

WHAT IS CLAIMED IS:

- 1 1. A method comprising:
2 receiving, at a service provider computer from a user device, a request to
3 access an account, the request including a device identifier and login credentials;
4 determining, by the service provider computer, whether the account is in a
5 high-risk state or a low-risk state;
6 upon determining that the account is in a low-risk state, and upon
7 determining that the login credentials are valid:
8 generating a verification cookie from the device identifier;
9 providing the verification cookie to the user device for storage in a
10 memory of the user device; and
11 providing access to the account via the user device; and
12 upon determining that the account is in a high-risk state, and upon
13 determining that the login credentials are valid:
14 retrieving the verification cookie from the memory of the user
15 device;
16 determining whether the verification cookie is valid; and
17 providing access to the account via the user device only if the
18 verification cookie is valid.
- 1 2. The method of claim 1, wherein the account is determined to be in
2 a high-risk state if a breach is detected with respect to the account.
- 1 3. The method of claim 1, wherein upon determining that the account
2 is in a high-risk state, and upon determining that the login credentials are valid, the
3 method further comprises completing a password reset process via the user device.
- 1 4. The method of claim 3, wherein the account is placed in a low-risk
2 state upon completing the password reset process.

1 5. The method of claim 1, wherein providing the verification cookie to
2 the user device for storage in the memory of the user device comprises replacing an
3 existing verification cookie stored in the memory of the user device.

1 6. The method of claim 1, wherein the verification cookie is encrypted
2 using a cryptographic key known to the service provider computer.

1 7. The method of claim 1, wherein determining whether the
2 verification cookie is valid comprises determining whether an obscured device identifier
3 in the verification cookie matches the device identifier.

1 8. The method of claim 7, wherein the obscured device identifier is an
2 encrypted version of a device identifier, and wherein determining whether the obscured
3 device identifier matches the device identifier comprises decrypting the obscured device
4 identifier and comparing the decrypted result to the device identifier.

1 9. The method of claim 7, wherein the obscured device identifier is a
2 hashed version of a device identifier, and wherein determining whether the obscured
3 device identifier matches the device identifier comprises hashing the device identifier
4 and comparing the hashed result to the obscured device identifier.

1 10. The method of claim 1, wherein determining whether the
2 verification cookie is valid comprises determining whether a creation date of the
3 verification cookie is before or after a date attributed to a breach detected with respect
4 to the account.

1 11. A service provider computer comprising:
2 a processor; and
3 a memory including instructions that, when executed with the processor,
4 cause the service provider computer to, at least:
5 receive, from a user device, a request to access an account, the
6 request including a device identifier and login credentials;
7 determine a current state of the account;

8 upon determining that the current state of the account is a high-risk
9 state, and upon determining that the login credentials are valid:
10 retrieve the verification cookie from the memory of the user
11 device;
12 determine whether the verification cookie is valid; and
13 provide access to the account via the user device only if the
14 verification cookie is valid.

1 12. The service provider computer of claim 11, wherein the verification
2 cookie has been generated by the service provider computer and provided to the user
3 device in response to a previous request to access the account via the user device.

1 13. The service provider computer of claim 12, wherein the verification
2 cookie has been generated in response to determining that the previous request to
3 access the account via the user device was made while the account was in a low-risk
4 state.

1 14. The service provider computer of claim 11, wherein the instructions
2 further cause the service provider computer to generate a second verification cookie
3 upon determining that the verification cookie is not valid, the second verification cookie
4 indicating that the user device is not authorized to access the account.

1 15. The service provider computer of claim 14, wherein the instructions
2 further cause the service provider computer to, upon receiving the second verification
3 cookie in a subsequent request to access the account, deny access to the account.

1 16. The service provider computer of claim 11, wherein the instructions
2 further cause the service provider computer to, upon determining that the verification
3 cookie is not valid, provide a notification that the login credentials are not valid.

1 17. The service provider computer of claim 11, wherein the instructions
2 further cause the service provider computer to initiate a password reset upon providing
3 access to the account via the user device.

1 18. The service provider computer of claim 11, wherein determining
2 whether the verification cookie is valid comprises determining whether an obscured
3 device identifier included in the verification cookie corresponds to the device identifier.

1 19. The service provider computer of claim 11, wherein the instructions
2 further cause the service provider computer to determine a breach date upon which the
3 account entered the high-risk state and wherein determining whether the verification
4 cookie is valid comprises determining whether the verification cookie was generated
5 after the breach date.