CLAIMS

1. A computer-implemented method comprising:

obtainingtraining, by a server system, at least (i) a transaction model to apply a first set of evidence factors to identify potentially anomalous activity associated with an activity pattern type;

classifying, by the server system and based on a set of attributes of a target entity, the target entity as belonging to at least (i) a first peer group data indicating: (i) multiple of entities classified as belonging to a particular peer group, that share a first set of attributes and (ii) a set of attributes associated with the multiple entities; second group of entities that share a second set of attributes, wherein the first peer group and the second group comprise at least one unique entity that is only included either the first peer group or the second peer group;

obtaining, by the server system and from one or more data sources, transaction data for the multiple target entity, transaction data for entities; included in the first peer group, and transaction data for entities included in the second peer group;

selecting, by the server system, one or morethe trained transaction models that are each trained to: model based on the set of attributes of the target entity;

(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 moretrained transaction modelsmodel, the transaction data for the multipletarget entity in relation to the transaction data for entities included in the first peer group to determine a first indicator for the target entity, wherein the first indicator represents a first classification of normalcy relative to transaction data of the first peer group with respect to the activity pattern type given the first set of attributes;

processing, by the server system and using the trained transaction model, the transaction data for the target entity in relation to the transaction data for entities

included in the second peer group to determine a second indicator for the target entity, wherein:

the second indicator represents a second classification of normalcy relative to transaction data of the second peer group with respect to the activity pattern type given the second set of attributes, and

the second classification of normalcy is different from the first classification of normalcy;

determining, by the server system and based on the first indicator, that transaction data for the target entity is potentially anomalous relative to the first classification of normalcy;

determining, by the server system and based on the second indicator, that transaction data for the target entity is not potentially anomalous relative to the second classification of normalcy;

adjusting, by the server system, the activity pattern type based on determining that transaction data for the target entity is (i) potentially anomalous relative to the first classification of normalcy and (ii) is not potentially anomalous relative to the second classification of normalcy;

generating, by the server system, a second set of evidence factors based on adjusting the activity pattern type;

re-training, by the server system, the transaction model to apply the second set of evidence factors to identify potentially anomalous activity ~~within the transaction data for the multiple entities;~~ associated with the activity pattern type that was adjusted;

computing, by the server system and for ~~each~~the target entity ~~included in the multiple entities~~, a prioritization indicator based at least on combining the ~~processing of~~first indicator and the ~~transaction data for the multiple entities,~~second indicator, wherein the prioritization indicator ~~representing a likelihood that~~is biased towards the first indicator based on transaction data ~~for a particular~~of the target entity ~~includes~~being determined to (i) be potentially anomalous ~~activity~~relative to the first classification of normalcy and (ii) not be potentially anomalous relative to the second classification of normalcy; and

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

2. The method of claim 1, wherein:

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

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

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

3. The method of claim 1, wherein:

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

~~the potentially anomalous activity comprise~~ the first indicator specifies 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~~first peer group.

4. The method of claim 1, wherein:

the first 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 included in the first peer group; and

~~the potentially anomalous activity comprise~~ the first indicator specifies 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~~first peer group.

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

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

~~an~~ 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~~entities included in the ~~multiple entities~~first peer group 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~~the target 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~~ target entity comprises a volume of transaction information;

processing the transaction data for the ~~multiple~~target entity in relation to the transaction data for entities ~~to identify potentially anomalous activity~~included in the first peer group to determine the first indicator for the target entity 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~~first indicator is determined within a first time period after the transaction data for the ~~multiple~~ entities included in the first peer group 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~~determine the ~~potentially anomalous activity~~first indicator within the transaction data for the ~~multiple~~ entities included in the first peer group.

~~11.~~ 9. The method of claim 1, wherein:

the transaction data for ~~the multiple~~ entities included in the first peer group 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 included in the first peer group is processed by the server system by processing each transaction data instance to ~~identify potentially anomalous activity within~~determine the first indicator associated with each transaction data instance for ~~the multiple~~ entities included in the first peer group.

~~12.~~ 10. 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~~training, by a server system, at least (i) a transaction model to apply a first set of evidence factors to identify potentially anomalous activity associated with an activity pattern type;

classifying, by the server system and based on a set of attributes of a target entity, the target entity as belonging to at least (i) a first peer group ~~data indicating: (i) multiple~~ of entities ~~classified as belonging to a particular peer group,~~ that share a first set of attributes and (ii) a ~~set of attributes associated with the multiple entities;~~ second group of entities that share a second set of attributes, wherein the first peer group and the second group comprise at least one unique entity that is only included either the first peer group or the second peer group;

obtaining, by the server system and from one or more data sources, transaction data for the ~~multiple~~ target entity, transaction data for entities~~;~~ included in the first peer group, and transaction data for entities included in the second peer group;

selecting, by the server system, ~~one or more~~the trained transaction ~~models that are each trained to:~~ model based on the set of attributes of the target entity;

~~(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~~trained transaction ~~models~~model, the transaction data for the ~~multiple~~target entity in relation to the transaction data for entities included in the first peer group to determine a first indicator for the target entity, wherein the first indicator represents a first classification of normalcy relative to transaction data of the first peer group with respect to the activity pattern type given the first set of attributes;

processing, by the server system and using the trained transaction model, the transaction data for the target entity in relation to the transaction data for entities included in the second peer group to determine a second indicator for the target entity, wherein:

the second indicator represents a second classification of normalcy relative to transaction data of the second peer group with respect to the activity pattern type given the second set of attributes, and

the second classification of normalcy is different from the first classification of normalcy;

determining, by the server system and based on the first indicator, that transaction data for the target entity is potentially anomalous relative to the first classification of normalcy;

determining, by the server system and based on the second indicator, that transaction data for the target entity is not potentially anomalous relative to the second classification of normalcy;

adjusting, by the server system, the activity pattern type based on determining that transaction data for the target entity is (i) potentially anomalous relative to the first classification of normalcy and (ii) is not potentially anomalous relative to the second classification of normalcy;

generating, by the server system, a second set of evidence factors based on adjusting the activity pattern type;

re-training, by the server system, the transaction model to apply the second set of evidence factors to identify potentially anomalous activity ~~within the transaction data for the multiple entities;~~ associated with the activity pattern type that was adjusted;

computing, by the server system and for ~~each~~the target entity ~~included in the multiple entities~~, a prioritization indicator based at least on combining the ~~processing of~~first indicator and the ~~transaction data for the multiple entities,~~second indicator, wherein the prioritization indicator ~~representing a likelihood that~~is biased towards the first indicator based on transaction data ~~for a particular~~of the target entity ~~includes~~being determined to (i) be potentially

anomalous ~~activity~~relative to the first classification of normalcy and (ii) not be potentially anomalous relative to the second classification of normalcy; and

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

11. ~~13.~~ The system of claim ~~12~~10, wherein:

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

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

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

12. ~~14.~~ The system of claim ~~12~~10, wherein:

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

~~the potentially anomalous activity comprise~~ the first indicator specifies 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~~first peer group.

13. ~~15.~~ The system of claim ~~12~~10, wherein:

the first 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 included in the first peer group; and

~~the potentially anomalous activity comprise~~ the first indicator specifies 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~~first peer group.

14. ~~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~~training, by a server system, at least (i) a transaction model to apply a first set of evidence factors to identify potentially anomalous activity associated with an activity pattern type;

classifying, by the server system and based on a set of attributes of a target entity, the target entity as belonging to at least (i) a first peer group ~~data indicating: (i) multiple~~ of entities ~~classified as belonging to a particular peer group,~~ that share a first set of attributes and (ii) a ~~set of attributes associated with the multiple entities;~~ second group of entities that share a second set of attributes, wherein the first peer group and the second group comprise at least one unique entity that is only included either the first peer group or the second peer group;

obtaining, by the server system and from one or more data sources, transaction data for the ~~multiple~~ target entity, transaction data for entities~~;~~ included in the first peer group, and transaction data for entities included in the second peer group;

selecting, by the server system, ~~one or more~~the trained transaction ~~models that are each trained to:~~ model based on the set of attributes of the target entity;

~~(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~~trained transaction ~~models~~model, the transaction data for the ~~multiple~~target entity in relation to the transaction data for entities included in the first peer group to determine a first indicator for the target entity, wherein the first indicator represents a first classification of normalcy relative to transaction data of the first peer group with respect to the activity pattern type given the first set of attributes;

processing, by the server system and using the trained transaction model, the transaction data for the target entity in relation to the transaction data for entities included in the second peer group to determine a second indicator for the target entity, wherein:

the second indicator represents a second classification of normalcy relative to transaction data of the second peer group with respect to the activity pattern type given the second set of attributes, and

the second classification of normalcy is different from the first classification of normalcy;

determining, by the server system and based on the first indicator, that transaction data for the target entity is potentially anomalous relative to the first classification of normalcy;

determining, by the server system and based on the second indicator, that transaction data for the target entity is not potentially anomalous relative to the second classification of normalcy;

adjusting, by the server system, the activity pattern type based on determining that transaction data for the target entity is (i) potentially anomalous relative to the first classification of normalcy and (ii) is not potentially anomalous relative to the second classification of normalcy;

generating, by the server system, a second set of evidence factors based on adjusting the activity pattern type;

re-training, by the server system, the transaction model to apply the second set of evidence factors to identify potentially anomalous activity ~~within the transaction data for the multiple entities;~~ associated with the activity pattern type that was adjusted;

computing, by the server system and for eachthe target entity included in the multiple entities, a prioritization indicator based at least on combining the processing offirst indicator and the transaction data for the multiple entities,second indicator, wherein the prioritization indicator representing a likelihood thatis biased towards the first indicator based on transaction data for a particularof the target entity includesbeing determined to (i) be potentially anomalous activityrelative to the first classification of normalcy and (ii) not be potentially anomalous relative to the second classification of normalcy; and

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

15. 17. The device of claim 1614, wherein:

the set of attributes associated withof the multiple entitiestarget entity comprises an attribute representing a business classification shared by the multiplefirst set of entities;

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

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

16.

18. The device of claim 1614, wherein:

the first set of attributes associated with the multiple entities included in the first peer group comprises an attribute identifying a set of transaction types of transactions

that are frequently performed by each entity included in the ~~multiple entities~~first peer group; and

~~the potentially anomalous activity comprise~~ the first indicator specifies 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~~first peer group.

17. ~~19.~~ The device of claim ~~16~~14, wherein:

the first 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 included in the first peer group; and

~~the potentially anomalous activity comprise~~ the first indicator specifies 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~~first peer group.

18. ~~20.~~ The device of claim ~~16~~14, wherein the transaction data for ~~each entity~~entities included in the ~~multiple entities~~ first peer group 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.

19. The method of claim 1, wherein training the transaction model to apply the first set of evidence factors to identify the potentially anomalous activity associated with the activity pattern type comprises:

obtaining a training dataset comprising a set of transaction patterns that are predetermined to be associated with potentially anomalous activity;

classifying each of the set of transaction patterns as corresponding to a particular activity pattern type;

selecting, from among the set of transaction patterns, one or more transaction patterns that are classified as corresponding to the activity pattern type; and

training the transaction model to apply the set of first evidence factors based on the one or more transaction patterns that were selected from among the set of transaction patterns.

20. The method of claim 19, wherein after training the transaction model to the apply the first set of evidence factors, the method further comprises:

determining, by the server system, a change to transaction activity patterns associated with the activity pattern type;

selecting, from among the set of transaction patterns, one or more updated transaction patterns that are re-classified as corresponding to the activity pattern based on the change to transaction activity patterns associated with the activity pattern type; and

re-training the transaction model to apply the first set of evidence factors based on the one or more updated transaction patterns that were selected from among the set of transaction patterns.

21. The method of claim 1, further comprising:

identifying, by the server system, one or more attributes of the target entity that have changed after the target entity classified to the first peer group of entities and the second group of entities; and

adjusting, by the server system, a peer group classification for the target entity based on the one or more attributes of the target entity that have changed after the target entity classified to the first peer group of entities and the second group of entities.

22. The method of claim 21, wherein adjusting the peer group classification for the target entity based on the one or more attributes comprises:

reclassifying the target entity to a third peer group of entities that share a third set of attributes, wherein the third set of attributes includes the one or more attributes of the

target entity that have changed after the target entity classified to the first peer group of entities and the second group of entities.

23. The method of claim 1, further comprising:

training, by the server system, a second transaction model to apply a second set of evidence factors to identify potentially anomalous activity associated with a second activity pattern type that is different from the activity pattern type;

classifying, by the server system and based on the set of attributes of the target entity, the target entity to a third peer group of entities that share a third set of attributes;

obtaining, by the server system and from the one or more data sources, transaction data for entities included in the third peer group;

selecting, by the server system, the trained second transaction model based on the second set of attributes;

processing, by the server system and using the trained second transaction model, the transaction data for the target entity in relation to the transaction data for entities included in the third peer group to determine a third indicator for the target entity, wherein the third indicator comprises fraudulent transactions; and

computing the prioritization indicator comprises computing the prioritization indicator based at least on combining the first indicator, the second indicator, and the third indicator.