Date of Hearing: June 9, 2026
Counsel: Dustin Weber

ASSEMBLY COMMITTEE ON PUBLIC SAFETY
Nick Schultz, Chair

SB 1208 (Grayson) – As Amended May 14, 2026

SUMMARY: Authorizes a law enforcement officer or prosecuting agency to obtain a search warrant to seize digital financial assets upon a showing of probable cause that the digital financial assets contain proceeds of a crime or proceeds traceable to a crime or have been used to facilitate a crime. Specifically, **this bill**:

1) Expands the crime of money laundering to include the use of digital financial assets, as defined.

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 meet either of the following:

   a) Contain or have contained the proceeds of a crime or proceeds traceable to a crime.

   b) Have been used to facilitate a crime.

3) States 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.

4) Provides that 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:

      i) 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

      ii) 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.

5) 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.

6) Authorizes the centralized exchange, digital financial assets issuer, or other party to notify the possessor of the digital financial assets that they have been frozen at the request of a California law enforcement agency.

7) Provides that the court shall issue a warrant where jurisdiction is established and probable cause appears in the affidavit.

8) Requires law enforcement, upon issuance of the warrant, to 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.

9) States 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.

10) 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.

11) States that a verified claim must be filed under penalty of perjury and supported by admissible evidence, and that 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.

12) Establishes 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.

13) Provides that all evidence and arguments not included in the initial claim are forfeited, absent a finding of good cause by the court.

14) 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.

15) States 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.

16) Provides 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.

17) 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.

18) 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:

    a) 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.

    b) 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.

    c) 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.

19) States 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.

20) Establishes 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.

21) States that jurisdiction extends to digital financial assets in any country when either of the following have been established:

    a) The possessor received a digital financial asset traceable to a crime perpetrated against a victim who was residing in California or was defrauded in this state.

b) 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 California or defrauded while in this state.

22) 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.

23) 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.

24) Includes legislative findings and declarations.

EXISTING LAW:

1) 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, and known as the Digital Financial Assets Law (DFAL). (Fin. Code, § 3101 et. seq.)

2) Provides that, as of July 1, 2026, 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.)

3) 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, as specified. (Fin. Code, § 3403.)

4) Authorizes the DFPI to assess civil penalties for digital financial asset business activity in violation of the DFAL, as provided. (Fin. Code, § 3407.)

5) Authorizes a search warrant to be issued on specified grounds. (Pen. Code, § 1524.)

6) States 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, 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) States 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. (Pen. Code, § 186.10, subd. (a).)

10) Punishes violations of the money laundering statute by imprisonment in a county jail for not more than one year or as a realigned felony punishable by imprisonment for 16 months, two years, or three years, 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. (Pen. Code, § 186.10, subd. (a).)

11) 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).)

12) States 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).)

13) 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).

14) 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. (Health & Saf. Code, § 103526.5.)

15) 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) 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.

    b) 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.

    c) 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).)

16) Defines "digital financial asset business activity" as any of the following:

    a) 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.

    b) 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.

    c) 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:

        i) A digital financial asset offered by or on behalf of the same publisher from which the original digital representation of value was received.

        ii) 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).)

17) 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.)

18) 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)

19) Defines "conduct" as including, but not being limited to, initiating, concluding, or participating in conducting, initiating, or concluding a transaction. (Pen. Code, § 186.9, subd. (a).)

20) Defines "financial institution" to include, 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, subd. (b).)

21) Defines "transaction" to include 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. (Pen. Code, § 186.9, subd. (c).)

22) Defines "monetary instrument" to include, among other things, United States 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. (Pen. Code, § 186.9, subd. (d).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Sponsor**: California Department of Justice.

2) **Author's Statement**: 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.

   "This bill helps to remedy the challenges posed by existing law in returning assets to scam victims. The bill establishes a process whereby California law enforcement agencies can issue a warrant to seize funds when they have reasonable cause and administer a fair process for the owner of the funds to show that the assets were not related to criminal activities. While more needs to be done from stopping these criminals from reaching Californians in the first place, this is a critical bill to improve the outcomes for victims of fraud and scams."

3) **Effect of the Bill:** SB 1208 would update the money laundering statute to include digital financial assets. It would additionally create a statutory framework to seize and force forfeiture of digital financial assets under specified conditions.

Between 2023 and 2024, the Legislature passed a trio of bills that together comprise California's DFAL, which creates a robust licensing and enforcement framework for certain cryptocurrency activities. (AB 39 (Grayson), Ch. 792, Stats. 2023, SB 401 (Limon), Ch. 871, Stats. 2023, and AB 1934 (Grayson), Ch. 945, Stats. 2024, codified at Fin. Code, § 3101 et. seq.) A "digital financial asset" is generally a digital representation of value that is not issued or backed by a government or central bank, of which cryptocurrencies are a primary subset. (Fin. Code, § 3102, subd. (g).)[1] These assets are often stored in a digital ledger known as the "blockchain," which California law defines 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." (Health & Saf. Code, § 103526.5.)

Beginning July 1, 2026, the DFAL requires companies to be licensed by the DFPI or have applied for a license 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. (Fin. Code, §§ 3102, subd. (i), 3201, et. seq.) 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. (Fin. Code, § 3401 et. seq.) The law also contains specific consumer protection provisions for cryptocurrency kiosk operators, including transaction limits designed to deter money laundering. (Fin. Code, § 3901 et. seq.) "Crypto kiosks" are effectively ATMs that accept or dispense cash in exchange for cryptocurrency.[2]

Layered atop this background is SB 1208, which establishes a relatively comprehensive asset forfeiture process for digital financial assets. Under this process, a law enforcement or prosecuting agency may obtain a search warrant to seize digital financial assets. 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. 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.

---

[1] See also *Cryptocurrency, Digital or Virtual Currency and Digital Assets 2025 Legislation* (Sept. 11, 2025) National Conference of State Legislatures <https://www.ncsl.org/financial-services/cryptocurrency-digital-or-virtual-currency-and-digital-assets-2025-legislation> [as of June 3, 2026].

[2] *Your Bitcoin on Every Block: An Introduction to Cryptocurrency Kiosks* (May 4, 2022) National Association of Attorneys General <https://www.naag.org/attorney-general-journal/your-bitcoin-on-every-block-an-introduction-to-cryptocurrency-kiosks/> [as of June 3, 2026].

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 higher burden of beyond a reasonable doubt, it is functionally a civil asset forfeiture scheme. Various policy and legal concerns have been levied against civil asset forfeiture schemes. This is discussed in more detail below.

The author contends that more tools are needed to combat the increasing prevalence of crypto-related frauds, scams, and other similar financial crimes. Data suggests continued challenges exist to address digital financial crime. The Federal Bureau of Investigation's (FBI) annual internet crimes report for 2024 states, "cryptocurrency has become an enticing means to cheat investors, launder proceeds, and engage in other illicit schemes."[3] The FBI received nearly 150,000 crypto-related complaints that year, with total crypto-related losses totaling roughly $9.3 billion.[4] 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.[5] One scam, known as "pig butchering," where 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.[6]

SB 1208 adds digital financial assets to the statute prohibiting money laundering. This would seem to suggest the bill's intent is geared towards addressing criminal activity, so it would seem natural for a criminal asset forfeiture framework to be part of the bill. Instead, SB 1208 creates what looks like a civil asset forfeiture scheme alongside a new criminal penalty. This hybrid of ideas finds some explanation in bill's findings and declarations:

> 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. 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. However, these organizations can be disrupted by seizing traceable proceeds of fraud and other funds they use in laundering the proceeds of fraud.

The findings and declarations section suggests there is little expectation that adding digital financial assets to the money laundering statute will lead to convictions of criminal enterprises, but that a new civil forfeiture framework is needed to disrupt these same criminal enterprises. The Court has expressed concern where fines are employed "in a measure out of accord with the penal goals of retribution and deterrence." (*Harmelin* v. *Michigan* (1991) 501 U.S. 957, at fn. 9.) The ability to permanently dispossess unlimited values of digital financial assets with no serious effort made at securing a criminal conviction could invite judicial scrutiny.

---

[3] Federal Bureau of Investigation: Internet Crime Report (2024) Federal Bureau of Investigation, Internet Crime Complaint Center, at p. 3 <https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf> [as of June 1, 2026].
[4] *Id.,* at 35.
[5] *Id.,* at pp. 39-40.
[6] Griffin et al., *How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering* (Feb. 29, 2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4742235> [as of June 1, 2026].

While the forfeiture framework proposed in SB 1208 appears decidedly civil in nature, and apparently not explicitly intending for forfeitures under the bill to have a retributive or deterrent effect, the pairing of a new criminal penalty and a civil asset forfeiture scheme in the same bill could create interpretive uncertainty.

4) **Practical Concerns:** Given the challenges associated with prosecuting entities engaged in cryptocurrency scams, a civil forfeiture approach may be the only viable method of providing restitution to the victims of fraudulent schemes. Yet, even if this approach is a realistic one, there remain numerous practical and legal concerns.

The author seems to acknowledge the difficulty of securing a criminal conviction in cases involving digital financial assets due to the complex and transnational components common to these crimes. Similar difficulties almost assuredly will arise during the process of attempting to force forfeiture of digital assets. While certain exchanges and the tracking of assets will be relatively straightforward, like working with Binance or tracking certain activity on the blockchain, investigators nevertheless may face great difficulty in trying to access data on crypto exchanges. Even in the case of a cooperative exchange, out-of-state companies ultimately may prove obstinate or inaccessible. Counsel for these companies may caution against involvement. Internationally based companies could be entirely untouchable, particularly without cooperation or intervention from the federal government and California's current relationship with the federal government remains understandably strained. If the primary purpose of the bill is to return assets to those from whom they have been stolen, then the volatility of digital financial assets may render many investigations unprofitable as certain assets may have significant value one day and no value the next. The ability to turn digital assets into hard currency and/or precious metals may create difficulties fully tracing the assets from victim to recovery. The complexity of certain investigations may create outsized financial and resource burdens, particularly on local agencies.

Given the practical challenges with recovering these assets, in combination with California's jurisdictional limitations, an unusually great number of things may have to go right to achieve the bill's desired outcomes. The question of jurisdiction is foundational to a sovereign's exercise of legal power or authority over a person or property.[7] The power of our courts to decide cases and issue orders, like warrants, is an essential element of jurisdiction.[8] Without clear jurisdiction California cannot properly exercise its authority to issue warrants to seize digital financial assets. SB 1208 at least seems to acknowledge these challenges in the findings and declarations and by stating an intent to "permit jurisdiction to the maximum extent permissible under the United States Constitution and Section 40.010 of the Code of Civil Procedure." The potentially sprawling nature of these investigations means jurisdictional issues may provide another relatively burdensome hurdle to seizure and forfeiture of fraudulently acquired digital assets.

SB 1208 raises other questions. 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

---

[7] *Jurisdiction*, Cornell Law School Legal Information Institute <https://www.law.cornell.edu/wex/jurisdiction> [as of June 3, 2026].
[8] *Ibid.*

assets. Authorization to seize and disgorge substitute assets appears at least somewhat common in other forfeiture contexts like prosecuting drug rings, but forfeiture under state law in those cases generally requires an underlying conviction. SB 1208 does not require an underlying conviction. Furthermore, in the context of drug prosecutions a boat used in the illegal smuggling of drugs may be logically substituted by an asset like a car. Substitute assets in the context of digital financial assets may not be so clear. Delineating the outer bounds of substitute assets in this context may be beneficial to ensure that only assets related to criminal activity are seized.

5) **Money Laundering:** Money laundering describes the process of concealing the origin of money obtained from illicit activities to make the source of such funds appear legitimate.[9] California's anti-money laundering statute, however, prohibits more than simply attempting to conceal the nature of ill-gotten assets. Our laws criminalize 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 seven-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. (Pen. Code, § 186.10.) 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. (Pen. Code, § 186.9, subd. (d).) 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 where the value of the transactions meets specified thresholds. (Pen. Code, § 186.10, subd. (c).)

   SB 1208 expands section 186.10 of the Penal Code to include transactions or attempted transactions involving digital financial assets, as defined in the DFAL. Cryptocurrency transactions largely occur outside the traditional banking system and are traded on "cryptocurrency exchanges," which act as a marketplace for digital assets similar to a stock exchange.[10] The bill's inclusion of digital financial asset transactions into the money laundering statute, in conjunction with the noted volatility of digital financial assets, may raise concerns over the application and effectiveness of the statute's tiered enhancement scheme. (Pen. Code, § 186.10., subd. (c).) Also, given the apparent focus on victim restitution in this bill, having a clear understanding of the precise values of these volatile assets at specific points in time could be important.

6) **Asset Forfeiture:** Forfeiture is a legal process that government can use to seize and dispossess property connected with criminal activity.[11] Depending on certain factors, like the legal nature of the proceeding providing for forfeiture, the process is considered either civil forfeiture or criminal forfeiture.[12] Civil forfeiture proceedings are *in rem*, which means they

---

[9] *What is money laundering?* United States Treasury Financial Crimes Enforcement Network <https://www.fincen.gov/what-money-laundering> [as of June 3, 2026].
[10] Maheshwari, R. *What are crypto exchanges and how do they work?* (Nov. 5, 2024) *Forbes* <https://www.forbes.com/advisor/in/investing/cryptocurrency/what-is-a-crypto-exchange/> [as of June 1, 2026].
[11] *Civil forfeiture*, Cornell Law School Legal Information Institute <https://www.law.cornell.edu/wex/civil_forfeiture> [as of June 3, 2026].
[12] *Ibid.*

are brought against the property, not a person.[13] Cash proceeds from a drug deal, for example, may be seized and forfeited in civil forfeiture proceedings if the government can show by the defined evidentiary standard that the property was involved in illicit activity. This makes sense in the context of drugs as property interests cannot be established in contraband. Supporters of asset forfeiture argue that this process allows law enforcement to disrupt criminal activity by restricting access to assets that may otherwise be used in crime.[14] 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.[15] For this reason, civil forfeiture schemes have drawn sharp criticism, with critics arguing that these schemes incentivize policing for profit.[16]

Criminal asset forfeiture proceedings, however, are *in personam*, which means they are brought against people.[17] They generally require an underlying criminal conviction, which requires meeting the beyond a reasonable doubt evidentiary standard before government can force forfeiture of property.[18] The property forfeited is generally limited to those assets that can be shown to have a connection to the underlying crime(s).[19] Here, the proceeding to force dispossession of property generally occurs only after a criminal conviction has been established.[20]

As mentioned, asset forfeiture is not without its critics not just due to the potentially perverse incentives created by civil asset forfeiture, but also due to the myriad constitutional concerns that intersect this process. While SB 1208 does attempt to legislate out the risk of creating perverse incentives by limiting where forfeited assets can be sent (e.g., General Funds, victims, but not law enforcement agencies) certain legal and practical concerns remain.

7) **Inconsistency with State Asset Forfeiture Frameworks:** 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. (Pen. Code, §§ 186-186.8.) 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. (Pen. Code, § 186.3.) The forfeited assets are typically 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. (*Ibid.*) 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. (Pen.

---

[13] *Ibid.*
[14] *Ibid.*
[15] *Ibid.*
[16] *Ibid.*
[17] *Ibid.*
[18] *Ibid.*
[19] *Ibid.*
[20] *Ibid.*

Code, § 186.3, subd. (a).) Thus, the forfeiture process under CPOC clearly represents a criminal asset forfeiture scheme.

Changes to asset forfeiture in drug crimes were also made by SB 443 (Mitchell), Chapter 831, Statutes of 2016. SB 443 generally requires a prosecuting agency to seek or obtain a criminal conviction for defined drug crimes to secure forfeiture of related assets. (Health & Saf. Code, § 11471.2, subd. (b); *cf.* Health & Saf. Code, § 11471.2, subd. (c).) Additionally, SB 443 increased the burden of proof in forfeiture proceedings from a clear and convincing evidence standard to beyond a reasonable doubt standard. (Health & Saf. Code, § 11488.4, subd. (i)(1).) Like asset forfeiture in the context of certain crimes involving controlled substances, asset forfeiture in the context of criminal profiteering requires an underlying conviction to dispossess assets from individuals. (Pen. Code, § 186.3, subd. (a).)

Given the statutory requirements for underlying convictions required for asset forfeiture in other parts of California law like criminal profiteering activities and specified drug crimes, SB 1208 stands out as inconsistent with California's approach to asset forfeiture. Furthermore, because criminal profiteering is defined to cover so many acts, including receiving stolen property (Pen. Code, § 186.2, subd. (a)(13)), false or fraudulent activities (Pen. Code, § 186.2, subd. (a)(21)), and notably, money laundering (Pen. Code, § 186.2, subd. (a)(22)), SB 1208 would effectively rescind the requirements for securing criminal convictions to dispossess someone of assets for numerous criminal profiteering crimes beyond just money laundering.

8) **Constitutional Concerns**: SB 1208 presents several constitutional concerns. This is due in part to the potential consequences arising from the bill, the lack of relative clarity in the law that guides the constitutional bounds of the issues stemming from this bill, and the existence of both standing alone and intersecting constitutional issues.

a) The Fourth Amendment: The Fourth Amendment of the United States Constitution provides that "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath of affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (U.S. Const., 4th Amend.) The Fourth Amendment protects people and extends to areas where an individual has a reasonable expectation of privacy. (*Carpenter v. United States* (2018) 585 U.S. 296.) States are required to comply with the Fourth Amendment because the Fourteenth Amendment's Due Process Clause incorporates to the States the protections afforded by the Fourth Amendment. (*Wolf v. Colorado* (1949) 338 U.S. 25 [recognizing the rights against unreasonable search and seizure are implicit to our concept of liberty], *Mapp v. Ohio* (1961) 367 U.S. 643 [incorporating the Fourth Amendment to States.].) Pursuant to the Fourth Amendment's protections against unreasonable searches and seizures, law enforcement generally must secure a warrant before conducting a search of private property. A seizure of property occurs whenever "there is some meaningful interference with an individual's possessory interests in that property." (*United States v. Jacobsen* (1984) 466 U.S. 109, 113.)

California law states that when property is alleged to have been stolen or embezzled, law enforcement must retain custody of that property pending the disposition of any court proceedings. (Pen. Code, § 1407.)

A search warrant requires probable cause that identifies or describes the person to be searched or property to be seized, and the particular facts *supporting an underlying crime*. (Pen. Code, § 1525.) SB 1208 tactically attempts to legislate around California state law in this space by, among other things, setting up its civil forfeiture framework notwithstanding California's search warrant statute. SB 1208 offers a metaphorical head nod at some intent to prosecute crime by including digital financial assets in the money laundering statute, but the civil forfeiture framework created by this bill requires no direct connection to a money laundering investigation or prosecution to secure a warrant to search, seize, and dispossess a person of digital property. Rather, simply establishing a probable nexus to "a crime" is sufficient to seize and dispossess someone of digital property. In fact, because this bill's forfeiture framework is effectively civil, a person really need not be involved in a crime at all. Just demonstrating that *the property* was likely involved in "a crime" is likely sufficient to dispossess a person of digital assets under this framework.

SB 1208 at least does appear to create an opportunity for an innocent owner to recover their property. This is certainly an important guardrail, but individual rights in the Constitution, including those rights contained in the Fourth Amendment, limit the powers of government and expressly protect individuals from government interference.[21] SB 1208 may offer an essential backstop to ensure lawful property owners are not ultimately dispossessed of their property, but this backstop is triggered only because government power will have been expanded and interference will have already occurred. Whether that interference is constitutionally justifiable is unclear.

b) The Fifth Amendment: The Fifth Amendment generally states that government may not take private property without just compensation. (U.S. Const., 5th Amend.) Known as the Takings Clause, States are required to compensate a property owner if property is taken. (*Chicago, Burlington & Quincy Railroad Co. v. City of Chicago* (1897) 166 U.S. 226.) The Takings Clause is implicated by SB 1208 because digital financial assets are property and the dispossession of this property authorized by the bill would be done by governmental agencies.

The Court has ruled that the Fifth Amendment generally does not require governments to compensate property owners for that property taken via asset forfeiture. (See *Bennis v. Michigan* (1996) 516 U.S. 442.) As noted by our Ninth Circuit Court of Appeals, however, this ruling was effectively overturned by the Civil Asset Forfeiture Reform Act (CAFRA), passed by Congress in 2000. (See 18 U.S.C. § 983(d)(1), *United States v. Ferro* (9th Cir. 2012) 681 F.3d 1105, 1112.) The court in *Ferro* wrote that "with this [law], Congress ensured that modern-day forfeiture differs from historical forfeiture, since the Supreme Court earlier noted a 'long and unbroken line of cases' which had previously held that, under certain historical forfeiture provisions, 'an owner's interest in property may be forfeited by reason of the use to which the property is put even though the owner did not know that it was to be put to such use.'" (*Ferro, supra*, at p. 1112.) It is unlikely, though ultimately unclear, whether SB 1208 will encounter Fifth Amendment scrutiny.

Importantly, CAFRA appears to govern only federal forfeiture actions and does not preempt states from also regulating in this area. The federal Bank Secrecy Act (BSA), however, does preempt state regulation in certain areas. (See 12 U.S.C. §§ 1829b, 1951-1960, 31 U.S.C. §§

---

[21] Laurence H. Tribe. *American Constitutional Law*, 3rd ed., at p. 10 (2000).

5311-5314, 5316-5336.) Article VI of the Constitution states that federal law is the supreme law of the land and it is this provision that precludes state regulation in areas where preemption is clearly established. (U.S. Const., art. VI, cl. 2.) Congressional intent is the touchstone of a preemption analysis. (*Wyeth v. Levine* (2009) 555 U.S. 555, 565.) It is unlikely that statutory preemption would be an issue with SB 1208 as the BSA is generally focused on reporting requirements to identify money laundering, while SB 1208 is focused on expanding the assets subject to the money laundering statute and how those assets can be forfeited.

c) The Fourteenth Amendment: The Fourteenth Amendment prohibits States from depriving individuals of life, liberty, or property without due process of law. (U.S. Const., 14th Amend.) Under the Due Process Clause of the Fourteenth Amendment, States ordinarily may not seize real property before providing procedural due process protections like notice and a hearing. (*United States* v. *James Daniel Good Real Property* (1993) 510 U.S. 43, 62.) States, however, are generally permitted to seize property subject to civil forfeiture when the property "could be removed, destroyed, or concealed before a forfeiture hearing." (*Calero-Toledo* v. *Pearson Yacht Leasing Co.* (1974) 416 U. S. 663, 679-680.)

California law provides additional restrictions on how government can treat seized or forfeited property. When property is not alleged to have been stolen or embezzled by a person, but rather is just "property stolen or embezzled," and the property is in the possession of law enforcement or the court, Penal Code sections 1409-1411 provide that the magistrate who has custody of the property "shall order it delivered to the owner upon satisfactory proof of ownership, and when reasonable notice and an opportunity to be heard have been given to the person from whom the property was taken." (*People v. Superior Court (McGraw)* (1979) 100 Cal.App.3d 154, 156.))

SB 1208 undoubtedly establishes due process mechanisms, but the bill arguably creates a constitutionally suspect inversion of seizure and dispossession authority. In other words, requiring a person in possession of digital financial assets to prove they are the rightful and innocent owner of such assets before ever being convicted or even accused of a crime could invite constitutional scrutiny.

d) The Sixth Amendment: The Sixth Amendment, among other things, guarantees the right to competent, effective counsel. (U.S. Const., 6th Amend.) The Sixth Amendment usually grants defendants a fair opportunity to acquire their counsel of choice. (*Powell v. Alabama* (1932) 285 U.S. 29, 53.) Securing the assistance of counsel often requires fungible resources like money and assets. Thus, "the Sixth Amendment guarantees a defendant the right to be represented by an otherwise qualified attorney whom that defendant can afford to hire." (*Luis v. United States* (2016) 586 U.S. 5, 12.) To this end, the Court held that the pretrial restraint of legitimate, untainted assets needed to retain counsel of choice violates the Sixth Amendment. (*Ibid*.)

Certain investigations that lead to seizures and dispossessions authorized under SB 1208 could create conflict with this holding. Should the property acquired by the government under this bill lead to criminal charges that property may be required to be held if that property is needed by the criminal defendant to retain counsel of their choice for their defense. This hurdle could slow or halt what appears to be the primary intent of the bill—the return of lost assets to victims. Of course, this issue can be sidestepped by simply not ever

prosecuting those involved with the scams, even if all relevant laws and the facts of the investigation permit such a prosecution. If that is always to be the outcome though, why bother including digital financial assets in the money laundering statute?

An argument could be made that the framework established in SB 1208 obviates the need to consider the *Luis* Court's decision because it is the guilty property that is seized and dispossessed, not property belonging to a guilty person. The *Luis* Court, however, engages in an illuminating discussion regarding how "tainted" property impacts ownership, and comparing their holding in this case to previous cases. (*Luis, supra*, at pp. 11-14.) The Court notes that tainted property, like a robber's loot, creates an imperfect property interest in the defendant but that the loot ultimately belongs to the victim. (*Id.* at p. 13.) Untainted property rightfully belongs to the defendant. (*Id.* at p. 12.) The Court further writes that "title to property used to commit a crime (or otherwise 'traceable' to a crime) often passes to the Government at the instant the crime is planned or committed." (*Id.* at p. 13.) It is important to acknowledge the underlying assumptions in the Court's analysis. Regardless of whether assets subject to forfeiture are tainted by some connection to crime, or are untainted, there seems to be an assumption in the Court's analysis that forfeited assets belong to *someone*. This is another reason the slender reed upon which civil asset forfeiture rests is problematic. Given these concerns, it is worth considering whether it is wise to continue employing a legal process that may be constitutionally dubious and is too often inherently inconsistent.

e) The Eighth Amendment: The Eighth Amendment protects individuals against excessive fines, and cruel and unusual punishment. (U.S. Const., 8th Amend.) The Court incorporated the Excessive Fines Clause to the States in a case where the State of Indiana sought civil forfeiture of an individual's SUV on the ground it had been used to transport contraband. (*Timbs v. Indiana* (2019) 586 U.S. 146.) While the Court remanded on the question of whether a vehicle valued at $42,000 was excessive relative to a criminal penalty with a maximum fine of $10,000, the Court reaffirmed that the Eighth Amendment limits the government's power to extract payments, whether in cash or in kind, as punishment for some offense. (*Id.* at p. 151.) The Court also restated that in situations where governments stand to benefit "it makes sense to scrutinize governmental action more closely." (*Id.* at p. 154.)

As previously mentioned, Congress passed CAFRA not just to abrogate the Court's decision in *Bennis*, but to incorporate guidelines to review forfeitures for proportionality, which largely tracks Eighth Amendment Supreme Court precedent. (*Ferro, supra*, at p. 1112.) Under the law, "a court should compare the forfeiture to the 'gravity of the offense,' and the claimant then has the burden of establishing the forfeiture is 'grossly disproportional' to the offense." (18 U.S.C. § 983(g)(2)-(3); see also *Ferro, supra*.) If the court establishes that the forfeiture is grossly disproportional to the offense, it must "reduce or eliminate the forfeiture as necessary to avoid a violation of the Excessive Fines Clause of the Eighth Amendment of the Constitution." *(Ibid.)*

The asset forfeiture scheme authorized by SB 1208 thus could run into Eighth Amendment problems if the forfeitures result in a value grossly disproportionate to the penalties of an offense that ends up being prosecuted following the forfeiture.

9) **Argument in Support**: According to the bill's sponsor, *California Department of Justice*, "Attorney General Bonta . . . urges your support for this legislation to enhance the ability of state and local law enforcement to combat the rapidly expanding scourge of cryptocurrency

scams and, just as importantly, help return cryptocurrency (also known as "digital financial assets") to the victims of such fraud.

"'Pig butchering,' a cryptocurrency scam wherein scammers manipulate and gain the trust of potential victims to induce them to transfer funds into fake cryptocurrency projects, has been estimated to result in over $75 billion dollars stolen and laundered via cryptocurrency from 2021 to 2024 nationwide.0F1 In 2025, 116,414 California victims reported over $3.67 billion lost to scams, ranking first among states for both number of victims and overall loss amount in the FBI's annual Internet Crime Report.1F2 In short, cryptocurrency fraud is a serious threat to public safety that is only growing worse, and victims of crypto scams are far too often unable to recover their losses and be made whole again.

"Existing seizure laws require a criminal conviction for the forfeiture of fraud proceeds. When it comes to cryptocurrency scams, however, prosecutors are limited in their ability to identify individual perpetrators, extradite them, and obtain a criminal conviction because these scammers are often part of transnational criminal organizations located overseas, protected by government corruption, or both. In such cases when the perpetrators are effectively beyond the reach of state and local law enforcement, it is much more difficult to effectuate the legal seizure and remission of stolen assets back to the victims of the fraud if a criminal conviction is a precondition.

"To modernize the law for the cryptocurrency age, SB 1208 will provide statutory authority to CA prosecutors to initiate a special proceeding of a criminal nature to seize cryptocurrency wallets and exchange accounts being used to launder fraud proceeds. This provides prosecutors with a much-needed tool to seize and return digital financial assets to victims of cryptocurrency fraud that does not require a criminal conviction, which is difficult for the reasons previously described. At the same time, SB 1208 provides robust due process protections, including specific criteria for obtaining a search warrant and due process for claimants to file a verified claim for the return of the seized property.

"Existing law also needs to be updated to make it easier to facilitate the return of digital financial assets to victims of cryptocurrency fraud. To the extent that current law provides for the return of stolen cryptocurrency, prosecutors must do so by proving that one victim is the true owner of the specific cryptocurrency that was seized. However, commingling and money laundering can make it difficult to prove which specific victim is the owner of the cryptocurrency, particularly when investigating multi-victim fraud schemes and organized money laundering.

"To address this, SB 1208 provides a mechanism to return seized cryptocurrency to identifiable victims of crime based on proof of the crime and the loss to the victims, rather than requiring proof of ownership through commingling. The bill requires digital assets recovered from seized cryptocurrency accounts to be used to compensate victims of the crimes or fraud, on a pro rata basis, up to the amount of their actual loss, and victims of similar or related crimes or frauds.

"SB 1208 is urgently needed legislation that will help law enforcement to disrupt the operations of criminal groups and scammers committing crypto fraud and better enable prosecutors to legally seize and return digital financial assets to Californian victims. For these reasons, Attorney General Bonta requests your support for SB 1208 to strengthen

protections against cryptocurrency fraud and help make victims of such fraud whole again."

10) **Argument in Opposition**: According to the *California Public Defenders Association*, "The California Public Defenders Association (CPDA), a statewide organization of public defenders, private defense counsel, and investigators, regrets to inform you that we oppose Senate Bill 1208 ("SB 1208") by Senator Grayson unless it is amended to provide guardrails to prevent the abuse of the money laundering statute against unbanked indigent individuals.

"Although the goal of combating transnational fraud and cryptocurrency-based money laundering is well intentioned, SB 1208 inadvertently creates a tool that will be misused against drug users and low level drug dealers and others who are unbanked and use cryptocurrency in place of cash resulting in more pretrial detention, greater disparity in plea bargaining and longer sentences.

I. The Amended Bill and Its Stated Purpose

"As amended, SB 1208 does two things: it expands the crime of money laundering under Penal Code section 186.10 to cover transactions in digital financial assets, and it creates a new civil forfeiture mechanism in section 186.13 aimed at transnational criminal organizations. Our objection is solely to the section 186.10 amendment.

"The legislative findings state that the bill's target is sophisticated transnational fraud – organized networks operating from countries beyond the reach of California courts, using cryptocurrency to launder proceeds of internet scams and human trafficking. That is a legitimate and serious problem. The problem is that the statutory mechanism chosen to address it reaches conduct far removed from that target and will disproportionately impact economically disadvantaged individuals who do not have access to the banking system and are increasingly using cryptocurrency instead of cash.

II. The Practical Problem: Section 186.10(b) as a Charging Leverage Tool

"The amended section 186.10(b) provides that each series of digital asset transactions within a seven-day period totaling over $5,000 – or over $25,000 within thirty days – constitutes a separate, punishable felony offense. For the transnational fraud operator this bill targets, that provision is appropriate and workable. For the street-level defendant who uses cryptocurrency as a payment substitute, it creates an additional felony charge that has nothing to do with concealment, layering, or the evasion of financial oversight.

"As public defenders, we represent individuals who are low-level drug dealers who may have made six cryptocurrency payments to a supplier over five days totaling $5,400. They are using cryptocurrency in place of cash. The cryptocurrency was transferred directly from them to their dealer. No financial institution was used. No concealment structure was employed. "There was no layering, no smurfing, no attempt to disguise the origin of funds. Under existing law, they would be charged with sales or possession for sales and face up to 5 years imprisonment. Under SB 1208, the prosecution could also charge them with money laundering and they would face an additional 4 years incarceration.

"This is not a theoretical concern. The separate-offense aggregation mechanism in section 186.10(b) functions in practice as a charging multiplier. A district attorney who can stack a

money laundering count onto an existing drug charge has substantially increased bargaining leverage in plea negotiations, regardless of whether the facts would ever support a money laundering conviction at trial. Individuals facing additional felony exposure – particularly those with prior strikes or facing immigration consequences – resolve cases differently than individuals facing the underlying charge alone. The result is that marginal crypto use in an otherwise ordinary drug case becomes a vehicle for increased sentences.

"A parallel concern arises in cases involving sex work, particularly online platforms where digital payments are used for discretion or accessibility rather than concealment. The "knowing" prong of section 186.10(a) – which reaches conduct where the actor knows the funds represent the proceeds of criminal activity – can plausibly reach the ordinary receipt of payment for already-criminalized conduct, effectively layering a separate money laundering felony onto prosecuted conduct without any showing of the sophistication or concealment intent the statute was designed to reach.

III. The Proposed Amendment Addresses This Problem Without Undermining the Bill's Purpose

Proposed SB 1208 Amendment – PC § 186.10, Subdivision (f)

Section 186.10 of the Penal Code is amended to add subdivision (f), to read:

186.10.

(f)(1) Notwithstanding subdivision (a), no person shall be prosecuted under this section solely on the basis of conducting or attempting to conduct a digital financial asset transaction, as defined in Section 3102 of the Financial Code, where all of the following conditions are met:

(A) The transaction or transactions were conducted by the person solely on their own behalf and not as a business, service, or intermediary for any third party; and

(B) The person did not receive direct financial compensation, fee, or other remuneration in exchange for conducting the transaction on behalf of another.

(2) This subdivision shall not apply where the prosecution establishes, by evidence independent of the transaction itself, that the person acted with the specific intent described in subdivision (a) or had actual knowledge that the digital financial asset directly and specifically represented the proceeds of criminal activity.

(3) For purposes of this subdivision, the aggregation of digital financial asset transactions to meet the threshold values set forth in subdivision (f)(1)(B) shall not be permitted unless the prosecution establishes by independent evidence that the transactions were conducted pursuant to a common scheme or plan to evade the thresholds of this section.

(4) Nothing in this subdivision shall be construed to:

(A) Provide a defense to any other criminal offense for which the underlying conduct may otherwise qualify;

(B) Immunize any person from civil forfeiture proceedings conducted pursuant to Chapter 8 (commencing with Section 186.2) where independent probable cause exists; or

(C) Limit the authority of any state or local agency to investigate suspected violations of this section or to seek records pursuant to lawful process.

"CPDA's proposed amendment addresses this concern by adding subdivision (f) to section 186.10, establishing guardrails to prevent the unintended further criminalization of individuals making digital asset transactions solely on their own behalf and without intermediary compensation. The proposed amendment contains two essential limiting conditions: (A) the transactions must be conducted solely for the person's own account and not as part of a business or intermediary service; and (B) the person must not have received compensation for conducting the transaction on behalf of another. In other words, the individual is using the cryptocurrency in place of cash or a credit card.

"Critically, these guardrails would not be available where the prosecution establishes by independent evidence that the person acted with the specific intent described in subdivision (a) or had actual knowledge that the digital assets directly and specifically represented criminal proceeds. Moreover, the proposed guardrails do not apply where aggregation is supported by independent evidence of a common scheme or plan to evade reporting thresholds. Finally, these guardrails do not provide a defense to any other criminal offense, immunize any person from civil forfeiture, or limit any agency's investigative authority.

"The guardrails thus directly align the statute's reach with its purpose. A transnational fraud operator moving hundreds of thousands of dollars in cryptocurrency through layered accounts does not benefit from the guardrails. A street-level drug user or dealer who used Bitcoin as a cash substitute in six small drug transactions over one week does. That distinction is exactly the one the Legislature should want to preserve with the purpose of the money laundering statute.

"For these reasons, on behalf of CPDA, we respectfully urge your "NO" vote when SB 1208 comes before you in the Assembly Public Safety Committee unless it is amended to address these issues."

11) **Related Legislation**:

a) AB 2285 (Valencia) would regulate a bank or a credit union under the examination authority of the Department of Financial Protection and Innovation (DFPI) with respect to its provision of digital asset custody services, staking services, and digital asset transaction services, as those terms are defined, including by requiring certain disclosures to customers and requiring certain financial safety measures. AB 2285 is pending hearing in the Assembly Banking & Finance Committee.

b) AB 2409 (Valencia) would prohibit a public officer and specified public employees, as those terms are defined, from issuing a meme coin, among other things. AB 2409 is pending referral in the Senate Rules Committee.

12) **Prior Legislation**:

a) SB 97 (Grayson), of the 2025-2026 Legislative Session, would have revised certain criteria of the DFAL to specify that a person who has submitted an application to engage in the business of digital financial assets is prohibited from engaging in that business until the person is licensed, among other things. SB 97 was ordered to the inactive file on the Assembly floor.

b) AB 1029 (Valencia), Chapter 85, Statutes of 2025, expand the definition of "investment" for purposes of the Political Reform Act of 1974 to include a digital financial asset, and would specifically require public officials to disclose interests in their digital financial assets, as specified.

c) AB 236 (Chen), of the 2025-2026 Legislative Session, would have prohibited the fee attached to an application to engage in digital financial asset business activities from exceeding $5,000. AB 236 was held in the Assembly Appropriations Committee.

d) AB 1118 (Chen), of the 2025-2026 Legislative Session, would have would have allowed a search warrant for stolen or embezzled currency, as specified, to include an order for such currency to be returned to a lawful owner identified in the warrant pursuant to specified procedures including a hearing, if requested, to determine that the currency was stolen or embezzled, before it is returned to its owner.

e) AB 1934 (Grayson), Chapter 945, Statutes of 2024, required a licensee to also maintain, if applicable, a report maintained at least monthly that demonstrates compliance with conditions that authorize the licensee to exchange, transfer, or store a digital financial asset or engage in digital financial asset administration, as specified.

f) SB 401 (Limon), Chapter 871, Statutes of 2023, provided for the regulation of digital financial asset transaction kiosks, as defined, by DFPI and would, among other things, prohibit an operator from accepting or dispensing more than $1,000 in a day from or to a customer via a digital financial asset transaction kiosk.

g) AB 39 (Grayson), Chapter 792, Statutes of 2023, prohibited a person from engaging in digital financial asset business activity, or holding itself out as being able to engage in digital financial asset business activity, with or on behalf of a resident unless certain criteria are met, including the person is licensed with DFPI, as prescribed.

h) AB 76 (Davies), of the 2023-2024 Legislative Session, would have modified the definition of "monetary instrument" to include "digital assets that use blockchain technology," as specified. AB 76 was held in the Senate Appropriations Committee.

i) AB 2269 (Grayson), of the 2021-2022 Legislative Session, would have created the DFAL, which would have prohibited a person from engaging in digital financial asset business activity, or holding itself out as being able to engage in digital financial asset business activity, with or on behalf of a resident unless any of certain criteria are met, including the person is licensed with the DFPI, as prescribed. AB 2269 was vetoed by the Governor.

j) SB 443 (Mitchell), Chapter 831, Statutes of 2016, required, among other things, a prosecuting agency to seek or obtain a criminal conviction for the unlawful manufacture or cultivation of any controlled substance or its precursors prior to an entry of judgment for recovery of expenses of seizing, eradicating, destroying, or taking remedial action with respect to any controlled substance.

REGISTERED SUPPORT / OPPOSITION:

Support

California Department of Justice (Sponsor)
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 District Attorneys Association
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 County District Attorney's Office
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' Assocation
Pomona Police Officers' Association
Riverside County District Attorney
Riverside Police Officers Association
Riverside Sheriffs' Association

Opposition

California Public Defenders Association

Analysis Prepared by: Dustin Weber / PUB. S. / (916) 319-3744