Date of Hearing: May 2, 2011

ASSEMBLY COMMITTEE ON BANKING AND FINANCE
Mike Eng, Chair
AB 1080 (Calderon) – As Amended: April 25, 2011

SUBJECT: Internet transactions: verification: banking and financial services.

SUMMARY: Requires a business that provides banking or other financial services over the internet to implement and maintain reasonable policies and procedures for authenticating and verifying the legitimacy of a consumer transaction over the internet. Specifically, this bill:

1) Provides for the policies and procedures that a business implements shall at a minimum be consistent with the best industry practices promulgated by the Federal Financial Institutions Examination Council.

2) Requires a business that allows the movement of funds or change of personal account information over the Internet to utilize an out of band, two factor authentication solution to ensure strong authentication and identity management of user performing transactions and accessing financial account information over the Internet.

3) Applies to transactions over the Internet that result in:

    a) The movement of funds to a new entity, account, or destination that is not a bill pay recipient recognized by the business in an established list of payment recipients;

    b) A transfer to a previously established recipient account that is inconsistent with prior payments sent to that account or that is 200% or greater than any previous payment to that account;

    c) An update of account information; or,

    d) The establishment of a new account or line of credit.

4) Authorizes a civil penalty in the amount of $3,000 may be imposed on a business that fails to conduct an Internet transaction with a consumer in compliance with the policies and procedures.

5) Allows consumers injured by a fraudulent transaction to institute a civil action to recover damages.

6) Exempts any entity regulated by the Department of Insurance excluding any entity that is regulated by both the Department of Insurance and the Department of Financial Institutions.

7) Defines "accessing financial account information" as any change to the information association with an account that risks exposing the consumer to monetary loss.

8) Defines "consumer" as any person or entity that is a customer of a business providing banking or other financial services.

9) Defines "out-of-band, two-factor authentication" as a matter of confirming the details of an online financial services transaction and the identity of its initiator shall employ a communications channel other than the Internet.

10) Defines "payment order" as either an actual, specific instruction to pay a specific amount to a specific payee, or the enrollment of that payee as an entity that is eligible for valid payment as some future time. If the latter is authenticated by multiple separate means then subsequent payments to that entity are not included in this definition and are not subject to this section

11) Defines "strong authentication" as a conformation via a communication channel other than the Internet of both the identity of the initiator of a transaction and the details of that transaction are those intended by the initiator.

12) Defines "update of account information" to include but is not limited to a change in any of the following:

    a) Profile information, including addresses, telephone number, and e-mail addresses;

    b) Payee or payroll information; or,

    c) Any other information that may place the account holder's funds at risk.

EXISTING FEDERAL LAW:

1) Establishes Regulation E, the Electronic Fund Transfer Act to establish the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services. The primary objective of the act and this part is the protection of individual consumers engaging in electronic fund transfers. (*12 C.F.R. § 205.1)*

2) Requires banks, savings associations, and credit unions to verify the identity of customers opening new accounts. (See e.g. 31 CFR Section 103.121, implementing section 326 of the USA PATRIOT Act, 31 USC Section 5318(l).)

3) Requires banks and savings associations to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family, or household purposes, with whom the institution has a continuing relationship. (See Interagency Guidelines Establishing Information Security Standards, implementing section 501(b) of the Gramm-Leach-Bliley Act, 15 USC 6801.)

EXISTING STATE LAW:

1) Makes it unlawful to knowingly access and, without permission, alter, damage, delete, destroy, or otherwise use any data, computer, computer system, or compute network to (1)

devise or execute a scheme to fraud or extort, or (2) wrongfully control or obtain money, property, or data. (Penal Code Section 502.)

2) Makes it unlawful to willfully use someone else's personal identifying information for an unlawful purpose, including obtaining or attempting to obtain credit, goods, services, or medical information in the name of the other person without that person's consent. (Penal Code Section 530.5.)

3) Requires a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices in order to protect the personal information from unauthorized access, use, modification, or disclosure. (Civil Code Section 1798.81.5.)

4) Requires commercial Web site operators and online services that collect personally identifiable information about California residents to conspicuously post their privacy policy on their Web site, or in the case of an online service, to make that policy available to the public. (Business & Professions Code Section 22575.)

FISCAL EFFECT: None.

COMMENTS:

AB 1080 requires businesses that provide banking or other financial services over the internet to follow three components: to implement and maintain reasonable policies and procedures for authenticating and verifying the legitimacy of a consumer transaction made over the Internet; to at a minimum be consistent with the best industry practices promulgated by the Federal Financial Institutions Examination Council (FFEIC); and, utilize an out-of-band, two factor authentication. If a business does not follow the above requirements a consumer can recover civil damages.

AB 1080 defines "out of band, two factor authentication" as a manner of confirming the details of an online financial services transaction and the identity of its initiator shall employ a communications channel other than the internet. This measure would ultimately require a business that provides financial services over the internet to use other means outside the internet to confirm the electronic transaction, for example a phone call.

This measure essentially freezes in time a method used for online security purposes. As technology evolves and hackers become more innovative, this measure would still require an out-of-band, two factor authentication. Rather than allowing businesses to research and determine what security method is best for them, this legislation makes this decision for them. The federal government currently does not regulate a specific form of security to be used by all businesses who conduct financial services over the Internet, rather they offer guidelines through the FFIEC. The FFIEC issues voluntary guidelines regarding a variety of customer verification techniques, including passwords, security questions, smart cards, biometrics, and "out-of-band "authentication (i.e. verification through some means other than an Internet transmission, such as a follow up phone call). FFIEC, established on March 10, 1979, is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System

(FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions.

The FFEIC made the following statement in December, 2010, "the Agencies are aware of the fact that a number of institutions are requiring the "out-of-band" authentication or verification of certain high value and/or anomalous transactions. Out-of-band authentication means that a transaction that is initiated via one delivery channel (e.g., Internet) must be re-authenticated or verified via an independent delivery channel (e.g., telephone) in order for the transaction to be completed. Out-of-band authentication is becoming more popular given that customer PCs are increasingly vulnerable to malware attacks. However, out-of-band authentication directed to or input through the same device that initiates the transaction may not be effective since that device may have been compromised. For business customers, the out-of-band authentication or verification can be provided by someone other than the person who first initiated the transaction and can be combined with other administrative controls. The use of out-of-band authentication or verification, for administrative changes to online business accounts, can be an effective control to reduce fraudulent funds transfers."

ARGUMENTS IN SUPPORT:

According to the Author, AB 1080 is needed to prevent the wrongful access of financial accounts. Cyber-attacks are becoming more frequent and much more sophisticated. Unfortunately, banking and financial services have fallen behind when it comes to protecting consumer accounts. Consumers mistakenly believe that the industry implements the latest technology in hacker defense, but this is not the case. Several publications have illustrated the problems with using the current, and very popular, username/password and computer Internet address. Under this method, a user logs in using a username and password. The e-mail notification for the computer internet address will generally only appear if the user initiates a login on a different computer. For most of the time, the customer accesses information using a single-factor authentication method – username/password. This method is outdated and ill equipped to handle many of the new cyber-attacks methods.

ARGUMENTS IN OPPOSITION:
According to the California Credit Union League, new technologies emerge every day which constantly transform consumer needs- this makes defining technologies in statue a constraint on the types of services financial institutions will be able to provide on the Internet. Defining technologies in statute would eliminate choice and prohibit financial institutions from exploring current and future technologies that could be more cost effective than out-of-band, two factor authentication while still providing the same, if not more protections.

PREVIOUS LEGISLATION:

AB 230 (Calderon, 2010 Legislative Session) would require a business that provides banking or-other financial services over the Internet to implement and maintain-reasonable policies and procedures for authenticating and verifying- the legitimacy of a consumer transaction over the Internet. The bill would authorize the imposition of a civil-penalty and a civil action. Gut and Amend. Withdrawn from Senate Judiciary without further action.

AB 1677(Calderon, 2007 Legislative Session) would require a business that provides banking or other financial services over the Internet to implement and maintain reasonable policies and procedures for authenticating and verifying the legitimacy of a consumer transaction over the Internet, and would require that these policies and-procedures be consistent with current best industry practices. It would allow penalties to be imposed on businesses that fail to meet this requirement. Moved to inactive.

Questions to Consider:

1) Will this bill require businesses that provide banking or financial services over the Internet to use a third party company and if so will this provide an additional loophole for consumer's information to be hacked?

2) As written, this measure would encompass all online stock transactions, is this the intent?

3) Could this measure encourage hackers to focus on California since this law would create one method of security for them to concentrate on?

4) If this measure requires, a third party company, could it actually create job loss at businesses who offer online financial services?

5) A number of phone services use the Internet through voice over internet protocol (VoIP), how would this measure work in these circumstances since the bill eliminates the ability to use the Internet with the out of band two factor authentication?

6) What happens in the case of a joint account, where one person conducted the transfer but the other person is called to verify?

7) What happens when a person makes an electronic transfer from outside the home but the phone number used on the account is a home phone?

8) Who makes the phone call to confirm the transaction? How will the consumer be able to confirm the person calling is who they say they are?

9) This measure puts in statute a specific type of technology to be used for all electronic transfers. What happens when technology evolves or banks find an even better way to protect consumer's information, if enacted, California will still be requiring an out of band two factor authentication?

10) Do any other states require businesses who offer online financial services to use an out of band, two factor authentication?

Suggested amendments:

1) Delete the definition of "payment order"

2) Clarify who the "initiator" is.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

American Express
California Bankers Association
California Chamber of Commerce
California Credit Union League
California Financial Services Association
California Independent Bankers
California Mortgage Bankers Association
California Retailers Association
National Business Coalition
State Farm

Analysis Prepared by: Kathleen O'Malley / B. & F. / (916) 319-3081