SB1186 Relating to Personal Information
Summary of Amendments in Senate Committees on Government Operations and Commerce & Consumer Protection

The words “any information in” were removed in the below subsection because they make the definition vague and overbroad, as pointed out in late testimony by the State Privacy & Security Coalition. The phrase unnecessarily broadens the scope to “any information” contained within the described documents, even when much of that information may be widely available. It is more effective to directly state what information should be protected (in this case, application and claims history).

(5) Health insurance information, including but not limited to an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify an individual, or [~~any information in~~] an individual's application and claims history, including any records of appeal; or

The State CIO, the Judiciary, and Hawaii Financial Services Association were in agreement that the removal of “that when used” clarifies the definition of personal information to include the combination of all of the following:

1. an individual's first name or first initial and last name;
2. an online user name, email address, or social media user name or other identifier of a social media account; AND
3. a password.

Removal of the “security question and answer” from this subsection addressed a concern expressed by the Hawaii Information Consortium LLC (HIC). Although this bill has to do with the definition of personal information in the context of a security breach, HIC makes the valid point that providers and agencies within the IT industry shape their mandatory encryption policies based on the definition. It is highly impractical for security questions and answers to be encrypted when they must be readily accessible to staff in the event that users require immediate access to accounts for which they’ve misplaced their access information.

(6) An online user name, email address, or social media user name or other identifier of a social media account [~~that when used~~] in combination with a password [~~or security question and answer~~] that would permit access to an online account.

The below forty-five day requirement was removed due to impracticality and because the statute already provides flexibility to accommodate investigations, a point raised by the Hawaii Financial Services Association. Furthermore, the forty-five day requirement can be perceived as conflicting with the ten-day requirement mention elsewhere in the statute.

... and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system. [~~Notification shall be made no later than forty-five days following the determination of the breach, unless provided otherwise in this section.~~]

The below text was taken out because it would actually remove a tool for notifying users of potential exposure. While it is true that the emails being used to notify users may be the same accounts at risk, that is not always the case in suspected breaches. Furthermore, email may be the only available method of contacting users. Removing a tool is counterproductive when all means of contacting users in the event of a breach should be considered.

(2) Electronic mail notice, for those persons for whom a business or government agency has a valid electronic mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. section 7001; [~~provided that in the case of a security breach involving personal information including or involving the login credential of an email account, the business or government agency shall not provide notification of the breach to that email address and shall instead provide notice by another method set forth in this subsection;~~]

Note: Additional late testimony submitted by the State Privacy & Security Coalition argued that “Account number, credit or debit card number” released by themselves should not be considered personal information. However, this amendment was not made. There exists sufficient public concern over the release of credit and debit card numbers – even by themselves – to warrant continued inclusion of that data in the definition of personal information.