WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

receiving, by a first server from a second server, first sensitive information relating to a user having an account with the second server;

in response to receiving the first sensitive information, transmitting, by the first server to the second server, a session identifier and a first Web token, wherein the second server forwards the session identifier to a user device so that the user device can access a data entry page;

providing, by the first server to the user device, a second Web token and the data entry page, wherein the second Web token is used to provide second sensitive information to the first server;

receiving, by the first server from the user device, the second sensitive information via the data entry page and the session identifier, wherein the second sensitive information is different to the first sensitive information; and

associating, by the first server, the first sensitive information with the second sensitive information;

wherein the first server and the second server communicate via a first communication channel and the first server and the user device communicate via a second, different communication channel.

2. The computer-implemented method of claim 1, wherein the first and second Web tokens are different Web tokens.

3. The computer-implemented method of claim 1, further comprising:

receiving, by the first server from the second server, a re-direct URL; and

providing, by the first server to the user device, the re-direct URL, such that a browser of the user device automatically accesses a resource associated with the second server using the re-direct URL after the second sensitive information has been inputted to the data entry page.

4. The computer-implemented method of claim 1, further comprising:

accessing, by the second server, the account of the user; and

obtaining the first sensitive information.

5. The computer-implemented method of claim 1, further comprising:

receiving, by the second server, an identifier of the user, wherein the identifier is associated with the account of the user.

6. The computer-implemented method of claim 1, wherein the first sensitive information comprises a loyalty card identifier.

7. The computer-implemented method of claim 1, wherein the second sensitive information comprises a payment card identifier.

8. The computer-implemented method of claim 6, wherein the first sensitive information comprises a loyalty card number.

9. The computer-implemented method of claim 1, wherein the first server has a database storing a first column including a plurality of first sensitive information including the first sensitive information, and a second column including a plurality of second sensitive information including the second sensitive information.

10. The computer-implemented method of claim 9, wherein the database further comprises a third column comprising a plurality of names corresponding to the plurality of first sensitive information and the plurality of second sensitive information.

11. The computer-implemented method of claim 9, wherein the first Web token and the second Web token are JSON Web tokens.

12. A computer program or a computer program product comprising instructions executable by a processor to cause the processor to perform the computer-implemented method of claim 1.

13. A server computer comprising:

a processor; and

a computer readable medium configured to store executable instructions,

wherein the server computer is configured to communicate with a user device and a second server computer, and the processor is configured to execute the stored executable instructions to:

receive, from the second server computer via a first communication channel, first sensitive information relating to a user having an account with the second server computer;

in response to receiving the first sensitive information, transmit, to the second server computer, a session identifier and a first Web token, wherein the second server computer forwards the session identifier to the user device so that the user device can access a data entry page;

provide, to the user device, a second Web token and the data entry page, wherein the second Web token is used to provide second sensitive information to the server computer;

receive, from the user device, the second sensitive information via the data entry page and the session identifier, wherein the second sensitive information is different to the first sensitive information, wherein the second sensitive information is received via the data entry page and a second, different, communication channel; and

associate the first sensitive information with the second sensitive information.

14. The server computer of claim 13, configured to:

host the data entry page accessible by the user device and configured to receive the second sensitive information.

15. The server computer of claim 13, wherein the first and second Web tokens are different Web tokens.

16. The server computer of claim 13, wherein the processor is configured to execute the stored executable instructions to:

receive, from the second server computer via the first communication channel, a re-direct URL; and

provide, to the user device via the second, different, communication channel, the re-direct URL, such that a browser of the user device automatically accesses a resource associated with the second server computer using the re-direct URL after the second sensitive information has been inputted to the data entry page.

17. A system comprising a client computer, a first server and a second server,
wherein the first server comprises a first processor, and a first non-transitory computer readable medium comprising code, executable by the first processor to:

interact with the second server and the client computer via respective data transfer channels;

receive, from the second server via the respective data transfer channel, first sensitive information relating to a user having an account with the second server and associated with the client computer;

in response to receiving the first sensitive information, transmit, to the second server, a session identifier and a first Web token, wherein the second server forwards the session identifier to the client computer so that the client computer can access a data entry page;

provide, to the client computer, a second Web token and the data entry page accessible by the client computer, wherein the second Web token is used to provide second sensitive information to the first server.

provide the data entry page accessible by the client computer;

receive, from the client computer via the respective data transfer channel, second sensitive information associated with the user via the data entry page and the session identifier, wherein the second sensitive information is different to the first sensitive information; and

link the first sensitive information with the second sensitive information;

wherein the client computer comprises a third processor, and a third non-transitory computer readable medium comprising code, executable by the third processor to:

access the data entry page to allow the user to input the second sensitive information into the data entry page; and

provide the second sensitive information to the first server via the respective data transfer channel;

wherein the second server comprises a second processor, and a second non-transitory computer readable medium comprising code, executable by the second processor to:

identify the account of the user;

retrieve the first sensitive information relating to the user using the identified account; and

send the first sensitive information to the first server via the respective data transfer channel.

18. The system of claim 17, wherein:

the client computer is configured to:

use the second Web token to provide the second sensitive information to the first server.