CLAIMS

1. A computer-implemented method comprising:

obtaining, by a server system, peer group data indicating: (i) multiple entities classified as belonging to a particular peer group, and (ii) a set of attributes associated with the multiple entities;

obtaining, by the server system and from one or more data sources, transaction data for the multiple entities;

selecting, by the server system, one or more transaction models that are each trained to:

(i) apply a particular set of evidence factors corresponding to the set of attributes associated with the multiple entities, and

(ii) identify transaction patterns representing potentially anomalous activity;

processing, by the server system and using the one or more transaction models, the transaction data for the multiple entities to identify potentially anomalous activity within the transaction data for the multiple entities;

computing, by the server system and for each entity included in the multiple entities, a prioritization indicator based on the processing of the transaction data for the multiple entities, the prioritization indicator representing a likelihood that transaction data for a particular entity includes potentially anomalous activity; and

enabling, by the server system, a user to perceive a representation of the priority indicators.

2. The method of claim 1, wherein:

the set of attributes associated with the multiple entities comprises an attribute representing a business classification shared by the multiple entities;

the one or more transaction models comprises a first machine learning model that is trained to (i) apply a set of evidence factors corresponding to transactions that are frequently performed by entities of the business classification shared by the multiple entities, and (ii) identify potentially anomalous transactions that have a likelihood of representing money laundering transactions; and

the prioritization indicator computed for each entity included in the multiple entities specifies a likelihood that transaction data for a particular entity includes transactions identified as potentially representing money laundering transactions.

3. The method of claim 1, wherein:

the set of attributes associated with the multiple entities comprises an attribute identifying a set of transaction types of transactions that are frequently performed by each entity included in the multiple entities; and

the potentially anomalous activity comprise transactions that have a transaction type that is not included in the set of transaction types of transactions that are frequently performed by each entity included in the multiple entities.

4. The method of claim 1, wherein:

the set of attributes associated with the multiple entities comprises an attribute identifying an average transaction value for transactions that are frequently performed by each entity included in the multiple entities; and

the potentially anomalous activity comprise transactions that have a transaction value exceeding the average transaction value for transactions that are frequently performed by each entity included in the multiple entities.

5. The method of claim 1, wherein the transaction data for each entity included in the multiple entities comprises:

historical transactions associated with a particular entity over a particular time period; and

an identification of reoccurring transactions associated with the particular entity over the particular time period.

6. The method of claim 5, wherein the transaction data for each entity included in the multiple entities further comprises a corpus of documents that are predetermined to satisfy one or more search criteria associated with a negative media search for the particular entity.

7. The method of claim 1, wherein:

the prioritization indicator comprises a score; and

a value of the score represents a number of potentially anomalous transactions included in the transaction data for a particular entity.

8. The method of claim 1, wherein:

the one or more transaction models comprises:

a first transaction model that is trained to (i) apply a first set of evidence factors corresponding to the set of attributes associated with the entities, and (ii) identify a first set of potentially anomalous transactions within a particular set of transactions based on applying the first set of evidence factors,

a second transaction model that is trained to (i) apply a second set of evidence factors corresponding to the set of attributes associated with the entities, and (ii) identify a second set of potentially anomalous transactions within a particular set of transactions based on applying the first set of evidence factors, and

wherein the first set of potentially anomalous transactions and the second set of potentially anomalous transactions represent different types of transaction patterns; and

processing the transaction data for the multiple entities comprises:

processing the transaction data using the first transaction model to identify the first set of potentially anomalous transactions within the transaction data for the multiple entities, and

processing the transaction data using the second transaction model to identify the second set of potentially anomalous transactions within the transaction data for the multiple entities; and

computing the prioritization indicator for each entity included in the multiple entities comprises:

computing, a first prioritization sub-indicator based on processing the transaction data for the multiple entities using the first transaction model, the first prioritization sub-indicator representing a likelihood that transaction data for a particular entity includes one or more of the first set of potentially anomalous transactions, and

computing, a second prioritization sub-indicator based on processing the transaction data for the multiple entities using the second transaction model, the prioritization indicator representing a likelihood that transaction data for a particular entity includes one or more of the second set of potentially anomalous transactions; and

aggregating the first prioritization sub-indicator and the second prioritization sub-indicator to compute the prioritization indicator.

9. The method of claim 8, wherein:

the first set of potentially anomalous transactions identified by the first transaction model comprises transactions involving money laundering; and

the second set of potentially anomalous transactions identified by the second transaction model comprises transactions involving terrorist funding activities.

10. The method of claim 1, wherein:

the transaction data obtained for the multiple entities comprises a volume of transaction information;

processing the transaction data for the multiple entities to identify potentially anomalous activity comprises processing, by the server system, the volume of transaction information such that the potentially anomalous activity within the transaction data for the multiple entities is identified within a first time period after the transaction data for the multiple entities is obtained; and

the first time period is shorter than a second time period required to manually process the volume of transaction information to identify the potentially anomalous activity within the transaction data for the multiple entities.

11. The method of claim 1, wherein:

the transaction data for the multiple entities is periodically obtained by the server system as transaction data instances that are obtained at specified times; and

the transaction data for the multiple entities is processed by the server system by processing each transaction data instance to identify potentially anomalous activity within each transaction data instance for the multiple entities.

12. A system comprising:

one or more computers; and

one or more storage devices storing instructions that, when executed by the one or more computers, cause the one or more computers to perform operations comprising:

obtaining, by a server system, peer group data indicating: (i) multiple

entities classified as belonging to a particular peer group, and (ii) a set of attributes associated with the multiple entities;

obtaining, by the server system and from one or more data sources, transaction data for the multiple entities;

selecting, by the server system, one or more transaction models that are each trained to:

(i) apply a particular set of evidence factors corresponding to the set of attributes associated with the multiple entities, and

(ii) identify transaction patterns representing potentially anomalous activity;

processing, by the server system and using the one or more transaction models, the transaction data for the multiple entities to identify potentially anomalous activity within the transaction data for the multiple entities;

computing, by the server system and for each entity included in the multiple entities, a prioritization indicator based on the processing of the transaction data for the multiple entities, the prioritization indicator representing a likelihood that transaction data for a particular entity includes potentially anomalous activity; and

enabling, by the server system, a user to perceive a representation of the priority indicators.

13. The system of claim 12, wherein:

the set of attributes associated with the multiple entities comprises an attribute representing a business classification shared by the multiple entities;

the one or more transaction models comprises a first machine learning model that is trained to (i) apply a set of evidence factors corresponding to transactions that are frequently performed by entities of the business classification shared by the multiple entities, and (ii) identify potentially anomalous transactions that have a likelihood of representing money laundering transactions; and

the prioritization indicator computed for each entity included in the multiple entities specifies a likelihood that transaction data for a particular entity includes transactions identified as potentially representing money laundering transactions.

14. The system of claim 12, wherein:

the set of attributes associated with the multiple entities comprises an attribute identifying a set of transaction types of transactions that are frequently performed by each entity included in the multiple entities; and

the potentially anomalous activity comprise transactions that have a transaction type that is not included in the set of transaction types of transactions that are frequently performed by each entity included in the multiple entities.

15. The system of claim 12, wherein:

the set of attributes associated with the multiple entities comprises an attribute identifying an average transaction value for transactions that are frequently performed by each entity included in the multiple entities; and

the potentially anomalous activity comprise transactions that have a transaction value exceeding the average transaction value for transactions that are frequently performed by each entity included in the multiple entities.

16. A non-transitory computer-readable storage device encoded with computer program instructions that, when executed by one or more computers, cause the one or more computers to perform operations comprising:

obtaining, by a server system, peer group data indicating: (i) multiple entities classified as belonging to a particular peer group, and (ii) a set of attributes associated with the multiple entities;

obtaining, by the server system and from one or more data sources, transaction data for the multiple entities;

selecting, by the server system, one or more transaction models that are each trained to:

(i) apply a particular set of evidence factors corresponding to the set of attributes associated with the multiple entities, and

(ii) identify transaction patterns representing potentially anomalous activity;

processing, by the server system and using the one or more transaction models, the transaction data for the multiple entities to identify potentially anomalous activity within the transaction data for the multiple entities;

computing, by the server system and for each entity included in the multiple

entities, a prioritization indicator based on the processing of the transaction data for the multiple entities, the prioritization indicator representing a likelihood that transaction data for a particular entity includes potentially anomalous activity; and

enabling, by the server system, a user to perceive a representation of the priority indicators.

17. The device of claim 16, wherein:

the set of attributes associated with the multiple entities comprises an attribute representing a business classification shared by the multiple entities;

the one or more transaction models comprises a first machine learning model that is trained to (i) apply a set of evidence factors corresponding to transactions that are frequently performed by entities of the business classification shared by the multiple entities, and (ii) identify potentially anomalous transactions that have a likelihood of representing money laundering transactions; and

the prioritization indicator computed for each entity included in the multiple entities specifies a likelihood that transaction data for a particular entity includes transactions identified as potentially representing money laundering transactions.

18. The device of claim 16, wherein:

the set of attributes associated with the multiple entities comprises an attribute identifying a set of transaction types of transactions that are frequently performed by each entity included in the multiple entities; and

the potentially anomalous activity comprise transactions that have a transaction type that is not included in the set of transaction types of transactions that are frequently performed by each entity included in the multiple entities.

19. The device of claim 16, wherein:

the set of attributes associated with the multiple entities comprises an attribute identifying an average transaction value for transactions that are frequently performed by each entity included in the multiple entities; and

the potentially anomalous activity comprise transactions that have a transaction value exceeding the average transaction value for transactions that are frequently performed by each entity included in the multiple entities.

20. The device of claim 16, wherein the transaction data for each entity included in the multiple entities comprises:

historical transactions associated with a particular entity over a particular time period; and

an identification of reoccurring transactions associated with the particular entity over the particular time period.