addition to the strict limits placed on the collection and maintenance of personal information by state agencies like DOJ, the IPA prohibits the disclosure of "any personal information in a manner that would link the information disclosed to the individual to whom it pertains" absent specific circumstances.[2] None of the listed exceptions to this restriction allow DOJ to disclose the personal private information of circumstantial FSC instructors.

b. Establishing Damages

The IPA generally allows plaintiffs to seek statutory damages of up to $2,500 per violation in addition to actual damages suffered from a breach, but only if the defendant is a private entity. But because DOJ is a state agency, *this $2,500 statutory damages provision does not apply*, leaving only actual damages as an available remedy against the State, and one that each individual plaintiff must be able to prove in any civil suit.

---

[1] See *City of Santa Barbara v. Superior Court*, 41 Cal. 4th 747, 754, 62 Cal. Rptr. 3d 527, 161 P.3d 1095 (2007); *Flowers v. Torrance Memorial Hospital Medical Center*, 8 Cal. 4th 992, 999, 35 Cal. Rptr. 2d 685, 884 P.2d 142 (1994); *Elsheref v. Applied Materials*, Inc., 223 Cal. App. 4th 451, 459, 167 Cal. Rptr. 3d 257, 79 Cal. Comp. Cas. (MB) 207 (6th Dist. 2014), review denied, (Apr. 30, 2014); See also CACI No. 400, BAJI No. 310.

[2] Cal. Civ. Code § 1798.24.

To prove actual damages, a plaintiff would show that DOJ's 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 certification of a class in a potential 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 accounts, other victims of DOJ's release of personal information may never suffer any resultant identity theft or tangible loss.

In each circumstance, to prevail on a claim that DOJ's violation of the law caused harm/damages to a victim, that victim would have to show individualized and material injury from the release of the information. If it is true that the one known recipient of the personal information—Mr. Mendelson—destroyed the information or otherwise did not disseminate it, then it is likely that victims of DOJ's release will not suffer a tangible and compensable harm.

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. There are too many variables from victim to victim to form any reliable conclusions about whether an individual victim of DOJ's personal information release could succeed in a lawsuit against DOJ alleging only emotional distress damages, especially in the absence of other types of injury suffered such as those identified above.

In conclusion, all victims may have a viable liability claim against DOJ for violating, inter alia, the IPA. All such claims, however, will be subject to proving actual and individualized damages arising out of the release of that victim's information.

c. 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 on a matter of interest, particularly to FSC instructors and firearms owners, any victim should act quickly to have a personalized legal consultation regarding whether he or she has grounds for a viable legal action.

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 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 such a claim results in loss of a claim or "right to sue" that government agency.

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

d. Statute of Limitations

As stated above, FSC instructors who had their information improperly disclosed have six months to file an administrative claim against DOJ. Based off the fact that DOJ began mailing notice to FSC instructors on December 28, 2016, we presume FSC instructors have until sometime in June to file any potential administrative claim against DOJ. We encourage FSC instructors to consult with an experienced attorney to accurately determine any deadlines based off their individual claims.

It is highly likely that any administrative claim will be denied. But denial of an administrative claim may give you the right to pursue a small claim against DOJ in state court. FSC instructs should be aware that there is a two-year deadline under the IPA for filing any action against a state agency.[3] We presume that because FSC instructors were notified on December 28, 2016, this means that the deadline to file a claim under the IPA is December 28, 2018. Even so, FSC instructors should pursue their claim immediately and consult with an experienced attorney to accurately determine any deadlines based off their individual claims.

For more information about filing a small claim, visit the California Courts website.

III. PROTECTING YOUR IDENTITY AND CREDIT RATING

Given the current uncertainty about the status of personal information obtained by the reporter, it is appropriate for victims to take additional steps to protect their identity and credit profile. To do so, they can monitor their credit reports to determine whether any personal information released by DOJ

[3] Cal. Civ. Code § 1798.49

has been used to engage in fraudulent credit transactions in their name. Victims 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

As noted in its letter to affected instructors, DOJ is offering a one-year membership of Experian's "ProtectMyID" service. The CRPA legal team makes no warranties about the efficacy of such services, but such services purport to regularly monitor members' credit and alert members to any unusual activity.

Victims 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.

Victims who are concerned about unauthorized revolving credit and other accounts being opened in their name using the 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.

Victims 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 by DOJ, 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 such as the type released by DOJ.

Victims 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, victims of DOJ's information release should consult with a tax specialist about the need for and desirability of alerting the federal Internal Revenue Service about the breach of their personal information. Criminals with access to individuals' Social Security Number and other private data can file false tax returns in those victim's names in order to seek 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 by DOJ 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.

IV. CONCLUSION

FSC instructors are victims of a violation of California law as a result of DOJ's unlawful release of personal information. And we encourage all FSC instructors affected by DOJ's improper disclosure to pursue any available claims they may have.

FSC instructors should 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 DOJ's personal information breach should consult with qualified counsel experienced in civil lawsuits regarding identity theft and government claims in order to determine what claims they each may have, what damages they each may have incurred, and what statutes of limitations or other deadlines for presenting such claims may be. Victims can contact their local bar association's lawyer referral service, or visit the State Bar of California website to locate qualified counsel. Additionally, FSC instructors should take steps to monitor their credit and use other identity theft prevention tools and resources to the extent such instructors know or reasonably believe they are or may become the victims of identity theft as a result of the DOJ's data breach.