Office of Senate Floor Analyses
(916) 651-4171

THIRD READING

Bill No: SB 505
Author: Richardson (D)
Amended: 1/5/26
Vote: 21

SENATE BANKING & F.I. COMMITTEE: 5-0, 1/7/26
AYES: Grayson, Niello, Cervantes, Richardson, Strickland
NO VOTE RECORDED: Hurtado, Limón

SENATE APPROPRIATIONS COMMITTEE: Senate Rule 28.8

SUBJECT: Money Transmission Act: authentication

SOURCE: Author

DIGEST: This bill prohibits a money transmitter from allowing a user to log in without using two-factor or multi-factor authentication.

ANALYSIS:

Existing federal law:

Pursuant to Regulation E (12 Code of Federal Regulations (CFR) Part 1005) which implements the Electronic Funds Transfer Act (15 U.S.C. 1693 et seq.):

1) 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 the transfer and from which the consumer receives no benefit. (12 CFR 1005.2(m))

2) Limits a consumer's liability related to unauthorized electronic fund transfers to $50 if the consumer notifies the financial institution within two days after learning of the loss or $500 if the consumer fails to notify within two days, as specified. (12 CFR 1005.6(b))

3) Provides procedures for resolving errors, including unauthorized electronic fund transfers, including time limits for a financial institution to investigate claims. (12 CFR 1005.11)

Existing state law:

1) Provides the Money Transmission Act, administered by the Department of Financial Protection and Innovation (DFPI), which requires licensure of persons engaged in the business of money transmission, unless the person is exempt. (Financial Code Section 2000 et seq.)

2) Defines "money transmission" as any of the following: selling or issuing payment instruments, selling or issuing stored value, or receiving money for transmission. (Financial Code Section 2003(q))

3) Defines a "payment instrument" as a check, draft, money order, traveler's check, or other instrument for the transmission or payment of money or monetary value, whether or not negotiable and provides that a "payment instrument" does not include a credit card voucher, letter of credit, or any instrument that is redeemable by the issuer for goods or services provided by the issuer or its affiliate. (Financial Code Section 2003(s))

4) Defines "stored value" as monetary value representing a claim against the issuer that is stored on an electronic or digital medium and evidenced by an electronic or digital record, and that is intended and accepted for use as a means of redemption for money or monetary value or payment for goods or services. Provides that "stored value" does not include a credit card voucher, letter of credit, or any stored value that is redeemable by the issuer for goods or services provided by the issuer or its affiliate, except to the extent required by applicable law to be redeemable in cash for its cash value. (Financial Code Section 2003(x))

This bill:

1) Prohibits, as of January 1, 2028, a digital wallet provider or money transmitter from allowing a user to log in without using two-factor or multifactor authentication for any log in by that user.

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

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

Comments

1) *Purpose*. According to the author:

   SB 505 strengthens consumer financial protections by requiring digital wallet providers and money transmitters operating in California to use mandatory two-factor authentication (2FA) or multifactor authentication (MFA) for all user logins. The bill is intended to reduce fraud and unauthorized account access by ensuring that stronger authentication measures are consistently applied across platforms.

2) *Background.* This bill seeks to reduce the risk of fraud losses stemming from a relatively small subset of incidences – namely, losses stemming from the unauthorized access of a user's online account with a nonbank payments platform. Unauthorized access refers to an incident where someone other than the accountholder gains access to the account without authorization from the accountholder, such as when one's account is "hacked" or their payments card is stolen or forged. This bill does not cover any products provided by a bank or credit union, such as a checking account or debit card. The bill covers only state-licensed money transmitters. Examples of money transmitters include Western Union, PayPal, and Block (provider of the Square and CashApp payments platforms).

   Notably, accountholders already benefit from protections from losses related to unauthorized account access under the federal Electronic Funds Transfer Act (EFTA). An accountholder who notifies their financial institution within two days of discovering a loss related to unauthorized access is liable up to $50 for the loss, with the financial institution liable for any amount exceeding $50. Despite this protection, many accountholders may be unaware of their obligation to report the loss within specified timelines, which may result in the accountholder bearing a higher loss.[1] Additionally, the accountholder may be unable to access the stolen funds temporarily as their financial institution investigates the alleged incident. Inarguably, the accountholder would be better off if the unauthorized access never occurred in the first place, but EFTA provides a meaningful safety net for accountholders in cases of unauthorized account access.

   Due to the liability associated with unauthorized account access, financial institutions employ various security methods to protect against unauthorized

[1] The specific contours of accountholder liability under EFTA are beyond the scope of this analysis, but suffice it to say, an accountholder may incur liability of up to $500 in cases where reporting to the financial institution does not occur within two days of the accountholder gaining knowledge of the loss(es).

access. Many (if not all) financial institutions that offer online access to financial products or services require the accountholder to provide a username and password to access the online platform. In addition to a username and password, many institutions require another form of authentication, particularly when a user enters the username and password using an electronic device that is not already associated with the account. Additionally, some financial institutions require additional authentication when a user initiates certain types of higher-risk transactions within the online platform, such as person-to-person payments which have been subject to growing rates of fraud in recent years. This bill seeks to mandate that an accountholder provide at least two forms of authentication each time the accountholder logs into the online platform.

Multifactor authentication can reduce the frequency of unauthorized account access, but it does not eliminate the risk. Some forms of multifactor authentication rely on sending a one-time access code to an accountholder's phone or email address. Yet this form of authentication provides little additional security benefit if the unauthorized person has already compromised the accountholder's digital electronic device, phone number, or email account. Moreover, many types of frauds and scams do not rely on gaining access directly to a victim's account; rather, the criminal attempts to fraudulently induce the victim into initiating funds transfers under false pretenses. Multifactor authentication does little, if anything, to prevent this large and growing area of financial vulnerability.

3) *Considerations for the author*. The desire to reduce financial losses from unauthorized account access is understandable, but the author may consider the trade-offs presented by a blanket requirement for at least two-factor authentication for every log in by an accountholder. As a baseline, the author may consider that financial institutions strive to achieve two broad goals that are not always aligned: account security and a positive user experience. As the financial institution imposes stricter access requirements on the user, the user may find the process more time consuming and cumbersome, leading to less satisfaction in the product or service. Additionally, the liability imposed on a financial institution by EFTA provides financial incentive to enhance account security, which provides additional assurance that the financial institution is not overly weighted towards providing the least burdensome user experience by sacrificing security.

   If the author deems the current incentive structure to be insufficiently protective of accountholders' interests, the author may consider whether a more tailored requirement for multifactor authentication is preferable to the blanket

requirement proposed by this bill, where multifactor authentication is required for each log in. Conversations with the financial institutions covered by this bill may help to identify a more targeted and balanced approach or may reveal information that suggests the financial institutions are striking a reasonable balance between account security and user experience under current law.

If the author decides to pursue the current approach or a more tailored one, this bill has drafting deficiencies that should be remedied. For example, there appears to be no benefit to distinguishing between "two-factor authentication" and "multifactor authentication," the bill defines "user login" when that terms is not used anywhere else in the bill, the bill refers to "digital wallet provider" but does not define that term, and the bill does not expressly recognize that accountholders may access their account in-person, such as via an agent who can facilitate a money transfer, and that the requirements of this bill should only apply when accessing an account digitally (assuming that is the intent of the author).

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

SUPPORT: (Verified 1/20/26)

Rise Economy

OPPOSITION: (Verified 1/20/26)

None received

ARGUMENTS IN SUPPORT: According to Rise Economy, "SB 505 strikes a thoughtful balance between innovation and consumer protection. It supports a more secure financial ecosystem while ensuring that Californians can continue to benefit from convenient digital payment options without unnecessary risk. The bill also provides ample time for implementation, giving businesses the opportunity to comply in a responsible and effective manner."

Prepared by: Michael Burdick / B. & F.I. / (916)651-4102
1/21/26 16:05:24

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