STATE OF NEW YORK

8677

IN SENATE

February 28, 2024

Introduced by Sen. HOYLMAN-SIGAL -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology

AN ACT to amend the general business law, in relation to peer-to-peer mobile payment service security; and to amend the financial services law, in relation to authorizing the financial frauds and consumer protection unit to enforce such provisions

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "Financial App Security Act".

§ 2. The general business law is amended by adding a new section 399-jj to read as follows:

§ 399-jj. Peer-to-peer mobile payment service security. 1. For the purposes of this section:

(a) "Peer-to-peer mobile service" means any app or app service that allows users to send and receive money from their mobile devices through a linked bank account or credit card or debit card using only a recipient's cell phone number or email address.

(b) "Biometric authentication" means either fingerprint or face identification for access to a service, or verification of an in-app action.

2. Every peer-to-peer mobile service shall require users to create a personal identification code associated with the user's account that is a minimum of four alpha-numeric characters associated with the user's account. When certain actions are taken, including but not limited to, actions defined in subdivision four of this section, the personal identification number must be used to authenticate the user's identity. The use of such personal identification code may not be substituted for any form of biometric authentication.

3. Every peer-to-peer mobile service shall require users to set a monetary amount for intended transfers above which the use of a personal identification number will be required to authenticate the user's identity.

EXPLANATION--Matter in **italics** (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD14473-02-4

4. The following actions require use of a personal identification number when using a peer-to-peer mobile service:

(a) any payment transaction initiated by the user exceeding the monetary limit set by said user;

(b) payment transactions initiated by the user that would bring said users twenty-four-hour payment transaction amount exceeding the monetary limit set by said user starting from the first transaction;

(c) payment transactions initiated by the user to another user whose account was created less than twenty-four hours prior to said transaction;

(d) payment transactions initiated by the user that appear suspicious based on said user's behavior and/or geolocation profile as determined by the service's existing behavioral analytics;

(e) any payment transactions initiated by the user after three successful payment transactions initiated by the user have been made within sixty minutes for amounts under the user's set monetary limit;

(f) any attempt to sign in to the service by the user to a new and/or unrecognized device;

(g) any attempt to sign in to the service after the account password has been reset in any manner, including but not limited to, password recovery service offered by the service; and

(h) any attempt to sign in to the service by the user after the device password has been reset.

5. A user's account will be locked after five unsuccessful attempts within a twenty-four hour period to input said user's personal identification number when required. The peer-to-peer mobile service can unlock said account after twenty-four hours if said user is able to verify their identity through a telephone call.

6. Any payment transactions initiated by the user after three successful payment transactions initiated by the user have been made within sixty minutes after the first successful payment for amounts, despite the input of the user's correct personal identification number, will have a forty-eight hour hold before the funds will be released to the recipient if:

(a) any of the transactions exceeds the user's set monetary limit; or

(b) the aggregate amount of the transactions exceeds the user's set monetary limit.

7. Any transaction placed on a forty-eight-hour hold can be cancelled by the user making the payment in the event of fraud or user-error after timely notification is made to the peer-to-peer mobile service.

8. Any peer-to-peer mobile service that does not comply with this section is prohibited from offering its services to users residing in the state of New York.

§ 3. Subsection (b) of section 403 of the financial services law is amended to read as follows:

(b) The financial frauds and consumer protection unit shall be a qualified agency, as defined in section eight hundred thirty-five of the executive law, to enforce the provisions of this article and article four of the insurance law and article II-B of the banking law and section 399-jj of the general business law.

§ 4. This act shall take effect on the sixtieth day after it shall have become a law.