SENATE COMMITTEE ON PUBLIC SAFETY

Senator Jesse Arreguín, Chair
2025 - 2026 Regular

Bill No:	SB 1208	**Hearing Date:**	April 21, 2026
Author:	Grayson		
Version:	April 6, 2026		
Urgency:	No	**Fiscal:**	Yes
Consultant:	AB		

Subject: ***Money laundering: digital financial assets***

HISTORY

Source: Department of Justice

Prior Legislation: AB 1934 (Grayson), Ch. 945, Stats. of 2024
SB 401 (Limon), Ch. 871, Stats. of 2023
AB 76 (Davies), died in Senate Appropriations, 2023
AB 39 (Grayson), Ch. 792, Stats. of 2023
AB 2269 (Grayson), vetoed, 2022

Support: Arcadia Police Officers' Association; Brea Police Association; Burbank Police Officers' Association; California Association of School Police Chiefs; California Coalition of School Safety Professionals; California Department of Justice; 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; 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 Police Officers Association Riverside Sheriffs' Association

Opposition: California Public Defenders Association

PURPOSE

The purpose of this bill is to expand the crime of money laundering to include transactions involving digital financial assets, as defined, and to establish 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.

Existing law, 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. (Fin. Code, §§ 3101 et. seq.)

Existing law defines "digital financial asset" as a digital representation of value that is used as a medium of exchange, unit of account, or store of value, and that is not legal tender, whether or not denominated in legal tender, but does not include any of the following:

- A transaction in which a merchant grants, as part of an affinity or rewards program, value that cannot be taken from or exchanged with the merchant for legal tender, bank or credit union credit, or a digital financial asset.
- A digital representation of value issued by or on behalf of a publisher and used solely within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform.
- A security registered with or exempt from registration with the United States Securities and Exchange Commission or a security qualified with or exempt from qualifications with the department. (Fin. Code, § 3102, subd. (g).)

Existing law defines "digital financial asset business activity" as any of the following:

- Exchanging, transferring, or storing a digital financial asset or engaging in digital financial asset administration, whether directly or through an agreement with a digital financial asset control services vendor.
- Holding electronic precious metals or electronic certificates representing interests in precious metals on behalf of another person or issuing shares or electronic certificates representing interests in precious metals.
- Exchanging one or more digital representations of value used within one or more online games, game platforms, or family of games for either of the following:
    - A digital financial asset offered by or on behalf of the same publisher from which the original digital representation of value was received.
    - Legal tender or bank or credit union credit outside the online game, game platform, or family of games offered by or on behalf of the same publisher from which the original digital representation of value was received. (Fin. Code, § 3102, subd. (i).)

Existing law 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:

- The person is licensed in this state by the Department of Financial Protection and Innovation (DFPI).
- The person has submitted a timely application for a license and is awaiting a decision.
- The person is exempt from licensure, as provided. (Fin. Code, § 3201; *see id.*, §§ 3201-3225.)

Existing law 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.)

Existing law authorizes the DFPI to assess civil penalties against licensees and non-licensed persons who engage in digital financial asset business activity in violation of the DFAW, as provided. (Fin. Code, § 3407.)

Existing law defines a "search warrant" as a written order in the name of the people, signed by a magistrate, directed to a peace officer, commanding him or her to search for a person or persons, a thing or things, or personal property, and, in the case of a thing or things or personal property, bring the same before the magistrate. (Pen. Code, § 1523.)

Existing law authorized a search warrant to be issued on one of several specified grounds. (Pen. Code, § 1524.)

Existing law 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. (Pen. Code, §186.2)

Existing law 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).)

Existing law sets forth requirements and procedures regarding a forfeiture action filed by the prosecution resulting from criminal profiteering crimes. (Pen. Code, §§ 186.4 – 186.8.)

Existing law, for the purpose of California's criminal money laundering statute, defines the following terms:

- "Conduct" includes, but is not limited to, initiating, concluding, or participating in conducting, initiating, or concluding a transaction.

- "Financial institution" includes, when located or doing business in this state, a national bank, state bank, savings and loan association, foreign bank, brokers or dealers in registerable securities, businesses dealing with money orders, investment bankers, insurers, gold or other specified mineral dealers, pawnbrokers, persons involved in transferring titles of real estate and certain other properties, and specified gambling establishments, among other things. (Pen. Code, § 186.9.)

- "Transaction" includes the deposit, withdrawal, transfer, bailment, loan, pledge, payment, or exchange of currency, or a monetary instrument, or the electronic, wire, magnetic, or manual transfer of funds between accounts by, through, or to, a financial institution.

- "Monetary instrument" includes, among other things, any currency or coin, bank check, cashier's check, money order, stock, investment security, gold and other specified minerals. This definition does not include specified personal checks.

- "Criminal activity" means a criminal offense punishable by death, state prison, imprisonment in county jail pursuant to criminal justice realignment, or an offense committed in another jurisdiction punishable by death or a term of imprisonment exceeding one year.

Existing law 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).)

Existing law 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.*)

Existing law 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.*)

Existing law 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.*)

Existing law 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).)

Existing law 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).)

Existing law 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 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.

This bill 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 meet either of the following:

- Contain or have contained the proceeds of a crime or proceeds traceable to a crime.
- Have been used to facilitate crime.

This bill 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:

- 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.
- 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.
- The search warrant may authorize seizure of substitute assets if the target disposed of the relevant digital financial assets.

This bill 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.

This bill 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.

This bill 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.

This bill 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. The thirty-day period begins on the date of service. The court shall not extend the time for filing a claim without good cause.

This bill provides that a verified claim must be filed under penalty of perjury and supported by admissible evidence. The claimant bears the burden by a preponderance of the evidence to show that the seized digital financial assets belong to the claimant and were obtained by legitimate means.

This bill provides that the claim must include specified identifying information regarding the claimant, including a photograph of the claimant and of an identity document, as specified, and must respond to all allegations in the petition for forfeiture and be supported by the evidence upon which the claimant intends to rely.

This bill provides that all evidence and arguments not included in the initial claim are forfeited, absent a finding of good cause by the court.

This bill specifies that upon filing of a claim, unless it is denied as plainly without merit, the court shall give the prosecuting agency time to file a response with any additional evidence and argument related to the claim, and, considering all relevant evidence, shall decide the claim and file an order resolving the claim or setting a hearing.

This bill 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.

This bill 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.

This bill specifies that the government's interest in distribution to victims shall take precedence over individual claims based on constructive trust or other civil claims that individual victims may assert.

This bill 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 the following requirements:

- The agency shall make efforts reasonably calculated to identify and provide notice to additional victims of the crimes or fraud schemes underlying the action and inform them of the procedure to file a claim.

- After the expiration of the claims period, the prosecuting agency shall grant or deny each claim and determine the amount of each victim's loss for approved claims. Determinations are not subject to appeal or judicial review.
- Once all additional claims are adjudicated, the prosecuting agency must distribute the seized digital financial assets to those victims whose cases were used as part of the action and those additional victims whose claims are approved on a pro rata basis up to the amount of their actual loss.

This bill provides that if a prosecuting agency determines that a claims procedure to identify additional victims is inappropriate or impractical, the agency shall still be required to return funds to all victims whose cases were used as part of this action on a pro rata basis up to the amount of the actual loss.

This bill 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.

This bill includes a statement of legislative intent that jurisdiction extends to digital financial assets in any country when either of the following have been established:

- The possessor received a digital financial asset traceable to a crime perpetrated against a victim who was residing in the State of California or was defrauded in the State of California.
- The possessor is a member of a conspiracy to commit money laundering and any member of the conspiracy received a digital financial asset traceable to a crime perpetrated against a victim who was residing in the State of California or defrauded while in the State of California.

This bill 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.

This bill specifies that service of process may be made using one or more of the following methods:

- 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.
- 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.
- 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.

This bill includes various legislative findings and declarations.

COMMENTS

1. Need for This Bill

According to the author:

> SB 1208 is an important bill in California's fight against consumer fraud and scams. Criminal organizations, especially transnational organizations, use digital financial assets in their complex schemes to defraud Californians and to launder the proceeds from their criminal activities. Using blockchain analysis, law enforcement agencies can track the movement of digital financial assets and work with digital asset custodians to freeze funds. Existing state law, however, requires a criminal conviction to effect forfeiture of fraud proceeds, a hurdle that is nearly impossible to clear when the alleged criminal is located overseas in a jurisdiction that does not cooperate with U.S. law enforcement agencies.

2. California's Digital Financial Asset Law

The last 10 years has seen the explosive growth of so-called "cryptocurrencies" from a niche technology to a multi-billion dollar asset class, outpacing traditional regulatory frameworks and raising significant questions about how to adapt criminal and banking laws to address these new digital currencies. Accordingly, between 2023 and 2024, the Legislature passed a trio of bills that together comprise California's Digital Financial Asset Law (DFAL), which creates a robust licensing and enforcement framework for certain cryptocurrency activities.[1] Broadly speaking, a "digital financial asset" is a digital representation of value that is not issued or backed by a government or central bank, and of which cryptocurrencies are a primary subset.[2]

Beginning July of 2026, the DFAL requires companies to be licensed by the Department of Financial Protection and Innovation (DFPI) or have applied for a license in order to engage in digital financial asset business activity, which refers to providing services that involve the exchange, transfer, storage or issuance of digital financial assets on behalf of others.[3] Entities not licensed by the DFPI are prohibited from engaging in digital financial asset business activity, and DFAL authorizes the DFPI to conduct on-site or remote examinations of licensees, suspend licenses or impose stiff civil penalties on non-compliant licensees, and conduct specified enforcement actions against non-licensees who engage in digital financial asset business activity.[4] The DFAL imposes extensive obligations on licensees regarding consumer disclosures, cybersecurity and data protection requirements, and minimum capital and liquidity requirements to mitigate financial risk. The law also contains specific consumer protection provisions for cryptocurrency kiosk operators, including transaction limits designed to deter money laundering.[5]

---

[1] AB 39 (Grayson) Ch. 792, Stats. of 2023, SB 401 (Limon) Ch. 871, Stats. of 2023, and AB 1934 (Grayson), Ch. 945, Stats. of 2024, codified at Fin. Code, §§ 3101 et. seq.

[2] These assets are often stored in a digital ledger known as the "blockchain," which is a computerized database that uses a decentralized network (known as a "consensus mechanism") to secure transaction records, control the creation of new assets, and verify the transfer of asset ownership.

[3] Fin. Code, §§ 3102, subd. (i), 3201, et. seq.,

[4] Fin. Code, § 3401 et. seq.

[5] Fin. Code, §§ 3901 et. seq. "Crypto kiosks" are essentially ATMs that accept or dispense cash in exchange for cryptocurrency.

The author contends that more tools are needed to combat the increasing prevalence of crypto-related frauds, scams and other similar financial crimes. The statistics seems to bear this out: the FBI's annual internet crimes report for 2024 underscores that "cryptocurrency has become an enticing means to cheat investors, launder proceeds, and engage in other illicit schemes," and tallied nearly 150,000 crypto-related complaints that year, with total crypto-related losses totaling roughly $9.3 billion.[6] California ranked at the top of the list for most crypto-related complaints and financial losses of any state with 19,508 complaints and $1.4 billion in losses.[7] One specific scam, known as "pig butchering," wherein scammers gain the trust of victims to induce them to transfer crypto funds into fake projects, resulted in over $75 billion in crypto assets stolen and laundered between 2021 and 2024, much of it flowing to criminal enterprises.[8] Accordingly, this bill seeks to establish new criminal penalties for nefarious conduct involving cryptocurrency and other digital financial assets by adapting two well-established legal frameworks: California's money laundering and criminal profiteering statutes.

3. Money Laundering

Generally, money laundering describes the process of illegally concealing the origin of money obtained from illicit activities to make the source of such funds appear legitimate. However, California's anti-money laundering statute prohibits more than simply attempting to conceal the nature of ill-begotten assets. Penal Code section 186.10 criminalizes the act of conducting or attempting to conduct one or more financial transaction through a financial institution involving one or more monetary instruments with a value of at least $5,000 within a 7- day period (or $25,000 within a 30 day period) when the defendant either 1) has the specific intent to promote criminal activity or 2) knows that the funds are the proceeds of criminal activity. Existing law defines "monetary instrument" as United States and foreign currency, checks, money orders, gold, silver, platinum, specified gemstones, stocks, bearer bonds, investment securities, and other types of financial assets.[9] The crime of money laundering is punishable as an alternate misdemeanor/felony, and the statute provides for several sentencing enhancements when the underlying crime is punished as a felony and the value of the transactions meets specified thresholds.[10]

This bill expands section 186.10 to include transactions or attempted transactions involving digital financial assets, as defined in DFAL. The bill does not require that such transactions be attempted or completed through a financial institution, likely due to the fact that cryptocurrency transactions largely occur outside the traditional banking system and are instead traded on "cryptocurrency exchanges," which act as a marketplace for digital assets, similar to a stock exchange.[11] The bill's incorporation of digital financial asset transactions into the money laundering statute does raise a question regarding the application of the statute's tiered enhancement scheme, which delineates the tiers based on the dollar value of assets transacted. Specifically, because the dollar value of a given cryptocurrency fluctuates based on several factors (market sentiment, supply and demand, etc.) and can experience significant volatility

---

[6] "Federal Bureau of Investigation: Internet Crime Report 2024." *Federal Bureau of Investigation, Internet Crime Complaint Center*. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf, pp. 3, 35-38.
[7] *Ibid,* pp.39-40
[8] Griffin, John and Kevin Mei. "How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering." 28 March 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4742235
[9] Pen. Code, § 186.9, subd. (d).
[10] Pen. Code, § 186.10, subd. (c).
[11] "What are crypto exchanges and how do they work?" *Forbes*. 5 November 2024. https://www.forbes.com/advisor/in/investing/cryptocurrency/what-is-a-crypto-exchange/

even over a short time period, how will the value of such assets be determined for the purposes of section 186.10's sentencing enhancements. Should it be dollar value at the time of the transaction? Or dollar value at the time of the prosecution? Imagine a cryptocurrency transaction in which a quantity of 60 Coin X, valued at $60,000, is laundered and subject to prosecution under section 186.10, but at the time charges are filed, the value of 60 Coin X has reached $160,000, and at the date of conviction, the value of the assets totals $1.2 million. For the purposes of sentencing, has $60,000, $160,000, or $1.2 million been laundered?

4. Forfeiture Actions for Digital Financial Assets

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.[12]

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.[13] 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.[14] 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.[15]

In any CPOC case in which a person is alleged to have been engaged in a pattern of criminal profiteering activity, assets are subject to forfeiture when the defendant has been convicted of at least two offenses from a list of more than thirty that qualify for prosecution under the statute. Thus, the forfeiture process under CPOC represents a criminal asset forfeiture scheme, as opposed to civil asset forfeiture. This process additionally requires a forfeiture hearing to be held

[12] "Civil asset forfeiture: Unfair, undemocratic, and un-American." *Southern Poverty Law Center*. 30 October 2017. https://www.splcenter.org/resources/reports/civil-asset-forfeiture-unfair-undemocratic-and-un-american/ ; Forbes, Steve. "Policing For Profit: The Case Against Civil Asset Forfeiture." *Forbes*. 25 February 2026. https://www.forbes.com/sites/steveforbes/2026/02/25/policing-for-profit-the-case-against-civil-asset-forfeiture/
[13] Pen. Code, §§ 186-186.8.
[14] Pen. Code, § 186.3.
[15] Pen. Code, § 186.8.

in conjunction with the trial of the underlying criminal offense, which is generally heard by the same court and/or jury hearing the criminal trial and requires the prosecutor to prove beyond a reasonable doubt that the defendant was engaged in criminal profiteering activity.[16] The CPOC process also allows parties claiming interest in the property or proceeds subject to forfeiture to submit a verified claim to the court stating an interest in the property, and if such claims are valid, allows these parties to receive a disbursement from the forfeiture proceeds.

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.

Because the forfeiture process proposed by this bill happens without a criminal conviction and permits the seizure of digital financial assets upon a showing of probable cause (as opposed to the much higher burden of beyond a reasonable doubt), it is functionally a civil asset forfeiture scheme. The bill's findings and declaration provide a justification for such an approach:

> Transnational criminal organizations are targeting California residents with sophisticated internet scams using cryptocurrency to steal and launder the fraud proceeds [and] often operate from countries with limited diplomatic cooperation and are protected by government corruption. Many organizations engage in human trafficking so that the person committing the scam is actually the victim of the criminal enterprise. Given all of these challenges, California state and local law enforcement have limited ability to identify the individual perpetrator, extradite them, and obtain a criminal conviction.

[16] Pen. Code, § 186.5.

Given the challenges associated with prosecuting entities engaged in cryptocurrency frauds and scams, a civil forfeiture approach may indeed be the only method of providing restitution to the victims of such criminal enterprises. Nevertheless, the Committee should be mindful of the aforementioned criticism leveled at civil forfeiture schemes (see page 10, supra).

The bill raises several other questions that the author and Committee may wish to consider. First, the bill provides that a warrant for digital financial assets may authorize seizure of "substitute assets," but does not define this term or impose any requirement that there be some nexus between the substitute assets and the original target assets. Such a requirement may be beneficial to ensure that only assets related to criminal activity are seized. Second, the bill provides that any digital financial assets not distributed to victims are to be kept in the custody of the law enforcement or prosecuting agency for a maximum of three years, but does not specify any further disposition of the assets. Should the bill specify the ultimate disposition of the funds, such as liquidation and distribution to the general fund of a local government, or that of the State? Finally, the bill provides that if the funds are seized form a blockchain address, "blockchain service" may be made by sending a link to the documents using the blockchain involved in the seizure. Although the term "blockchain" is well understood in the context of cryptocurrency transactions, it is not defined in this bill, and only once elsewhere in California statute.[17] Given the property interests at stake in this bill, and the importance of legally sound service of process procedures, including a definition of "blockchain," even via cross-reference, may be beneficial.

5. Prior Legislation

The provision of this bill incorporating digital financial assets into California's anti-money laundering statute is similar to a past effort to enact such a regulation. AB 76 (Davies), introduced in 2023, would have modified the definition of "monetary instrument" for the purposes of section 186.10 to include "digital assets that use blockchain technology." However, that measure was advanced prior to the enactment of DFAL, and therefore did not include definitional cross-references to that law. The construction advanced in this bill represents a much more statutorily efficient approach.

6. Argument in Support

According to the California Police Chiefs Association:

> Under current law, law enforcement agencies are increasingly encountering sophisticated criminal enterprises that exploit gaps in statute—particularly in the rapidly evolving area of digital assets. Transnational criminal organizations, including major drug cartels, are now leveraging cryptocurrency as a tool to move and conceal illicit proceeds at a scale and speed that traditional financial systems cannot match.
>
> Recent analysis has shown that cartels such as the Sinaloa Cartel have experimented with and adopted cryptocurrency to launder proceeds from narcotics trafficking, using networks of crypto ATMs, peer-to-peer brokers, and

[17] Health and Safety Code, § 103526.5 defines "blockchain technology" as "a decentralized data system, in which the data stored is mathematically verifiable, that uses distributed ledgers or databases to store specialized data in the permanent order of transactions recorded."

exchanges to convert bulk cash into digital assets and move funds across borders with reduced detection. These organizations also use cryptocurrency to obfuscate financial trails, making it significantly more difficult for law enforcement to identify, trace, and interdict illicit proceeds. In some cases, cartel-linked money laundering schemes have relied on digital currencies as a "critical conduit" to move millions of dollars tied to organized crime.

At the same time, illicit cryptocurrency activity is growing globally, with billions of dollars flowing through criminal networks annually, underscoring the urgent need for modernized enforcement tools. SB 1208 represents a necessary and forward-looking response to these threats. By clarifying and strengthening statutory authorities related to digital assets, this bill will provide law enforcement with the tools needed to investigate, trace, and disrupt cryptocurrency-based money laundering and other financial crimes. Importantly, enhanced legal clarity will allow agencies to better leverage blockchain intelligence tools—capabilities that have proven essential in identifying criminal networks, tracing illicit funds across jurisdictions, and supporting successful prosecutions.

7. Argument in Opposition

According to the California Public Defender's Association:

While framed as a technical update, the bill materially expands money laundering liability in a way that risks overcriminalizing low-level conduct without meaningfully improving public safety. In practice, digital financial assets are increasingly used in informal, low-dollar transactions, particularly among "unbanked" or indigent individuals. According to an article in *CalMatters*, "1 in 4 Californians lacks full access to banks, studies say…..Being unbanked greatly impacts people of color and low-income families. Nearly 1 in 2 Black and Latino households in California is unbanked or underbanked, state officials said." Additionally, the federal government has compounded the issue of being "unbanked" by systematically cancelling immigrants Social Security Numbers leaving them without access to their bank accounts or other assets in an effort to make them "self-deport".

By extending money laundering statutes into this space, SB 1208 collapses the distinction between underlying offenses and secondary financial conduct, exposing individuals to additional felony liability for behavior that is already fully captured by existing criminal statutes. In other words, under SB 1208 an individual who sells one bag of heroin to a buyer and accepts digital currency could be charged with both the drug sales and money laundering. Similarly, a sex worker who accepts digital currency from a customer could be charged with both solicitation and money laundering.

Two common scenarios more fully illustrate this concern. First, in low-level narcotics cases, digital payments are often used simply as a substitute for cash. A series of modest transactions—none of which would independently justify a laundering charge—can now be aggregated to meet statutory thresholds, transforming routine conduct into a separate felony with enhancements. Second,

in low-level prostitution cases, particularly those historically associated with online platforms, digital payments may be used for discretion or accessibility rather than concealment. SB 1208 allows ordinary receipt and transfer of funds in these contexts to be reframed as "facilitating" criminal activity, effectively layering additional charges onto already prosecuted conduct without requiring meaningful evidence of concealment or sophistication.

-- END --