

## CLAIMS

### WHAT IS CLAIMED IS:

1. A system, comprising:  
a non-transitory memory storing instructions; and  
one or more hardware processors coupled to the non-transitory memory and configured to read the instructions from the non-transitory memory to cause the system to perform operations comprising:

determining a device fingerprint of a first device of a first user;

detecting, from the first device of thea first user, an authentication request for an access to an account of a second user in a first application executing on the first device;

processing the authentication request on behalf of the first user using an authentication credential for the account of the second user, wherein the authentication request is processed while preventing viewing of the authentication credential by the first user, wherein processing the authentication request comprises determining that the authentication request is for an application use session of the first application by the first user based on the device fingerprint and a cookie on the first device, wherein the cookie is a stored browser cookie on the first device which is used to track the first user's application use session through the first application and/or an application extension on the first device; and

providing a use of the account of the second user in the first application, wherein the use of the account is limited based on a limitation set by the second user and/or by a service provider managing the account for the use of the account.

2. The system of claim 1, wherein ~~prior to detecting the authentication request, the~~ operations further comprise:

~~determining a device fingerprint of the first device; and~~

determining that the authentication request is for ~~the~~an application use session of the first application further based on at least one of~~by the first user based on at least one of the device fingerprint,~~ a timestamp for the application use session, ~~a cookie on the first device,~~ or a token on the first device.

3. The system of any one of claims 1 or 2, wherein prior to detecting the authentication request, the operations further comprise:

receiving, from the second user, a request for delegation of ~~the account~~the use of the account by the first user, wherein the request comprises the limitation on the use of the account, and wherein the limitation comprises one of a time limit on the use of the account, a purchase amount limit on purchases made using the account, a website use limit for login of the account on a website, an application use limit for the login of the account in an application, or an account access limitation to service provided by the account,

wherein the device fingerprint is determined in response to the request for the delegation of the account use to the first user.

4. The system of any one of claim 1-3, wherein the detecting the authentication request comprises one of receiving a request to enter the authentication credential in a field within the first application, determining a navigation to a webpage within the first application, or determining that the first application is opened on the first device.

5. The system of any one of claims 1-4, wherein prior to detecting the authentication request, the operations further comprise:

using a second application on the first device to monitor the first application for the authentication request, wherein the second application provides a password management service for the system,

wherein the authentication request is detected through the second application, and wherein the processing the authentication request comprises causing the second

application to automatically fill the authentication credential into the authentication request within the first application.

6. The system of claim 5, wherein prior to detecting the authentication request, the operations further comprise:  
notifying the first user of an availability of the account for the use by the first user through the second application, wherein the first user is notified of the availability with the limitation on the use of the account.

7. The system of any one of claims 1-6, wherein the processing the authentication request further comprises:  
detecting that the authentication request requires two-factor authentication;  
~~seraping-determining~~ a code for the two-factor authentication from a message sent to a second device of the second user; and  
processing the authentication request using the authentication credential for the account and the code.

8. The system of any one of claims 1-7, wherein the providing the use of the account comprises monitoring the use of the account within the first application using the cookie and preventing the use of the account if the use violates the limitation.

9. The system of any one of claims 1-8, wherein the operations further comprise:  
receiving a checkout process for a transaction in the first application, wherein the checkout process uses the account for processing the transaction;  
determining whether the transaction complies with the limitation on the use of the account; and  
processing the transaction through the checkout process based on the determining whether the transaction complies with the limitation.

10. The system of any one of claims 1-9, wherein the operations further comprise:

in response to one of an expiration of the use of the account based on the limitation or a violation of the limitation on the use of the account, logging the first application out of the account; and

deleting the authentication credential from the first device.

1140. The system of claim 104, wherein prior to logging the first application out of the account, the operations further comprise:

receiving a request to perform a prohibited action with the account based on the limitation; and

redirecting an interface of the first application to a block notification, wherein the block notification notifies the first user that the prohibited action is prevented based on the limitation.

~~11. The system of claim 1, wherein the operations further comprise:~~  
~~in response to one of an expiration of the use of the account based on the limitation or a violation of the limitation on the use of the account, logging the first application out of the account; and~~

~~deleting the authentication credential from the first device.~~

12. The system of any one of claims 1-11 wherein processing the authentication request further comprises:

determining the application extension for the first application on the first device, wherein the application extension is associated with authenticating the account of the second user on the first device;

automatically entering the authentication credentials for the account to the first application via the application extension; and

inserting the cookie on the first device.

13. The system of any one of claims 1-12, wherein the first application comprises a browser application on the first device, and wherein the detecting, the processing, and the providing are performed through a browser extension provided by the system for the browser application.

14. The system of claim 13, wherein the operations further comprise:  
receiving, through the browser extension, a webpage navigation request to access a webpage associated with changing at least one of personal information for the account or a password of the account;  
preventing, through the browser extension, navigation to the webpage based on the webpage navigation request; and  
displaying, through the browser extension, a message associated with the navigation.

15. A method comprising:  
receiving, by a password management application on a computing device, an authorization for a use of an account by a first user, wherein the account is controlled by a second user;  
receiving a request for the use of the account in a transaction processing application on the computing device;  
fetching, by the password management application, an account credential for the account from an online service provider associated with the account; and  
responsive to the request in the transaction processing application, entering, by the password management application, the account credential to an authentication process for the account in the transaction processing application without revealing the account credential to the first user on the computing device;

wherein when the computing device logs into the second user's account or when the second user delegates usage to the first user and a notification is sent to the computing device, determining by the password management application, a device fingerprint of the computing device; and

determining by the password management application that the request in the transaction processing application is for use of the account by the first user based on the device fingerprint and a cookie on the computing device, wherein the cookie is a stored browser cookie on the computing device which is used to track the first user's use of the account on the computing device through the transaction processing application and/or an extension on the computing device.

16. The method of claim 15, further comprising:  
detecting, using the password management application, a navigation request to access a prohibited account action for the first user; and  
redirecting the transaction processing application to a message alerting the first use of the prohibited account action.

17. The method of claim 16, wherein the prohibited account action comprises one of a password change action, a password reset action, or a view request for financial information stored with the account.

18. A non-transitory machine-readable medium having stored thereon machine-readable instructions executable to cause a machine to perform operations comprising:

receiving, from a computing device of a first user, an indication of a requested authorized use of a website;

determining the first user does not have an account with the website;

determining the first user has an authorization from a second user to use an account of the second user for an authorized use of the website; and

providing, to the website, login credentials for the account of the second user, wherein at least a portion of the login credentials are not shown on the computing device of the first user;

wherein when the computing device logs into the second user's account or when the second user delegates usage to the first user and a notification is sent to the computing device, determining a device fingerprint of the computing device; and

determining that the request authorized use of the website is for a use of the account by the first user based on the device fingerprint and a cookie on the computing device, wherein the cookie is a stored browser cookie on the computing device to track the first user's use of the account on the computing device through the website which is displayed through a browser extension or a transaction processing application on the computing device.

19. The non-transitory machine-readable medium of claim 18, wherein the authorization comprises restrictions set by the second user and/or an entity managing the account of the second user.

20. The non-transitory machine-readable medium of claim 18, wherein the operations further comprise:

detecting an attempt to navigate to a first interface that displays sensitive information for the second user; and

navigating the computing device to a second interface that prevents display of the sensitive information.