Date of Hearing: June 22, 2026

ASSEMBLY COMMITTEE ON BANKING AND FINANCE
Avelino Valencia, Chair
SB 505 (Richardson) – As Amended June 22, 2026

SENATE VOTE: 40-0

SUBJECT: Money Transmission Act: authentication

SUMMARY: This bill prohibits a digital wallet provider or money transmitter operating in the state from allowing a user to log in without using two-factor authentication or multifactor authentication for any login by that user.

Specifically, **this bill**:

1) Defines "multifactor authentication" to mean an authentication process that requires more than two forms of verification.

2) Defines "two-factor authentication" to mean a security process that requires two distinct forms of verification.

3) Defines "user login" to mean an action by which a user accesses an account or platform for the purpose of initiating, receiving, or managing money transmission services for the first time after logout.

4) Prohibits a money transmitter (licensee) operating in the state from allowing a user to log in without using two-factor authentication, multifactor authentication, or reasonably equivalent or more secure access control for any login by that user.

5) Requires a process for reverifying the identity of the user, device or system using two-factor authentication, multifactor authentication, or reasonably equivalent or more secure access control

6) Requires the licensee to provide the user the ability to report an error or suspected fraud using the same platform through which the user accessed the service or a reasonable accessible alternative.

7) Allows the licensee to use a risk-based approach that balances consumer protection with reasonable access, including provided factors, when implementing the controls described in #4.

EXISTING LAW:

California

1) Requires persons engaged in the business of money transmission to be licensed and overseen by the Department of Financial Protection and Innovation (DFPI). Financial Code (Fin.Code) section 2030.

2) Defines "money transmission" to mean any of the following:

a) Selling or issuing payment instruments to a person located in this state.

b) Selling or issuing stored value to a person located in this state. Or

c) Receiving money for transmission from a person located in this state.

3) Defines "multi-factor authentication" to mean authentication through verification of at least two of the following types of authentication factors:

a) knowledge factors, such as a password;

b) possession factors, such as a token; Or

c) inherence factors, such as a biometric characteristic. 11 California Code of Regulation (C.C.R.) section 7001(u).

4) Defines "victim of identity theft" to mean a person who had their personal identifying information used without authorization by another to obtain credit, goods, services, money, or property, and did not use or possess the credit, goods, services, money, or property obtained by the identity theft, and has submitted a Federal Trade Commission identity theft report. California Civil Code (Civ.Code) section 1798.92(d).

5) Defines "claimant" to mean a person who has or purports to have a claim for money or an interest in property in connection with a transaction procured through identity theft. Civ.Code section 1798.92(a).

6) Permits a person who is the victim of identity theft to bring an action against a claimant to establish that the person is a victim of identity theft in connection with the claimant's claim against that person. Civ.Code section 1798.93 (a)

7) If a victim of identity theft can show that at least 30 days prior to filing an action, they

a) Provided written notice to the claimant that at the address designated by the claimant for complaints related to credit reporting issues that a situation of identity theft might exist and explaining the basis for that belief.

b) That the claimant failed to diligently investigate the victim's notification of a possible identity theft. And

c) That the claimant continued to pursue its claim against the victim after the claimant was presented with facts that were later held to entitle the victim to a judgment pursuant to this section.

The victim is entitled to, among other damages, a civil penalty of up to $30,000. Civ.Code section 1798.93(c)(6).

Federal

1) Defines "electronic fund transfer" to mean any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order,

instruct, or authorize a financial institution to debit or credit an account. 15 United States Code (U.S.C.) section 1693a (7).

2) If a person-to-person (P2P) payment provider directly or indirectly holds an account belonging to a consumer, they are considered a financial institution. Regulation E. 12 CFR 1005.2 (i).

3) Defines "unauthorized electronic fund transfer" to mean an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit, but the term does not include any electronic fund transfer:

   a) initiated by a person other than the consumer who was furnished with the card, code, or other means of access to such consumer's account by such consumer, unless the consumer has notified the financial institution involved that transfers by such other person are no longer authorized,

   b) initiated with fraudulent intent by the consumer or any person acting in concert with the consumer, or

   c) which constitutes an error committed by a financial institution. 15 U.S.C. section 1693a(12).

4) Provides for the following as acts constituting an error: (1) an unauthorized electronic fund transfer;

   a) an incorrect electronic fund transfer from or to the consumer's account;

   b) the omission from a periodic statement of an electronic fund transfer affecting the consumer's account which should have been included;

   c) a computational error by the financial institution;

   d) the consumer's receipt of an incorrect amount of money from an electronic terminal;

   e) a consumer's request for additional information or clarification concerning an electronic fund transfer or any documentation required by this subchapter; or

   f) any other error described in regulations of the Bureau. 15 U.S.C. section 1693f(f).

5) Requires a financial institution to investigate an alleged error, determine if an error has occurred, and report or mail such investigation and determination to the consumer within specified times if it has been given written or oral notice by a consumer that enables the financial institution to identify the name and account number of the consumer, indicates the consumer's belief that the account contains an error, and reasons for the consumer's belief that an error occurred. 15 U.S.C. section 1693f(a).

6) Requires a financial institution to correct the error if it has determined that an error has occurred. Or provide an explanation of finding if, after its investigation, it has determined that an error has not occurred. 15 U.S.C. section 1693f(b) and (d).

7) Permits treble damages for certain willful conduct. 15 U.S.C. section 1693f(e).

FISCAL EFFECT: **Unknown. This bill is keyed Fiscal by Legislative Counsel.**

COMMENTS:

1) Purpose

According to the Author

"The use of money transmitters among consumers has continued to grow at a fast rate, with estimates saying 70% of Californians now use them on a regular basis. Despite consumers' growing utilization of these services to handle, store, and send their money, money transmitters don't have the same level of protections that other financial services are required by law to provide – including banks and credit unions. SB 505 will help protect Californian's money through common sense account security laws, protecting consumers from fraud, unauthorized account access, and the loss of their hard-earned money."

2) Background

In 2025, the United Kingdom saw a 112% increase in financial fraud related to stolen devices.[1] In London alone, Metropolitan Police data shows us more than 70,000 phones were reported stolen in 2025.[2] A coordinated theft ring in New York made headlines in February 2024. In these incidents, criminals operating mopeds and scooters committed a series of 62 robberies, snatching mobile devices and handbags from women, bypassing security on banking applications and conducting unauthorized financial transactions.[3]

In response to increased theft through money transmitter apps, in January 2024, Manhattan District Attorney Avlin Bragg, Jr. issued a letter to money transmitters Venmo, Zelle, and CashApp, calling for better consumer protections from fraud.[4] As a solution, Bragg asked for "more safety measures, such as lowering the limit of daily transfers, requiring wait times on larger transfers, and for a confirmation when suspicious transfers occur. Even something as small as canceling a transaction would help."[5]

---

[1] UK banks see 62% spike in scam attempts, BioCatch, (London) April 15, 2026. https://www.biocatch.com/press-release/uk-banks-see-spike-in-scam-attempts Last visited 6/11/2026.
[2] *Id*.
[3] "7 migrants charged in string of cellphone robberies; 7 others sought", ABC7 NY, February 6, 2024. http://abc7ny.com/post/crime-spree-phones-stolen-nyc-migrants-new-york-city/14390546/?userab=kabc_content_recs-577*variant_a_control-2480%2Cwls_content_recs-584*variant_b_trending_wls-2517%2Cwpvi_content_recs-586*variant_a_control_wpvi-2520%2Cotv_web_content_rec-539*variant_c_trending-2268%2Cotv_search_page_design_unification-546*variant_b_search_redesign-2300%2Cabcn_popular_reads_exp-542*variant_b_7days_filter-2288 Last visited 6/11/2026.
[4] Manhattan District Attorney Alvin Bragg, Jr., Calls On Venmo, Zelle, Cash App To Better Protect Consumers From Fraud. January 23, 2024. https://manhattanda.org/manhattan-district-attorney-alvin-bragg-jr-calls-on-venmo-zelle-cash-app-to-better-protect-consumers-from-fraud/ Last visited 6/11/2026/
[5] *Id*.

3) What this bill does

SB 505 will require users of money transmitter apps to use reauthentication and secure access control requirements during every login attempt. The bill requires money transmitters ("licensees") to maintain written procedures approved by an individual who is responsible for oversight and implementation of the licensee's security program. The licensee must use a risk-based assessment that balances consumer protection with reasonable user access when implementing requirements.

The bill provides licensees a lot of latitude when assessing factors for implementation. This should offer flexibility for different approaches as needed to best work with a licensee's existing infrastructure. The definition of multifactor authentication (MFA) is broadly written to allow for evergreen application even with emerging security methods. This bill requires licensees to provide its users a method to report an error of suspected fraud using the same platform the user uses to access money transmission services, or a reasonably acceptable alternative in order to make error reporting more accessible.

4) What this bill does not do

a) This bill does not require an automatic logout or session timeout after a user logs in. This does allow users to remain logged into their accounts as desired without the need to use heightened secure access control until they logout. Notably, while this is the current practice for many popular licensees, this law does effectively create a new requirement for all licensees to provide heightened authentication access controls while still allowing users the option to maintain a frictionless experience.

b) This bill aims to solve a very specific problem, and arguably, one that already has a solution. When a stolen device is used by a thief to transfer money or make purchases, these are considered unauthorized transactions subject to the EFTA, user agreements, and the California Identity Theft Act. These laws, which provide for recovery of attorneys' fees and statutory damages, are strong incentives for licensees to ensure security measures on their platforms. However, as to fraud, wherein a user is tricked or coerced into making an unwanted transaction themself, these transactions are considered authorized, thus not subject to statutory recourse. According to the latest data, approximately 1.4 million identity theft cases were reported to the Federal Trade Commission last year, while one million cases of fraud were reported.[6]

c) This bill does not allow users to opt in or out of these security protocols, however do note comment (a) above regarding user login. This may create barriers for users with disabilities. Designing accessible MFA requires offering flexible verification methods, supporting assistive technologies like screen readers, and minimizing the need to manually memorize or transcribe codes between devices. According to the World Health Organization, approximately 1.3 billion people, or 16% of the world's population, live

---

[6] FTC Consumer Sentinel Network 2025, https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/AllReportsbyState Last visiter 6/11/2026. It is important to note that fraud is notoriously underreported with victims often feeling ashamed or embarrassed. Conversely, because there is a pathway to recovery, identity theft is easily reported to a dedicated website meant to collect ID theft information for the purposes of recovery. As a result, the data may be skewed.

with a disability affecting daily life and online access.[7] In 2025, 5.56 billion people, 67.9% of the global population, used the internet.[8] Over 2.2 billion people worldwide have vision impairments, making accessible design is essential for inclusion.[9] And about 430 million people globally experience disabling hearing loss and thus depend on visual cues and written content.[10] When authentication systems are inaccessible, the result is not just frustration for users with impairments. It can be the difference between paying a bill on time or incurring late fees and/or incurring overdraft fees. Presently, MFAs and OTPs are not mandated on consumers, but rather on the companies and its users who have access to sensitive consumer information.[11] These federal and state privacy laws are also heavy incentives for companies with consumer information to provide strong security measures around access to data.

d) This bill does not protect against other forms of identity theft in banking. According to its latest report, the Identity Theft Resource Center (ITRC) identified unauthorized access to computer or mobile devices to be only 15% of the reported forms of identity compromise type.[12] (Other forms include, data breach, impersonation, scam to obtain personal identifying information (PII), physical items stolen, mail, and pictures of PII or documents taken.)

5) Other considerations

While it is notable that the current laws are designed to put the onus of data security on the entities holding the sensitive information by using private rights of action and statutory damages as the stick, a 2022 investigation conducted by the office of Senator Elizabeth Warren found that "[b]anks are not repaying customers who contest "unauthorized" Zelle payments – potentially violating federal law and CFPB rules."[13] The study makes clear findings for increased fraud and scam claims over the most recent three years with no repayment for consumers, which is consistent with the position that, even though fraudulently induced, these payments are authorized.[14] However, the report found a more troubling trend with unauthorized transactions.

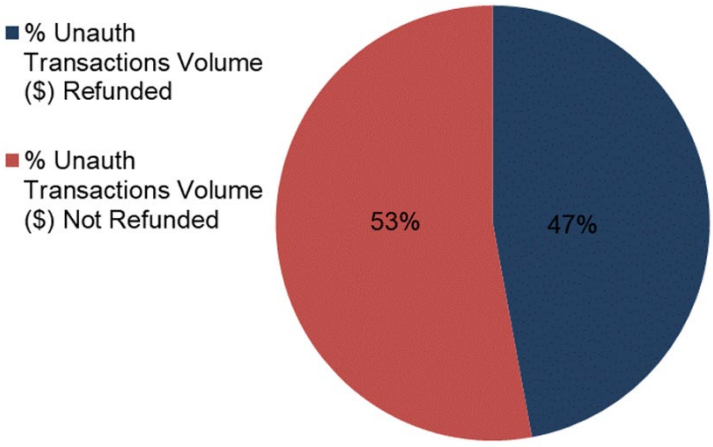
---

[7] "Disability" Fact Sheet, World Health Organization (March 7, 2023). https://www.who.int/news-room/fact-sheets/detail/disability-and-health Last visited 6/13/2026.
[8] Kemp, Simon, "Digital 2025:Global Overview Report, Data Reportal (February 5, 2025)
[9] "Blindness and Vision Impairment" Fact Sheet, World Health Organization (February 10, 2026). https://www.who.int/en/news-room/fact-sheets/detail/blindness-and-visual-impairment Last visited 6/13/2026.
[10] "Deafness and Hearing Loss" Fact Sheet, World Health Organization (March 3, 2026). https://www.who.int/news-room/fact-sheets/detail/deafness-and-hearing-loss Last visited 6/13/2026.
[11] In 2024, the Federal Trade Commission updated the Safeguards Rule (part of the Gramm-Leach-Bliley Act), deeming that the change was necessary due to the changed security and threat landscape. The rules apply to non-bank financial institutions. An entity is a "financial institution" if it's engaged in an activity that is "financial in nature" or is "incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C § 1843(k). (Examples are: auto dealers that extend credit to lease cars, collection agencies, tax preparation firms). FTC Safeguards Rule: What your Business Needs to Know. FTC. (December 2024), https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know Last visited 6/13/2026.
[12] "2025 Trends in Identity Report "Identity Theft Resource Center (2025) at 9. https://www.idtheftcenter.org/wp-content/uploads/2025/06/2025-ITRC-Trends-in-Identity-Report.pdf Last visited 6/13/2026.
[13] "Facilitating Fraud: How Consumers Defrauded on Zelle are Left High and Dry by the Banks that Created it.", Office of Sen. Elizabeth Warren. (Oct. 2022). https://www.warren.senate.gov/imo/media/doc/ZELLE%20REPORT%20OCTOBER%202022.pdf Last visited 6/14/2026.
[14] *Id.* at 5.

Banks failed to refund 53% of funds Zelle customers lost through *unauthorized* transactions. The study states:

> "These data are deeply troubling. They not only reveal that banks are breaking their word about repaying victims harmed by Zelle – they also indicate that the banks may be violating the CFPB's Regulation E rules, which require banks to make consumers whole after an unauthorized fraudulent transaction. That concern is amplified by repeated reports by the CFPB, Federal Reserve Board, and Federal Deposit Insurance Corp. that bank violations of Regulation E's error resolution rules, including the protection against unauthorized transfers, are common."[15]

Fig. 3: Banks Fail to Refund 53% of Funds Zelle Customers Lose Through Unauthorized Transactions



Note: Chart describes the share of the dollar value of Zelle customer fraud claims refunded by banks between 2021 and the first six months of 2022. Reflects data from PNC Bank, U.S. Bank, Truist, and Bank of America. JPMorgan and Wells Fargo did not provide complete data and are excluded from the analysis.

One potential cause for this failure to comply can simply be that the stick is too small. An EFTA claim only provides for reasonable attorney's fees and costs, actual damages, and up to $1000 in statutory damages.[16] Zelle transfer limits are determined by the user's bank, but generally range up to $3,500 per day. Thus, to enforce an action against a bank and Zelle for failure to comply with the EFTA, with a recovery of $4,500 and attorney's fees and costs can take more than two years, in federal court, with several depositions.[17] This simply is not worth the perceived cost and stress to many people. As a result, the systemic structures used to incentivize self-policing of financial institutions are inadequate. *See also* Consumer Financial Protection Bureau v. Comerica Bank for a recent case of pattern of practice for non-compliance with the EFTA.[18]

---

[15] *Id.* at 8.
[16] 15 U.S.C. 1693m.
[17] The EFTA requires the financial institution to investigate the consumer's claims of errors. This often takes several layers of internal review including customer service representatives, internal investigators, and management.
[18] In December 2024, the federal CFPB filed a lawsuit against Comerica Bank for its failure to administer its federal benefits program providing Social Security benefits primarily to elderly and disabled adults using a prepaid debit

Arguments in Support

"SB 505 protects vulnerable Californians from the harms caused by payment fraud through digital transactions on stored value platforms. In 2024, the second most common method of fraud reported to the FTC was through payment app or service. Californians alone reported a loss of over $1.6 billion due to fraud, with the most common type of fraud occurring because of an imposter scam.

These scams are everywhere. Almost every one of your constituents has experienced the despair of watching a misdirected payment on Venmo disappear, or hearing from a relative that they have been the victim of a scam facilitated by the lack of safeguards on CashApp. If these same payments had been made by credit card or debit card, consumers would be protected as long as they reported the problem promptly. But because these transactions were on a peer-to-peer app, the consumers' money is gone.

By definition, stored value platforms have access to information about both the sending and receiving accounts in a digital transaction. Therefore, they can and should take more responsibility to protect customers from the fraud committed on their platforms by scammers who have been allowed to open or access accounts where they can receive stolen funds.

SB 505 establishes protections for customers of stored value platforms who have been victimized by fraud schemes. More specifically, SB 505 requires operators of these stored value platforms to reimburse customers who have suffered losses from fraudulently induced transfers. The bill specifies how stored value platform operators should allow customers to submit claims for reimbursement of fraudulently induced transfers, including clear disclosures of the right to request reimbursement. And the bill also helpfully details how stored value platform operators must investigate claims for reimbursement of fraudulently induced transfers."-- *California Low Income Consumer Coalition (CLICC)*

Arguments in Opposition

"SB 505 could disproportionately affects (*sic*) underbanked or unbanked consumers, many of whom rely on stored value platforms as their primary financial tool in the absence of traditional banking options. By imposing greater liability on these platforms for fraudulent transfers, the bill may drive up operating costs, which could in turn result in higher fees or more stringent eligibility requirements— barriers that already-marginalized consumers can ill afford. These heightened costs and tighter controls could reduce the availability or accessibility of low-fee, convenient stored value services that underbanked individuals depend on to manage day-to-day financial needs. Consequently, those who can least afford traditional banking services might find themselves with fewer practical alternatives, potentially exacerbating financial exclusion and economic inequality."-- *Technet*

---

card. The complaint alleged violations under the EFTA for, among other causes, failure to timely investigate notices of errors. The case was ultimately dismissed without prejudice in any early sweep of cases by the incoming Trump Administration. CFPB v. Comerica Bank, United States District Court For The Northern District Of Texas Dallas Division. Case 3:24-cv-03054-B.

REGISTERED SUPPORT / OPPOSITION:

Support Last verified 6/18/2026

California Cyber Alliance
California Low-income Consumer Coalition
National Consumer Law Center, INC.
Rise Economy

Opposition Last verified 6/18/2026

Technet

Analysis Prepared by: Desiree Nguyen Orth / B. & F. / (916) 319-3081