TODD JOHNS
SHERIFF/CORONER
DIRECTOR

Office of the Sheriff

Office of Emergency Services

1400 E. Main Street, Quincy, California 95971 • 530-283-6300 •

PRESS RELEASE

FOR IMMEDIATE RELEASE
07/11/2022

CCW Data Breach Update

This week, CCW holders who were denied or granted a permit between 2011 and 2021 should be receiving communication from the Attorney General regarding the unauthorized data breach by the California Department of Justice (DOJ). This letter explains What Happened, What Information Was Involved, What They Are Doing, What You Can Do, and provides contact information for the DOJ.

To reiterate our earlier statement on this issue, we are incensed about this data breach and remain concerned for the safety and security of our CCW holders past and present. We strongly encourage those who receive the letter from the DOJ to take all appropriate steps to safeguard your personal information to include enrolling in the free IDX service provided. There will be an enrollment code on your letter from the DOJ.

A copy of the letter is attached.

Visit us online at plumascounty.us and follow us on Facebook

###

Contact information:
Chandler Peay
Deputy Sheriff/Public Information Officer

State of California
Office of the Attorney General

ROB BONTA
ATTORNEY GENERAL

July 8, 2022

RE: **Notice of Data Breach**

Dear [redacted]

This letter is to inform you of a recent security incident that involved an unauthorized release of your personal information by the California Department of Justice (DOJ). This information primarily relates to individuals who were denied or granted a concealed and carry weapons (CCW) permit between 2011-2021, and was disclosed in connection with an update to our Firearms Dashboard Portal. While we are not aware of any actual or attempted misuse of your information, we are providing you with an overview of the incident, our ongoing response, and resources available to you right now to help protect your identity, should you feel it is appropriate to do so.

What Happened
As announced on June 29, 2022, personal information was disclosed on June 27, 2022 in connection with the update of DOJ's Firearms Dashboard Portal. After DOJ learned of the data exposure, the Department took steps to remove the information from public view and shut down the Firearms Dashboard. The dashboard and data were available for less than 24 hours.

What Information Was Involved
As of the date of this letter, the information that we have determined was exposed includes full name, date of birth, address, gender, race, CCW license number, California Information Index number (which is automatically generated during a fingerprint check for a CCW or for another purpose), and other government-issued identifiers. In some cases, exposed information may also include driver's license number, and internal codes corresponding to the statutory reason that a person is prohibited from possessing a firearm. Social Security numbers or any financial information were **not** disclosed as a result of this event.

What We Are Doing
We are working to improve security, mitigate risk, and have launched an investigation into how this occurred at DOJ. We have removed the information from public view, shut down the Firearms Dashboard, and are contacting individuals who have been impacted by the breach to provide additional information and resources for them. Additionally, we are conducting a review of our policies and procedures and working to implement additional security measures to protect the security of information in our possession and communicating regularly with our law enforcement partners throughout the state.

As an added precaution and to provide direct assistance to those impacted, we have established a call center to address any questions you may have. We are also offering complimentary access to credit monitoring services through IDX, which includes: 12 months of triple-bureau credit monitoring, CyberScan dark web monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

We encourage you to contact IDX with any questions and to enroll in the free credit monitoring services by calling (833) 909-4419 or going to https://response.idx.us/dojca and using the Enrollment Code provided at the top of this letter. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is October 8, 2022.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing financial account statements and monitoring your credit reports for suspicious activity. In addition, we recommend you contact IDX with any questions and to enroll in the free credit monitoring services.

You may also take the following steps:

- **Monitor your credit.** One of the best ways to protect yourself from identity theft is to monitor your credit history. To obtain free copies of your credit reports from the three major credit bureaus go to www.annualcreditreport.com.

- **Consider placing a free credit freeze on your credit report.** Identity thieves will not be able to open a new credit account in your name while the freeze is in place. You can place a credit freeze by contacting each of the three major credit bureaus:
  - Equifax: www.equifax.com/personal/credit-report-services/credit-freeze/; 1-866-349-5191
  - Experian: www.experian.com/freeze/center.html; 888-397-3742
  - TransUnion: www.transunion.com/credit-freeze; 800-680-7289

- **Place a fraud alert on your credit report.** A fraud alert helps protect you against the possibility of someone opening new credit accounts in your name. A fraud alert lasts 90 days and can be renewed. To post a fraud alert on your credit file, you must contact one of the three major credit reporting agencies listed above. Keep in mind that if you place a fraud alert with any one of the three major credit reporting agencies, the alert will be automatically added by the other two agencies as well.

- **Additional Resources.** If you are a victim of identity theft, contact your local police department or sheriff's office right away. You may also report identity theft and generate a recovery plan using the Federal Trade Commission's website at identitytheft.gov. For more information and resources visit the Attorney General's website at oag.ca.gov/idtheft.

For More Information

You will find detailed instructions for credit monitoring enrollment services on the enclosed Recommended Steps document.

We sincerely regret the unacceptable disclosure of your personal data and I offer my sincerest apology on behalf of the entire Department of Justice. We urge you to consider the steps we have provided to help protect yourself from the possibility of identity theft. We want to assure you that we are taking appropriate actions with regard to the staff involved. If you have any questions or concerns regarding this letter, please call (833) 909-4419 or go to the DOJ web page at www.oag.ca.gov/DataExposure for any additional questions you may have.

Sincerely,

Rob Bonta

ROB BONTA
Attorney General