
THIRD READING

Bill No: SB 1208
Author: Grayson (D)
Amended: 5/14/26
Vote: 21

SENATE PUBLIC SAFETY COMMITTEE: 6-0, 4/21/26
AYES: Arreguín, Seyarto, Caballero, Cortese, Pérez, Wiener

SENATE APPROPRIATIONS COMMITTEE: 7-0, 5/14/26
AYES: Cervantes, Seyarto, Cabaldon, Dahle, Grayson, Richardson, Wahab

SUBJECT: Money laundering: digital financial assets

SOURCE: Department of Justice

DIGEST: This bill expands the crime of money laundering to include transactions involving digital financial assets, as defined, and establishes a process for the forfeiture of digital financial assets that contain the proceeds of crime or that have been used to facilitate crime, as provided.

ANALYSIS:

Existing law:

- 1) The Digital Financial Assets Law (DFAW), generally governs the digital financial asset business activity of a person doing business in California or, wherever located, who engages in or holds itself out as engaging in the activity with, or on behalf of a resident, except for activity by several specified entities. (Finance (Fin.) Code, §§ 3101 et. seq.)
- 2) Defines “digital financial asset” and “digital financial asset business activity” for the purposes of DFAW. (Fin. Code, § 3102, subds. (g), (i).)
- 3) Provides that, beginning July 1, 2025, a person shall not engage in digital financial asset business activity, or hold itself out as being able to engage in

digital financial asset business activity, with or on behalf of a resident of the state unless any of the following is true:

- a) The person is licensed in this state by the Department of Financial Protection and Innovation (DFPI).
 - b) The person has submitted a timely application for a license and is awaiting a decision.
 - c) The person is exempt from licensure, as provided. (Fin. Code, § 3201; *see id.*, §§ 3201-3225.)
- 4) Authorizes the DFPI to take an enforcement measure, as defined, against a licensee or person that is not a licensee but has engaged, is engaging, or is about to engage in digital financial asset business activity with, or on behalf of, a resident in several specified instances. (Fin. Code, § 3403.)
 - 5) Defines “criminal profiteering” as an act committed or attempted or a threat made for financial gain or advantage, which act or threat may be charged as a crime under several specified criminal statutes, including as embezzlement, extortion, receiving stolen property, violation of laws governing corporate securities, money laundering, offenses relating to unauthorized access to computers, computers systems, or computer data, and several others. (Penal (Pen.) Code, §186.2)
 - 6) Provides that in any case in which a person is alleged to have been engaged in a pattern of criminal profiteering activity, as defined, upon a conviction of the underlying offense, the assets specified assets shall be subject to forfeiture upon proof of the profiteering activity. (Pen. Code, §186.3, subd. (a).)
 - 7) Sets forth requirements and procedures regarding a forfeiture action filed by the prosecution resulting from criminal profiteering crimes. (Pen. Code, §§ 186.4 – 186.8.)
 - 8) Provides that any person who conducts or attempts to conduct a transaction or more than one transaction within a seven-day period involving a monetary instrument or instruments of a total value exceeding \$5,000, or a total value exceeding \$25,000 within a 30-day period, through one or more financial institutions (1) with the specific intent to promote, manage, establish, carry on, or facilitate the promotion, management, establishment, or carrying on of any criminal activity, or (2) knowing that the monetary instrument represents the proceeds of, or is derived directly or indirectly from the proceeds of, criminal

activity, is guilty of the crime of money laundering. (Pen. Code, § 186.10, subd. (a).)

- 9) Provides that the aggregation periods do not create an obligation for financial institutions to record, report, create, or implement tracking systems or otherwise monitor transactions involving monetary instruments in any time period. (*Ibid.*)
- 10) Provides that in consideration of the constitutional right to counsel afforded by the Sixth Amendment to the United States Constitution and Section 15 of Article I of the California Constitution, when a case involves an attorney who accepts a fee for representing a client in a criminal investigation or proceeding, the prosecution shall additionally be required to prove that the monetary instrument was accepted by the attorney with the intent to disguise or aid in disguising the source of the funds or the nature of the criminal activity. (*Ibid.*)
- 11) Provides that a violation of this statute shall be punished by imprisonment in a county jail for not more than one year or as a realigned felony, by a fine of not more than \$ 250,000 or twice the value of the property transacted, whichever is greater, or by both that imprisonment and fine. However, for a second or subsequent conviction for a violation of this section, the maximum fine that may be imposed is \$500,000 or five times the value of the property transacted, whichever is greater. (*Ibid.*)
- 12) Provides that, for the purposes of this statute, each individual transaction conducted in excess of \$5,000, each series of transactions conducted within a seven-day period that total in excess of \$5,000, or each series of transactions conducted within a 30-day period that total in excess of \$25,000, shall constitute a separate, punishable offense. (Pen. Code, § 186.10, subd. (b).)
- 13) Provides that in any instance where money laundering is punished as a felony, the defendant shall be subject to additional terms of imprisonment depending on the value of the transaction or transactions. (Pen. Code, § 186.10, subd. (c)(1).)
- 14) Specifies that any additional term of imprisonment shall not be imposed unless the facts of a transaction or transactions, or attempted transaction or transactions, of the alleged value, are charged in the accusatory pleading, and are either admitted to by the defendant or are found to be true by the trier of fact. (Pen. Code, § 186.10, subd. (c)(2).)

This bill:

- 1) Expands the existing money laundering statute to include the use of digital financial assets, specifically providing that any person who conducts or attempts to conduct a transaction or more than one transaction within a seven-day period involving a monetary instrument or instruments of a total value exceeding \$5,000, or a total value exceeding \$25,000 within a 30-day period using any digital financial asset, either with the specific intent to promote, manage, establish, carry on, or facilitate the promotion, management, establishment, or carrying on of any criminal activity, or knowing that the monetary instrument represents the proceeds of, or is derived directly or indirectly from the proceeds of, criminal activity, is guilty of the crime of money laundering.
- 2) Authorizes a law enforcement officer or public prosecutor to obtain a search warrant to seize digital financial assets or wallets, accounts, or similar things containing digital financial assets (collectively “digital financial assets”) upon a showing of probable cause that the assets either contain or have contained the proceeds of a crime, are traceable to a crime, or have been used to facilitate crime.
- 3) Provides that the warrant application shall specify any centralized exchanges, addresses, or other locations assets from which digital financial assets will be seized. The affidavit shall describe how the warrant will be served, such as delivery to a known law enforcement portal of a centralized exchange, digital financial assets issuer, or via some other method. The search warrant shall specify the amount of digital financial assets to be seized from each location, subject to the following:
 - a) The search warrant may authorize seizure of either all digital financial assets where money laundering can be shown or digital financial assets up to the amount of proceeds received, the amount of digital financial assets used to facilitate crime, or the amount of digital financial assets traceable to crime, in other cases.
 - b) The search warrant may authorize seizure of digital financial assets related to crimes and victims in other jurisdictions so long as jurisdiction relating to a California crime is established.
 - c) The search warrant may authorize seizure of substitute assets if the target disposed of the relevant digital financial assets.

- 4) Authorizes a law enforcement officer to send a written request to freeze digital financial assets to allow time to pursue a search warrant pursuant to this bill, and requires a centralized exchange, digital financial assets issuer, or other party receiving such a request to freeze the relevant digital financial assets for ten calendar days from receipt of the request. The centralized exchange, digital financial assets issuer, or other party may, but is not required to, notify the possessor of the digital financial assets that they have been frozen at the request of a California law enforcement agency.
- 5) Provides that the court shall issue a warrant where jurisdiction is established and probable cause appears in the affidavit. Upon issuance of the warrant, law enforcement shall execute the warrant by taking the digital financial assets into law enforcement custody for safekeeping or taking such other actions as are necessary to prevent the property from being transferred or dissipated.
- 6) Provides that within 180 days of any seizure of digital assets conducted pursuant to a warrant, a public prosecutor may initiate a special proceeding of a criminal nature by applying to the court on behalf of the People of the State of California to forfeit the seized digital financial assets, but if no such proceeding is initiated, and no other law prohibits the return, the seized digital financial assets may be returned to the party from whom it was seized, unless the period is extended by the court upon a showing of good cause.
- 7) Provides that if a special proceeding is initiated, the public prosecutor must make efforts reasonably calculated to provide notice to all readily ascertainable potential owners of such property, and anyone with a known security interest. Each person noticed has thirty days to file a verified claim to demonstrate that the funds were obtained by legitimate means. The thirty-day period begins on the date of service. The court shall not extend the time for filing a claim without good cause.
- 8) Provides that any resolution of disputed issues related to a claim shall be at a court hearing, and that the court may halt proceedings at any time if it determines that it has sufficient information to resolve the claim and issue an ordering resolving the validity of the claim, as specified.
- 9) Provides that after all claims are resolved, the court shall issue a final, unappealable judgement forfeiting the remaining digital financial assets, ownership of which shall immediately transfer to the prosecuting agency for distribution to the victims, as specified.

- 10) Requires the seized funds to be used to compensate victims of the crimes or fraud schemes underlying an action pursuant to this bill, up to the value of their actual loss, and authorizes the prosecuting agency to establish a claims procedure to include victims whose cases were not used to establish the underlying crimes or fraud schemes, subject to specified requirements.
- 11) Provides that any digital financial assets not distributed to victims as set forth above shall be kept in the custody of the law enforcement or prosecuting agency for a maximum of three years, upon which time the forfeited assets shall be distributed to the general fund of the jurisdiction that initiated the prosecution.
- 12) Provides that a special proceeding to recover digital financial assets may be filed in any county where any victim of the underlying crimes or fraud schemes resides or in any county where any portion of the crimes or underlying fraud schemes occurred, and may be prosecuted by a City Attorney, District Attorney, or the Attorney General.
- 13) Specifies that service of process may be made using one or more of the following methods:
 - a) If funds are seized from an account at a centralized exchange, notice by one of the following methods shall be deemed to be sufficient notice: email, mail, or telephone, as specified.
 - b) If funds are seized from a blockchain address, blockchain service may be made by sending a link to the documents using the blockchain involved in the seizure.
 - c) Upon a showing that none of the listed methods of service are possible or practical, the court shall permit service by publication, or in any other means provided by law.

Comments

Forfeiture generally follows one of two legal routes: criminal or civil. While all forfeitures are technically triggered by illegal conduct, they are classified as civil or criminal based on the type of procedure which ends in confiscation of the subject property. The law typically uses the term “seizure” to refer to the taking and holding of evidence that may be associated with a crime to use those items as proof in a later criminal trial. Cash proceeds from a drug deal, for example, may be “seized” at the time of a criminal arrest. Criminal asset forfeiture, by contrast, is typically done after the trial has resulted in a conviction. Forfeiture refers to the

process by which the cash proceeds are distributed to law enforcement and other entities within the jurisdiction. In civil forfeitures, the guilt or innocence of the property owner is irrelevant – it is enough that the property was involved in the unlawful behavior to which forfeiture attaches. Civil asset forfeiture has allowed the government to seize and keep cash, cars, real estate, and any other property suspected of being connected to criminal activity even if the owner is never convicted of a crime. For this reason, civil forfeiture schemes have drawn sharp criticism, with critics arguing that such schemes disproportionately impact the poor, violate various constitutional guarantees and the presumption of innocence, and incentivize law enforcement overreach and unjust enrichment.

The California Control of Profits of Organized Crime Act (hereinafter, “CPOC”) sets forth the asset forfeiture procedure for property and proceeds acquired through a pattern of criminal profiteering activity. Under CPOC, the prosecuting agency can seek forfeiture of any property interest whether tangible (such as buildings, real property, and vehicles) or intangible (such as life insurance policies and shares of a company) acquired directly or indirectly through a pattern of criminal profiteering activity and all of the proceeds of a pattern of criminal profiteering activity, including all things of value that may have been received in exchange for the proceeds immediately derived from the pattern of criminal profiteering activity. Typically, the forfeited assets are distributed to the State’s General Fund, and/or the local governmental entity, whichever prosecutes, and existing law provides little to no direction for the use of such funds.

This bill establishes a comprehensive asset forfeiture process – loosely modeled after CPOC – for digital financial assets that contain or have contained the proceeds of a crime or proceeds traceable to a crime or that have been used to facilitate crime. Under this process, a law enforcement or prosecuting agency may obtain a search warrant to seize digital financial assets, provided the search warrant application and affidavit include specified information. The scope of the warrant may include all digital assets where money laundering can be shown, assets up to the amount of proceeds received, the amount used to facilitate crime, or the amount traceable to a crime, or assets related to crimes and victims in other jurisdictions as long as jurisdiction related to California is established.

Under the bill, law enforcement or prosecuting agencies may send a request to have digital assets frozen pending the issuance of the search warrant permitting seizure, at which point the agency must execute the warrant and seize the assets. Within 180 days of this seizure, the prosecutor may initiate a forfeiture action regarding the seized assets, and the bill establishes a claim process whereby claimants may appeal to the court that the seized assets belong to the claimant and

were obtained by legitimate means. After these claims are resolved at a court hearing, ownership of the forfeited assets transfers to the prosecuting agency, which is required to distribute the assets to victims of the crimes underlying the forfeiture action or other victims it identifies. The bill also specifies that a forfeiture action may be filed in any county where any victim resides or in any county where any portion of the underlying crimes occurred, and may be prosecuted by a city attorney, a district attorney, or the Attorney General. Finally, the bill specifies how service of process may be made upon a centralized cryptocurrency exchange or a blockchain address holding the seizable assets.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: Yes

According to the Senate Appropriations Committee:

Unknown court cost pressures to adjudicate money laundering offenses involving digital financial assets (Trial Court Trust Fund, General Fund).

Unknown incarceration costs to the Department of Corrections and Rehabilitation as money laundering is punishable as a felony. There may be few, if any, physical arrests due to the nature of digital financial fraud (General Fund).

SUPPORT: (Verified 5/14/26)

California Department of Justice (source)
Arcadia Police Officers' Association
Brea Police Association
Burbank Police Officers' Association
California Association of School Police Chiefs
California Bankers Association
California Coalition of School Safety Professionals
California Community Banking Network
California Credit Union League
California Narcotic Officers' Association
California Police Chiefs Association
California Reserve Peace Officers Association
Claremont Police Officers Association
Corona Police Officers Association
Culver City Police Officers' Association
Fullerton Police Officers' Association
Little Hoover Commission

Los Angeles School Police Management Association
Los Angeles School Police Officers Association
Murrieta Police Officers' Association
Newport Beach Police Association
Palos Verdes Police Officers Association
Placer County Deputy Sheriffs' Association
Pomona Police Officers' Association
Riverside County District Attorney
Riverside Police Officers Association
Riverside Sheriffs' Association

OPPOSITION: (Verified 5/14/26)

California Public Defenders Association

Prepared by: Alex Barnett / PUB. S. /
5/18/26 15:24:03

**** **END** ****