Gone are temporary passwords!

Great News! Black Knight has developed a more streamlined, user friendly process to handle password reset requests.

The new method introduces a modern design, confirms the user request, and retains flexibility while guiding the user through the process to successfully complete the password reset request.
These changes will be effective with the Paragon 5.71 update. For full details, see below.

Benefits:
1. Incorporates a more user friendly and contemporary design.
   - The email or text message received by the user will indicate that the user can ignore the reset request if he or she did not make it.
   - The user can access the Paragon login page directly from the reset success message.
1. **Adds the ability to confirm the user requesting the password reset, eliminating someone resetting another user's password.**
2. User passwords are not destroyed until the user successfully submits a new password.
   - If a user remembers his or her password after making a reset request he or she can allow the request to expire without affecting the current password.

Change Summary:
1. Temporary passwords will be retired in favor of hyperlinks that redirect the user to a dedicated password reset page.
2. The dedicated password reset page will dynamically alert the user to his or her compliance with the password complexity rules set in Paragon.
3. Administrators will be able to set a user's password manually. The complexity rules will still apply.
   - Administrators no longer have to send vendor password resets to themselves.
   - Administrators may set the user password to any valid combination they choose.
   - Administrators have a backup method of resetting passwords that is not dependent upon users' receipt of an email or text message.