

WHAT IS CLAIMED IS:

1. A method for double anonymization of data, comprising:
receiving, by a receiving device of a first computing system, a plurality of first data sets, each first data set including at least a set identifier and including personally identifiable information;
anonymizing, by the first computing system, each of the first data sets, wherein anonymizing includes at least replacing the set identifier included in each first data set with a hashed identifier and deidentifying the personally identifiable information, where the hashed identifier is generated via the application of one or more hashing algorithms to at least the corresponding set identifier;
electronically transmitting, by a transmitting device of the first computing system, the plurality of anonymized first data sets to a receiving device of a second computing system, wherein the second computing system is distinct and separate from the first computing system;
anonymizing, by the second computing system, each of the anonymized first data sets, wherein anonymizing includes at least replacing the hashed identifier with a double-hashed identifier, the double-hashed identifier being generated via application of one or more hashing algorithms to at least the corresponding hashed identifier; and
storing, in the second computing system or a third separate and distinct computing system, the plurality of double anonymized first data.
2. The method of claim 1, wherein,
if the double anonymized data sets are stored in the third computing system, the third computing system is controlled by a separate entity from the first computing system and second computing system, and
if the double anonymized data sets are stored in the second computing system, the second computing system is controlled by a separate entity from the first computing system.
3. The method of claim 1, wherein the second computing system does not receive or possess personally identifiable information.

4. The method of claim 1, wherein the first computing system is configured to discard the personally identifiable information subsequent to the deidentification.
5. The method of claim 1, wherein the one or more hashing algorithms used by the first computing system and the second computing system include at least one different hashing algorithm.
6. The method of claim 1, wherein the hashed identifier is generated via the application of one or more hashing algorithms to the corresponding set identifier and a first salt value.
7. The method of claim 6, wherein the double-hashed identifier is generated via application of one or more hashing algorithms to the corresponding hashed identifier and a second salt value.
8. The method of claim 7, wherein the one or more hashing algorithms used by the first computing system and the second computing system are equivalent.
9. The method of claim 7, wherein the first computing system does not receive or possess the second salt value, and the second computing system does not receive or possess the first salt value.
10. The method of claim 1, wherein each first data set includes data related to an electronic payment transaction, the set identifier is a primary account number used in the related electronic payment transaction, and the personally identifiable information is comprised of the primary account number.
11. A system for double anonymization of data, comprising:
a first computing system; and
a second computing system, wherein

first computing system is configured to

receive, by a receiving device of the first computing system, a plurality of first data sets, each first data set including at least a set identifier and including personally identifiable information,

5 anonymize each of the first data sets, wherein anonymizing includes at least replacing the set identifier included in each first data set with a hashed identifier and deidentifying the personally identifiable information, where the hashed identifier is generated via the application of one or more hashing algorithms to at least the corresponding set identifier, and

10 electronically transmit, by a transmitting device of the first computing system, the plurality of anonymized first data sets to a receiving device of a second computing system, wherein the second computing system is distinct and separate from the first computing system, and

 the second computing system is configured to anonymize each of the
15 anonymized first data sets, wherein anonymizing includes at least replacing the hashed identifier with a double-hashed identifier, the double-hashed identifier being generated via application of one or more hashing algorithms to at least the corresponding hashed identifier, wherein

 the plurality of double anonymized first data sets is stored in the second
20 computing system or in a distinct and separate third computing system.

12. The system of claim 11, wherein

 if the double anonymized data sets are stored in the third computing system, the third computing system is controlled by a separate entity from the first computing
25 system and second computing system, and

 if the double anonymized data sets are stored in the second computing system, the second computing system is controlled by a separate entity from the first computing system.

30 13. The system of claim 11, wherein the second computing system does not receive or possess personally identifiable information.

14. The system of claim 11, wherein the first computing system is configured to discard the personally identifiable information subsequent to the deidentification.

5 15. The system of claim 11, wherein the one or more hashing algorithms used by the first computing system and the second computing system include at least one different hashing algorithm.

10 16. The system of claim 11, wherein the hashed identifier is generated via the application of one or more hashing algorithms to the corresponding set identifier and a first salt value.

15 17. The system of claim 16, wherein the double-hashed identifier is generated via application of one or more hashing algorithms to the corresponding hashed identifier and a second salt value.

18. The system of claim 17, wherein the one or more hashing algorithms used by the first computing system and the second computing system are equivalent.

20 19. The system of claim 17, wherein
the first computing system does not receive or possess the second salt value,
and
the second computing system does not receive or possess the first salt value.

25 20. The system of claim 11, wherein
each first data set includes data related to an electronic payment transaction,
the set identifier is a primary account number used in the related electronic
payment transaction, and
the personally identifiable information is comprised of the primary account
30 number.