Date of Hearing: April 30, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 716 (Chen) – As Introduced February 19, 2019

SUBJECT: Fictitious business name statements.

SUMMARY: This bill would authorize the use of an electronic acknowledgment verifying the identity of the registrant using a remote identity proofing process to ensure the registrant's identification, as specified, for purposes of filing fictitious business name statements with the country clerk. Specifically, **this bill would**:

1) Authorize a county clerk to accept an electronic acknowledgment verifying the identity of the registrant using a remote identity proofing process ensuring the registrant's identification.

2) Require the identity proofing process to follow, to the extent reasonable, the federal guidelines for security and privacy and shall include dynamic knowledge-based authentication, or an identity proofing method consistent with the electronic authentication guidelines of the National Institute of Standards and Technology (NIST).

3) Authorize a county clerk to use a remote identity proofing process for the purposes of presentation for filing of a fictitious business name statements, as specified.

4) Make other technical and non-substantive changes.

EXISTING LAW:

1) Provides for the regulation of individuals or partnerships doing business under fictitious business names. (Bus. & Prof. Code Secs. 17900-17930.)

2) Defines "fictitious business name" to mean the name of a business organization that does not include, depending on the type of business organization, the name of the owners, partners, corporation, limited partnership, or limited liability company. (Bus. & Prof. Code Sec.17900.)

3) Defines "registrant" to mean a person or entity who is filing or has filed a fictitious business name statement, and who is the legal owner of the business. (Bus. & Prof. Code Sec. 17903.)

4) Requires a person that regularly transacts business in this State under a fictitious business name to file a fictitious business name statement. (Bus. & Prof. Code Sec. 17910.)

5) Requires fictitious business name statements to be filed with the clerk of the county in the principal place of business or, if the place of business is not in this State, with the Clerk of Sacramento County. (Bus. & Prof. Code Sec. 17915.)

FISCAL EFFECT: This bill has been keyed nonfiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of the bill**: This bill seeks to streamline the process for registering or renewing fictitious business names with county clerk offices by allowing counties to offer an online registration or renewal process. This bill is sponsored by California Association of Clerks and Election Officials.

2) **Author's Statement**: According to the author, this bill "would allow for a fully-online identification authentication for Fictitious Business Name Statements. This common-sense bill will improve customer service by local agencies, allowing our constituents to save valuable time by eliminating the need for applicants to appear in person to apply for or extend their fictitious business name. This process is commonplace in 2019 and is more than appropriate to offer to the public for this local government service."

3) **Effectiveness concerns of dynamic knowledge-based authentication**: The process of registering a fictitious business name (FBN) with the county clerk's office allows for the creation of a public record of ownership for business that operates under a name that is different than that of the owner(s). The effectiveness of the registry kept by the county clerk's office, however, is only as good as the accuracy of the information that the clerk is provided. To that end, the party seeking to register a FBN is required to show some immediate proof of identity (*e.g.*, state issued identification or proof of incorporation) to the clerk when the party seeks to register or reregister their FBN. Alternatively, as of 2014, county clerks may provide for the use of a notarized "Affidavit of Identity Form" to allow parties to renew or register their FBN without having to show up in person at the clerk's office but still maintain some assurance of the registrants' actual identity. (*See* AB 1325 (Lara, Ch. 238, Stats. 2012).)

   This bill would create a third option for registration utilizing dynamic knowledge-based authentication in place of either physically showing identification or providing a notarized affidavit. In principle, "knowledge-based authentication" is straightforward. It is simply a process for verifying someone's identity by asking them a question that only they (theoretically) know the answer to. This can come in many forms, but the two most prevalent are user names in combination with passwords, and personal knowledge questions such as, what was your high school mascot? These two examples are known as "simple" knowledge-based authentication.

   "Dynamic knowledge-based authentication" does not typically rely on information provided directly from the party. Instead, dynamic knowledge-based authentication relies on questions based on the applying party's record (generally public records) to challenge their identity. Typically, an applicant is presented with a series of addresses or email accounts (or any other piece of identifiable information) and asked to verify which, if any, have been associated with them in the past. This method has the benefit of relying on information provided by sources other than the applicant, but still raises some security concerns given the ubiquity of public information on the internet.

   Simply put, information that dynamic knowledge-based authentication systems most frequently relies on is publically available information. This information can be found using internet searches, public records act requests, and using certain internet services, like PeopleFinder.com. Further, the effectiveness of all knowledge-based authentication systems (dynamic, or otherwise) is increasingly questionable as the rate and scope of data breaches

continues to compound. Specifically, each time a database of account information is breached, the information may become public which leads to the aggregation of username and password combinations, personal challenge questions and answers, email address, physical addresses, and any other information tied to an account. All of this information can then be used to circumvent both simple and dynamic knowledge-based authentication systems.

Available alternatives, however, likely require in-person or "live verification," which requires either having an applicant show their credentials in person (what is nominally required now), or having their credentials verified though a live virtual process that provides similar assurances the applicant is who they say they are. Discounting the former (as that standard would totally defeat the purpose of this bill), the latter is an attractive alternative that comes with potential implementation problems; namely, cost and time.

The live online verification process requires that the applicant be linked to the verifier (clerk) though a live direct video connection, where the applicant video feed is verified to be of a live person and their presentation of verifying documents can be confirmed. Such a process may take a fair amount of time to establish, and would require an implementation cost of either contracting for the verification service through third parties or establishing the technical infrastructure and training clerks to use the system. In addition, this service would arguably only be available to individuals with computers with video capacity, thereby eliminating this option for many individuals with insufficient means to purchase this equipment.

Staff notes that in balancing the risk of fraud against the increase in utility and considering the cost of implementation, it appears that allowing the implementation of dynamic knowledge-based authentication could create an alternative process for the purposes of fictitious name filing and registration that is at least as secure as the current process and will provide increased utility that will arguably benefit some communities and individuals. This bill would also authorize an identity proofing method consistent with the electronic authentication guidelines if NIST, as further discussed below.

4) **Questions about the proper level of assurance in the electronic authentication guidelines**: This bill authorizes the use of an identity proofing method consistent with the electronic authentication guidelines of NIST as an alternative to dynamic knowledge-based authentication. These NIST guidelines offer four levels of authentication protocols elevating in security from one to four. Specifically, the NIST guidelines detail the exact types of threat that each level is resistant against. (NIST, *Electronic Authentication Guidelines* (Aug. 2013); *see* Table on p. 79.) Only level 3 and above protect against phishing and pharming (*i.e.*, verifier impersonation), which is exactly the type of fraud that the FBN in-person or notarized affidavit requirements are designed to prevent. Accordingly, the author has accepted the following amendment to clarify that only level 3 and above authentication are acceptable alternatives. This should arguably ensure that remote verification process is at least as reliable as dynamic knowledge-based verification and still give individual county clerks the flexibility to adopt the best process available.

Suggested amendment:

Page 5, line 25 after "consistent with" insert: "*level 3 identity assurance as described in"*

5) **Prior legislation:** AB 1325 (Lara, Ch. 238, Stats. 2012) allowed county clerks to require a registrant that mails a fictitious business name statement to a county clerk's office for filing to submit a completed and notarized affidavit of identity statement, as specified.

REGISTERED SUPPORT / OPPOSITION:

Support

California Association of Clerks and Election Official (sponsor) `

Opposition

None

Analysis Prepared by: David Watson / P. & C.P. / (916) 319-2200