ASSEMBLY THIRD READING
AB 2674 (Schiavo)
As Amended April 23, 2026
Majority vote

SUMMARY

This bill requires financial institutions to take specified preventive measures to help protect customers from financial harm stemming from suspect transactions.

Major Provisions

1) Defines "suspect transaction" to mean account activity that is an attempted or successful transfer, withdrawal, or deposit of money, into or from the account, in which the surrounding circumstances are suspicious, unusual, consistent with known deceptive tactics, or likely to be the result of financial abuse or deception.

2) Requires a depository institution (DI), as specified, to provide scam recognition and prevention training to employees no less often than once every six months.

3) Prohibits a DI from ignoring or devaluing any sign of financial abuse or deception based on the age, language capacity, or education of a customer.

4) Requires a DI that suspects financial abuse or deception with respect to any in-person suspect transaction shall employ all of the following preventive measures:

   a) Advise the customer to independently verify the information and inform the customer that the transaction cannot be undone.

   b) Encourage the customer to contact a nonprofit, nationally recognized fraud hotline that can help determine if the situation is harmful.

   c) If a customer has provided the depository institution with the contact information for an optional trusted third party and the depository institution does not have reason to believe that the trusted third party is causing, or will cause, financial harm to the customer, the depository institution may contact the trusted third party.

   d) For any suspect transaction, a depository institution shall disclose to the customer that the depository institution cannot be held liable for harms related to the suspect transaction that result in financial abuse or deception if it has complied with this section.

5) Requires the DI to display a notice containing information to warn the customer of a scams and fraud if a suspected translation occurs online and not in an expedited transaction.

COMMENTS

1) The Current Issue

Federal Trade Commission data show that consumers reported losing more than $12.5 billion to fraud in 2024, which represents a 25% increase over the prior year.[1] Of people who reported their age, those aged 20-29 reported losing money to fraud in 44% of reports filed with the FTC, while people aged 70-79 reported losing money in 24% of their reports and people aged 80 and over reported it in 21% of their reports.[2] Despite credit card fraud accumulating the greatest number of reports, bank transfers and payments accounted for the highest aggregate losses reported in 2024 ($2.09 billion); losses were over seven times the amount reported lost to credit card fraud.[3] The same report found that military consumers reported over 99,000 fraud complaints, including 44,587 imposter scams that reportedly cost them over $199 million in 2024. As of 2022, 99% of families owned at least one financial asset, and 98.6% owned a transaction account.[4]

2) Fraud v. Identity Theft

The difference between fraud and identity theft is the difference between a victim having a claim to recover their funds or not. *Identity theft* is the unauthorized use of a victim's identity or other personal identifying information to gain access to their property. *Fraud*[5] is the inducement of action by the victim under false pretenses in order to gain access to their property. Aside from statutory recourse under the California Identity Theft Act and the federal Electronic Funds Transfer Act, at a fundamental level, because some unauthorized person conducts the transaction, identity theft is a breach of the contractual agreement against unauthorized transactions for credit cards and DIs with their customers. But the latter, fraud, is not because the *customer* is the party that conducts the transaction; state of mind is not consequential. From a theoretical standpoint, this is conventionally sound; customers should have access to their funds upon demand. However, existing law recognizes the need for further safeguards from DIs given their unique vantage point.

Under existing law, employees of DIs are trained to recognize behaviors and patterns that may indicate that an elderly customer[6] is falling victim to a scam. Common examples of such indicators are confusion, out of pattern spending, changes in transaction patterns, and requests that fall outside of a customer's normal behavior. Upon recognition of the scam, employees are trained to use different discreet intervention methods to attempt to dissuade the customer from completing the suspicious transaction. Ultimately, under the current law, the DI can choose to entirely deny the transaction or complete the transaction as requested by the customer. AB 2674 builds on these existing practices by requiring additional interventions, both in-person and online, when a transaction is suspected to be a result of fraud.

---

[1] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024 Last accessed 4/13/26.
[2] Data Book 2024. Consumer Sentinel Network, 2024. pp 4.
[3] *Ibid*.
[4] *Changes in U.S. Family Finances from 2019 to 2022*, https://www.federalreserve.gov/publications/october-2023-changes-in-us-family-finances-from-2019-to-2022.htm at page 16. A "transaction account" includes checking accounts, savings accounts, money market accounts, call accounts, and prepaid debit cards.
[5] The terms "fraud" and "scam" may be used interchangeably.
[6] Customers of credit unions are referred to as "members". For purposes of this analysis, the term "customer" will be used to mean both bank customers and credit union members.

3) What the Bill Does-In-Person Transactions

In 2024, the Federal Bureau of Investigations (FBI) issued an announcement about the use of generative artificial intelligence (AI) to commit financial fraud.[7] The announcement shared the ways criminals used generative AI to create convincing text, images, voice cloning, and videos to fool consumers into financial traps. One of the tips for consumers to protect themselves provided in the announcement was independent verification: *"Verify the identity of the person calling you by hanging up the phone, researching the contact of the bank or organization purporting to call you, and call the phone number directly."* The Consumer Financial Protection Bureau (CFPB) warns[8] "*Criminals and con artists use many scams to target unsuspecting people—of all ages—who have access to money. Consumer scams happen on the phone, through the mail, e-mail, or over the internet. They can occur in person, at home, or at a business.*" The CFPB lists several signs of a scam, but categorically, these signs share a common theme of pressuring a person to pay immediately, in a form that is cash-like and irreversible.

AB 2674 requires the DI's employees to deploy their fraud recognition and prevention training when a suspicious transaction arises as well as 1) encourage the customer to independently verify the need for the transaction by contacting the person for whom the transaction is initiated if the customer did not initiate the first communication, 2) encourage the customer to contact a nationally recognized third-party fraud support hotline to help determine if the situation is harmful, 3) contact a trusted designated contact person if the DI does not have reason to suspect that the contact person would cause harm, and 4) notify the customer that the DI cannot be held liable for harm caused by any deception related to the transaction if it completed these steps.

Under the first intervention, the customer is encouraged to independently verify the need for the transaction by calling not the source of the original communication, but rather the subject for whom the transaction is made. For example, if the caller is seeking bail money for a niece, call the niece directly, or look up the number of the jail independently to verify, not the number of the jail if one is provided by the caller. Because financial frauds rely on a sense of urgency and emotional attachment, an intervention to break the illusion can be effective, though not in all instances. There are scams where there is no ability to independently verify information reliably.

The second and third interventions encourage the customer to seek help from an outside party. Experts have recommended a national fraud hotline as an effective tool because some customers believe that a relative or known person may be unreliable because they stand to gain an inheritance or gift. Additionally, the hotline helps victims walk through their illusion to better differentiate fact from fiction.

The fourth intervention is another approach to appealing to a customer's judgement. This intervention puts forward the risk involved with the transaction. Taken in context with the other interventions, naming the risk that the customer is about to incur can be effective enough to encourage the customer to follow through with independent verification.

Furthermore, a scammer can coach a person into bypassing known intervention. For this reason, the training to recognize and intervene in suspected fraud is left broad 1) for flexibility as fraud

---

[7] https://www.ic3.gov/PSA/2024/PSA241203. Last visited 4/14/26
[8] https://www.consumerfinance.gov/ask-cfpb/what-are-some-classic-warning-signs-of-possible-fraud-and-scams-en-2094/ Last visited 4/14/26

techniques change, 2) to prevent criminals from coaching victims through all possible interventions if otherwise prescribed by law, and 3) to permit DI to develop trainings on a localized level that is effective for its customers.

Conversely, if a customer makes an out-of-pattern transaction that they are certain is legitimate, these interventions do not stop the transaction or otherwise prevent the customer from receiving their money from the DI.

The author acknowledges that this bill will not capture all scam, such as long-term fraud like romance scams or "pig butchering"--the name given to scams involving the building of trust over time to gain a victim's confidence to invest largely in a fake business or investment. However, it will help a significant number of consumers, especially since the banks are better positioned to see trends than a consumer who may encounter a trendy scam for the first time.

4) What the Bill Does- Online Transactions

The bill also seeks to address online transfers of money to scammers. The bill applies to non-expedited bank transfers and requires a warning message to be displayed in the language that the consumer customarily conducts business.

Advocates have concerns about the effectiveness of a single warning. Consumers disillusioned by fraud usually require guided questioning to allow the consumer to reach their own conclusion. This approach is used for seniors considering reverse mortgages.[9] Additionally, similar warnings are prevalent in other money transmission applications in addition to many DIs, albeit in different terms. Given the frequency of such warnings, there is an argument that this warning may not be particularly effective due to warning desensitization.

According to the Author
"AB 2674 helps protect people from increasingly common and sophisticated financial scams. Today's scams often use tactics like impersonating trusted individuals, creating a sense of urgency, or even using artificial intelligence to sound convincing, which can lead to devastating and irreversible financial losses. This bill requires banks and financial institutions to better train their employees to recognize these scams, step in when something seems suspicious, and clearly warn customers before money is sent. By taking these simple but important steps, AB 2674 makes it easier to stop fraud before it happens."

Arguments in Support
"Financial scams, including impersonation, coercion, and deception schemes, continue to cause devastating and often irreversible harm to Californians. While banks invest billions of dollars annually in cybersecurity infrastructure, fraud detection systems, and network monitoring tools, these systems are often primarily designed to protect institutional platforms rather than intervene when consumers themselves are being deceived. As a result, consumers frequently bear the full financial loss, even when warning signs were detectable in real time.

[9] https://canhr.org/reverse-mortgage-suitability-self-evaluation-worksheet/ Last visited 4/14/26.

AB 2674 takes a balanced and pragmatic approach to tackle this difficult and persistent problem. Through increased education and stronger mechanisms to prevent and intervene in suspicious transactions, AB 2674 tackles financial abuse from all angles." *Unite Here*

Arguments in Opposition
"A fundamental concern with AB 2674 is that it effectively shifts liability to financial institutions for authorized transactions that were induced by fraud. Under longstanding payment system rules and federal law, including the Electronic Fund Transfer Act and Regulation E, the key legal distinction in fraud cases is whether a transaction was authorized or unauthorized. When a consumer personally initiates a payment—even if that consumer was deceived by a scam—the transaction is treated as authorized within the payment system. Financial institutions typically have no visibility into external communications or circumstances that led the consumer to initiate the payment. These scams frequently occur through text messages, phone calls, social media platforms, or online marketplaces that exist entirely outside the financial services system.

By creating liability for transactions that consumers themselves authorized, AB 2674 places responsibility on banks and credit unions for events that occur outside their control and beyond their ability to monitor. In practice, this standard would expose financial institutions to lawsuits whenever a consumer later claims they were persuaded or pressured into making a payment." *California Bankers Association*

FISCAL COMMENTS

The following comments are from the analysis of the Assembly Appropriations Committee.

1) Minor and absorbable costs to the Department of Financial Protection and Innovation to update informational materials and examinations to reflect required training, interventions, and warnings a licensee must follow.

2) Ongoing cost pressures of an unknown amount, potentially in excess of $150,000, to the courts in additional workload by creating new requirements for a depository institution enforceable under the Unfair Competition Law (UCL) (General Fund (GF) or Trial Court Trust Fund (TCTF)). A claim under the UCL may be brought by either a public prosecutor or a person who lost money or property as the result of the unlawful conduct. It is unclear how many civil actions may be filed statewide and how much court time may be needed to resolve each case, but it generally costs approximately $1,000 to operate a courtroom for one hour. Although courts are not funded on the basis of workload, increased pressure on staff and the TCTF may create a demand for increased court funding from the GF. The state budget provides annual GF backfills to the TCTF to offset revenue reductions, totaling approximately $117.3 million in fiscal year 2025-26.

VOTES

ASM BANKING AND FINANCE: 7-1-1
YES: Valencia, Fong, Krell, Michelle Rodriguez, Blanca Rubio, Schiavo, Soria
NO: Dixon
ABS, ABST OR NV: Chen

ASM JUDICIARY: 10-0-2
YES: Kalra, Bauer-Kahan, Bryan, Connolly, Dixon, Harabedian, Papan, Sanchez, Stefani, Zbur
ABS, ABST OR NV: Macedo, Pacheco

ASM APPROPRIATIONS: 13-0-2
YES: Wicks, Aguiar-Curry, Calderon, Caloza, Dixon, Fong, Mark González, Krell, Pacheco, Pellerin, Sharp-Collins, Solache, Ta
ABS, ABST OR NV: Hoover, Tangipa

UPDATED

VERSION: April 23, 2026

CONSULTANT: Desiree NguyenOrth / B. & F. / (916) 319-3081 FN: 0002801