Exhibit M-2

ClearStar's Authentication Plan

1.2.   Aurora Website Service

1.2.1.   Password Requirements
Passwords must conform to the following rules:

- Must be at least 8 characters (and no more than 64)
- Must have at least one lower case letter (more than one is fine)
- Must have at least one UPPER CASE letter (more than one is fine)
- Must have at least one number (more than one is fine)
- Must have at least one special or punctuation character, such as $, %, @, !, *, or & (more than one is fine)

1.2.2.   Password Change Frequency
All passwords must be changed after 365 days.

ClearStar Authentication Plan	1

1.2.3.   Lockout
An account must be locked after four unsuccessful authentication attempts.

1.2.4.   Session Timeout
Session timeouts will enforce system/session idle timeouts of 20 minutes. This duration is necessary to support business operations. Due to the formats that various jurisdictions use to return background information, users must spend longer periods of time transcribing text data from paper records into individual text fields.

1.2.5.   Multifactor Authentication
Multiple factor authentication may be applied. In-band multiple factor authentication via email. Out-of-band authentication via cell phone text message.