KFS will be implementing an additional layer of security to address an audit finding regarding our system access. Similar to other systems, KFS will ask users to respond to a second-level security question in addition to their userid and password. This type of security is already in place for ePayment and will soon be in place for other UH applications such as Timesheet and Payment System (TAPS). If users do not already have second-level security questions, you will be prompted to set them up the first time you login under the new security method.

The first time a user logs in to KFS, he/she must set up their Level 2 Authentication which consists of 5 second-level security question and answer sets and the selection of an image to be displayed upon subsequent logins. The latter is to reassure the user that the website is legitimate, meaning they should always see their selected image when logging in.

*Note: These challenge/response questions are different from the UH password reset questions.*
For subsequent logins (in the screenshot below), users will be required to answer 1 of 5 of their second-level security questions, and will see the image they initially selected. Users will have 5 chances to answer one of their second-level security questions correctly. If none of their second-level security questions are answered correctly, their account will be locked and will need to be reset by contacting the ITS Help Desk (808-956-8883).

An invalid response to second-level security question will result in an error message that also informs users on how many logins remain before their account is locked.

Note: The user is given the option to edit their second-level security questions/answers and change their image selection on this page (by clicking the checkbox). Information Technology Services (ITS) developed this additional layer of security generically for multiple applications to use. Each user’s questions/answers will be the same for all applications.