

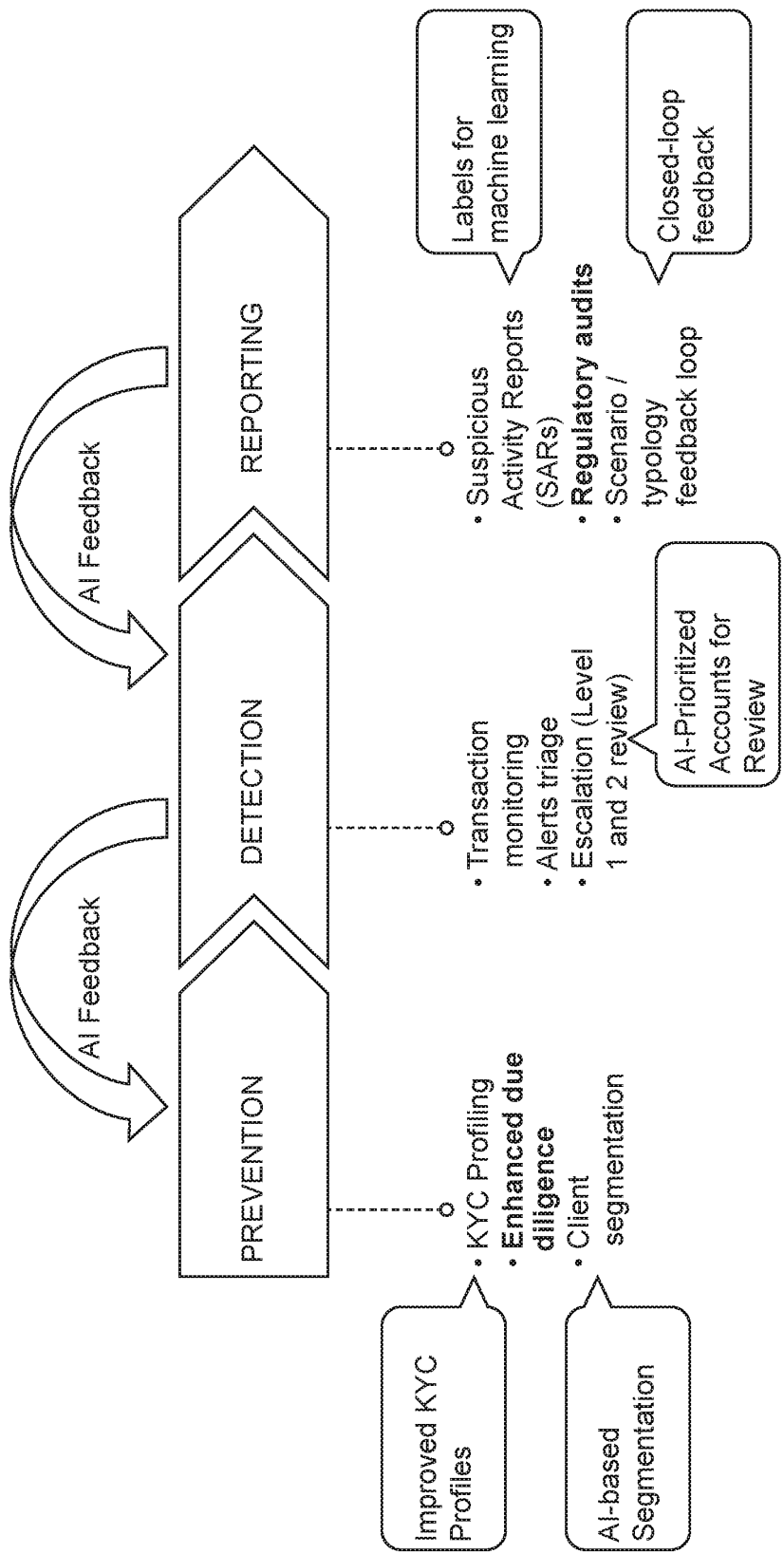


FIG. 1

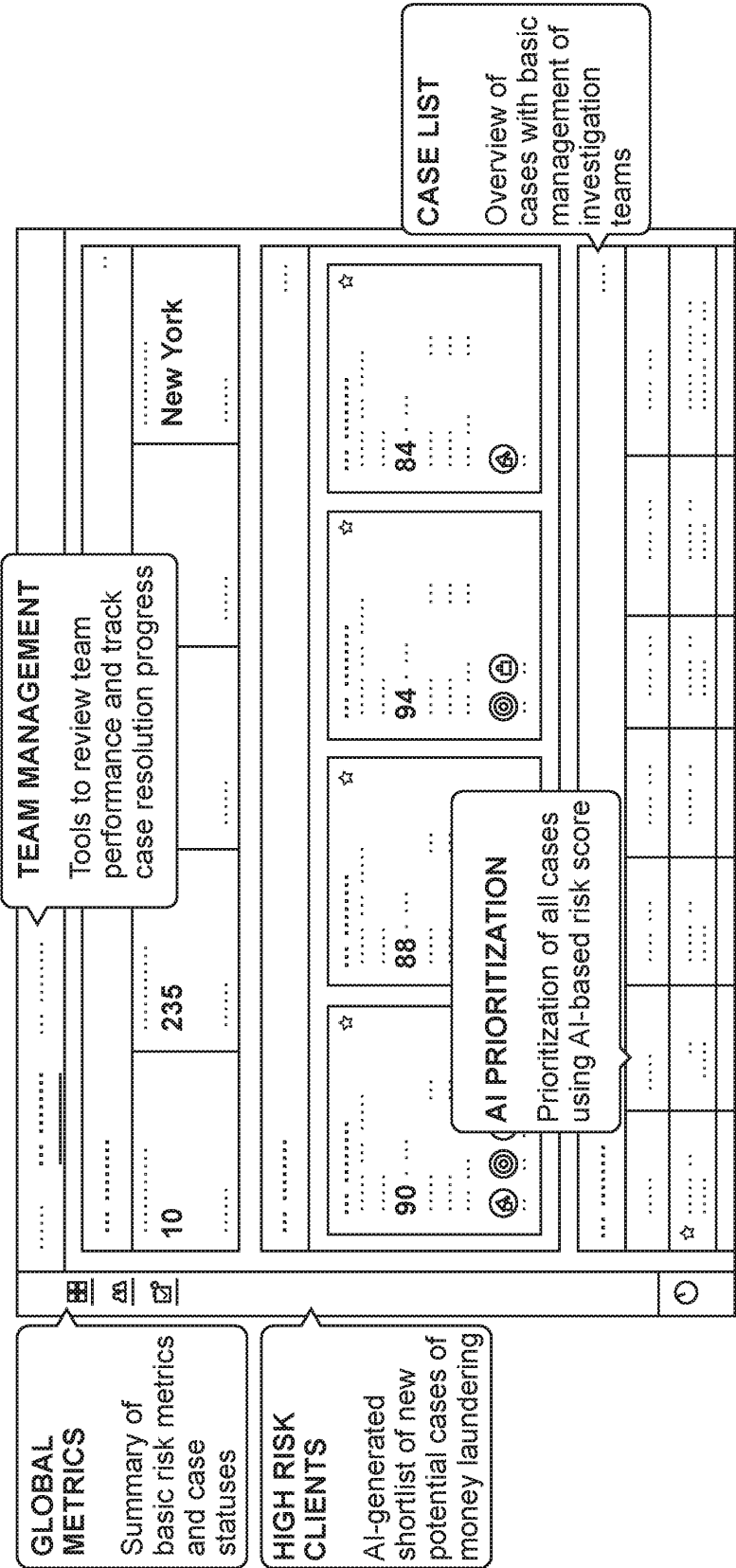


FIG. 2A

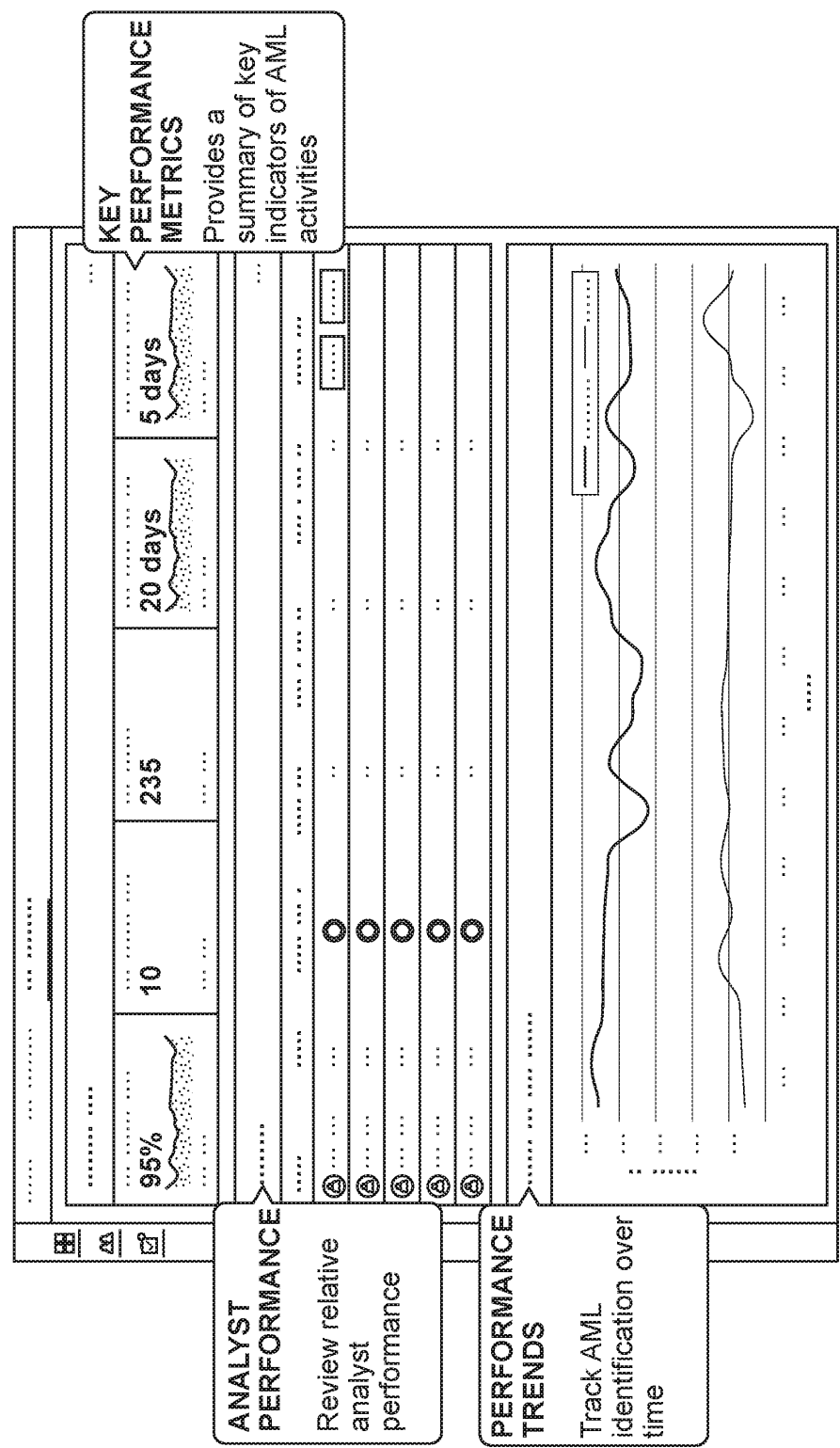


FIG. 2B



FIG. 3

☐				
☐		☒	Account	Last Status Change
			710485470	4/11/2017

Access Quick-View

FIG. 4

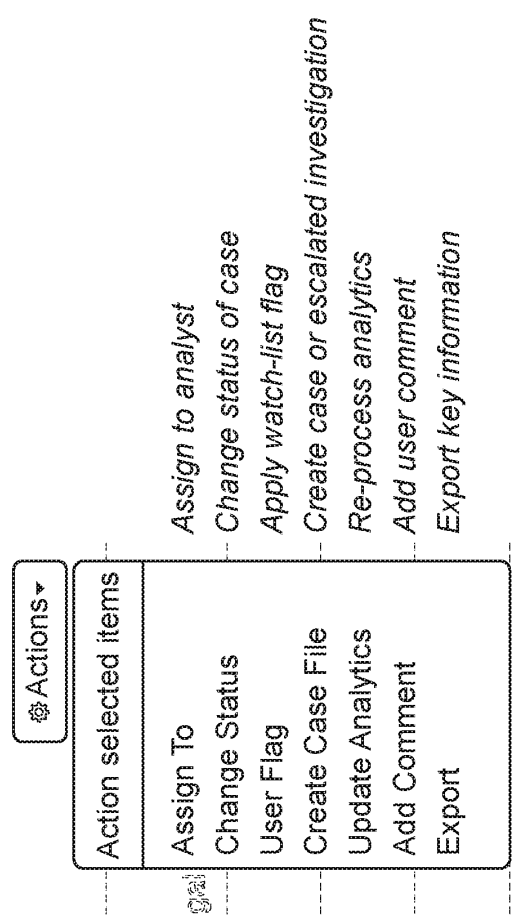


FIG. 5

Create case, add to
watchlist, add comment

Stephen G. Blake ☆		90	3	0	
Structuring					
		5	123	\$2000	
		\$11m			

FIG. 6

User Flag	X
Flag	Watch List X
Close Save	

Alert Name*

Alerts

Tags

X Alert

⊗

▼Choose a timeseries to monitor

Source Type*?

Search or pick...

Filter*?

Search or pick...

Metric*?

Search or pick...

Interval*?

Search or pick...

Browse

⊗

▼Set Trigger Conditions

Alert Threshold*?

>

31

during a period of

Search or pick...

☑

▼Notifications (optional)

To?

Manage Contacts

Name	Subscribe to Email	Subscribe to SMS
Jake	OFF	ON
Scott	ON	OFF

1-2 of 2 items

Message?

Save

Reset

FIG. 8

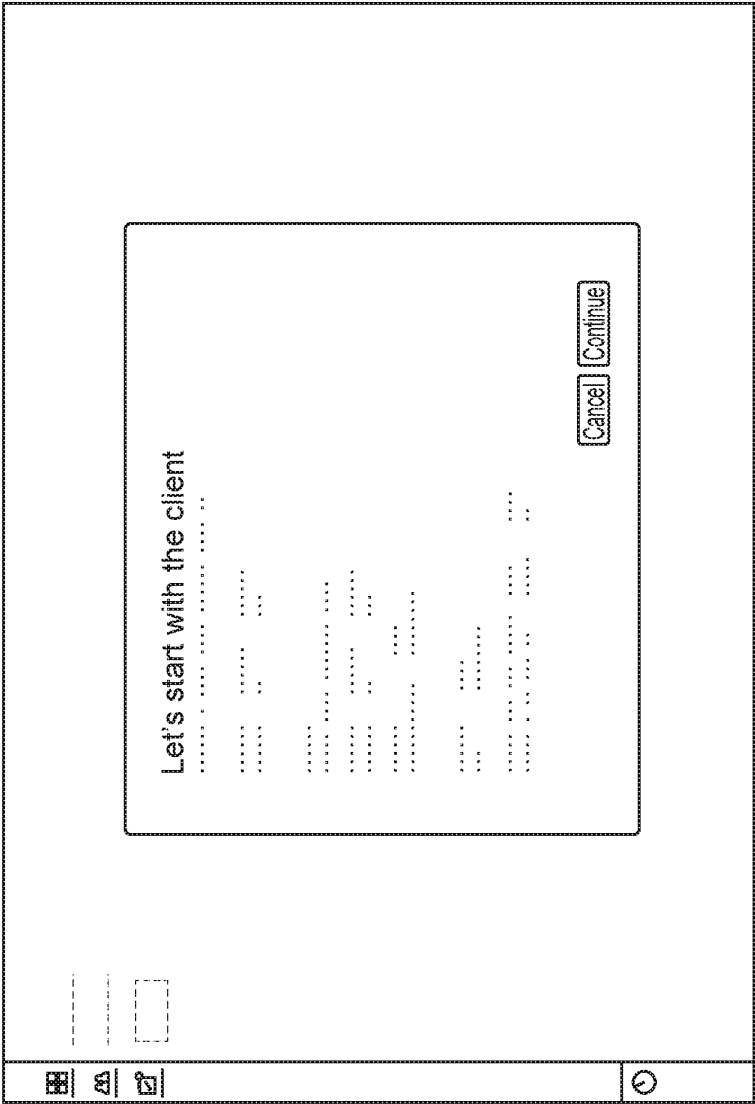


FIG. 9A

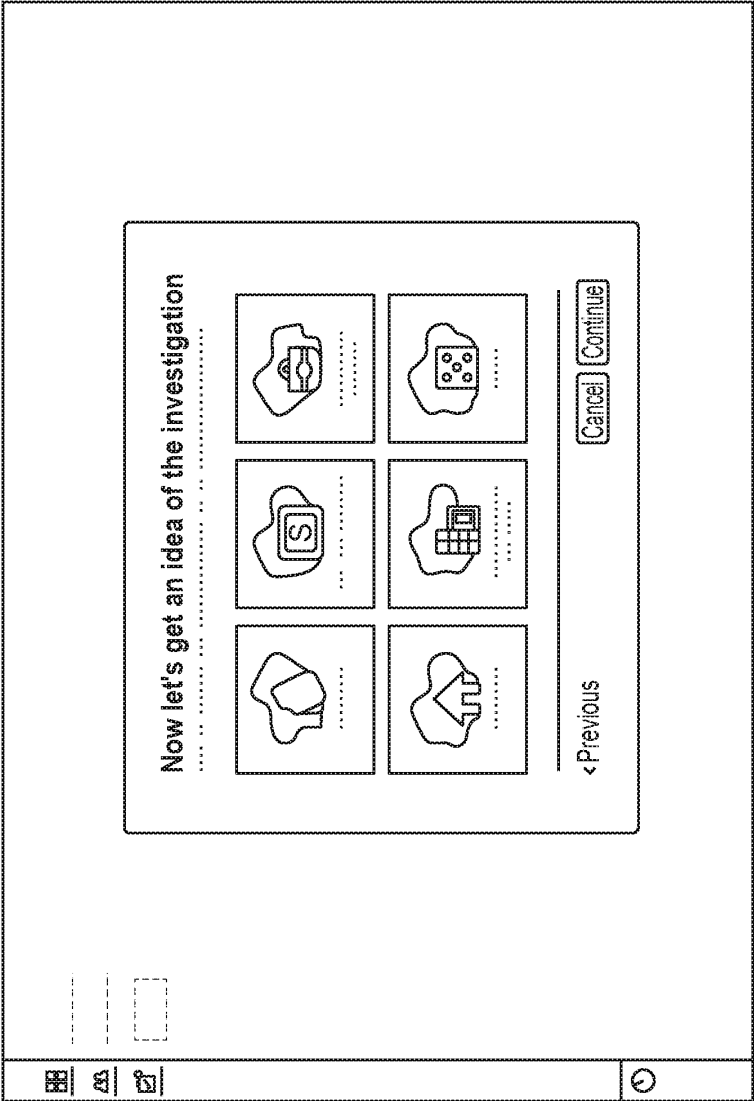


FIG. 9B

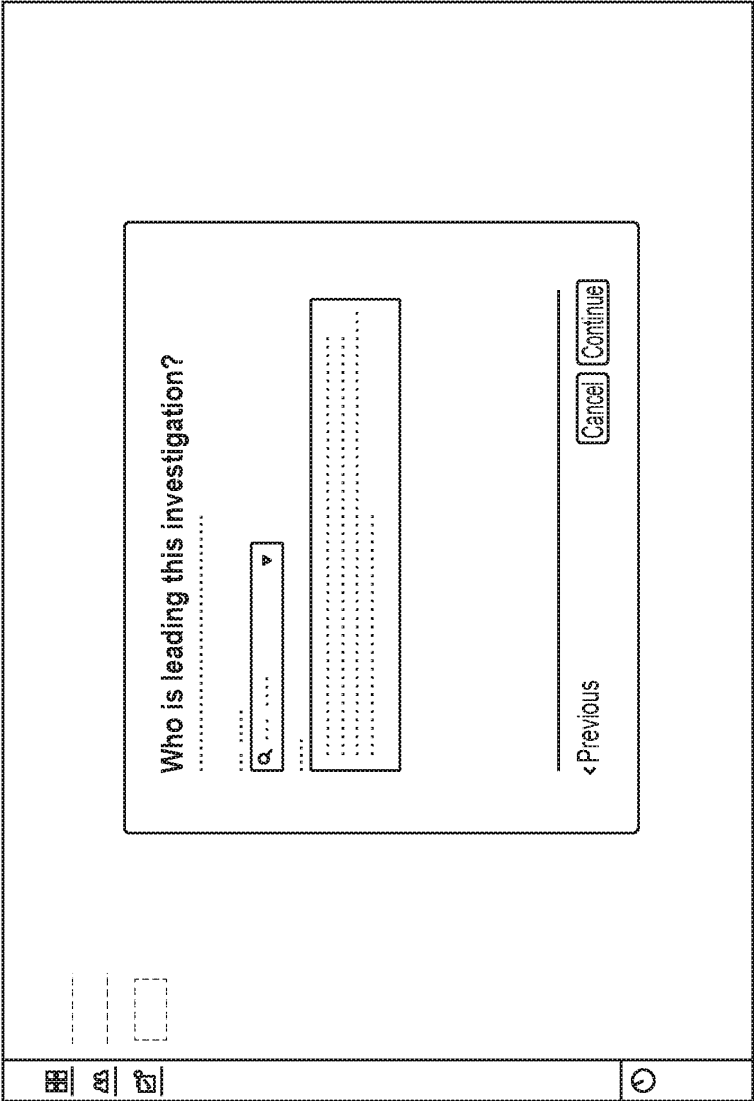


FIG. 9C

MACHINE LEARNING PROCESS

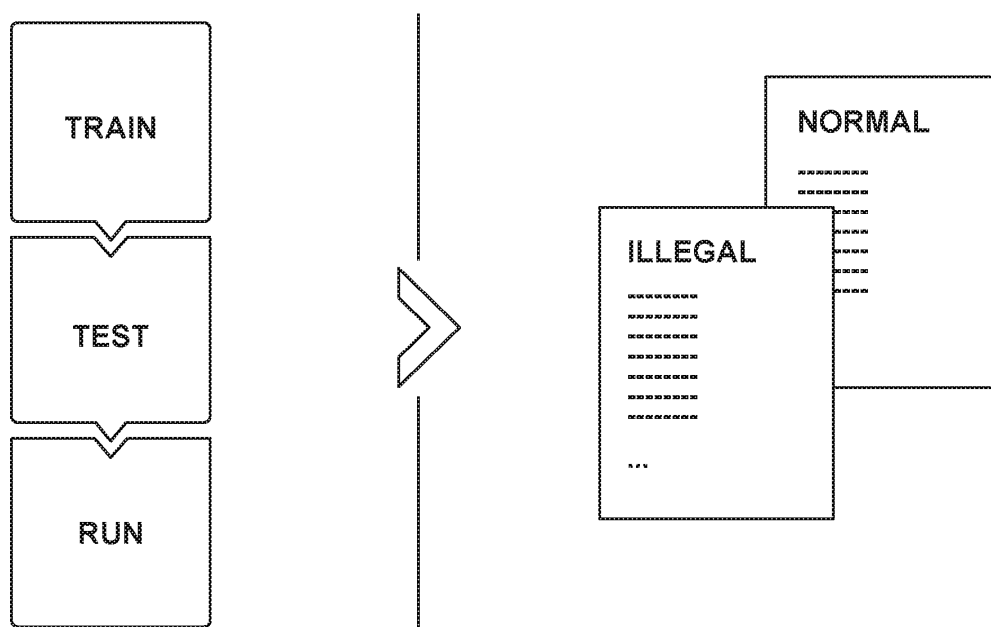


FIG. 10

Machine Learning Features
Account Training Set

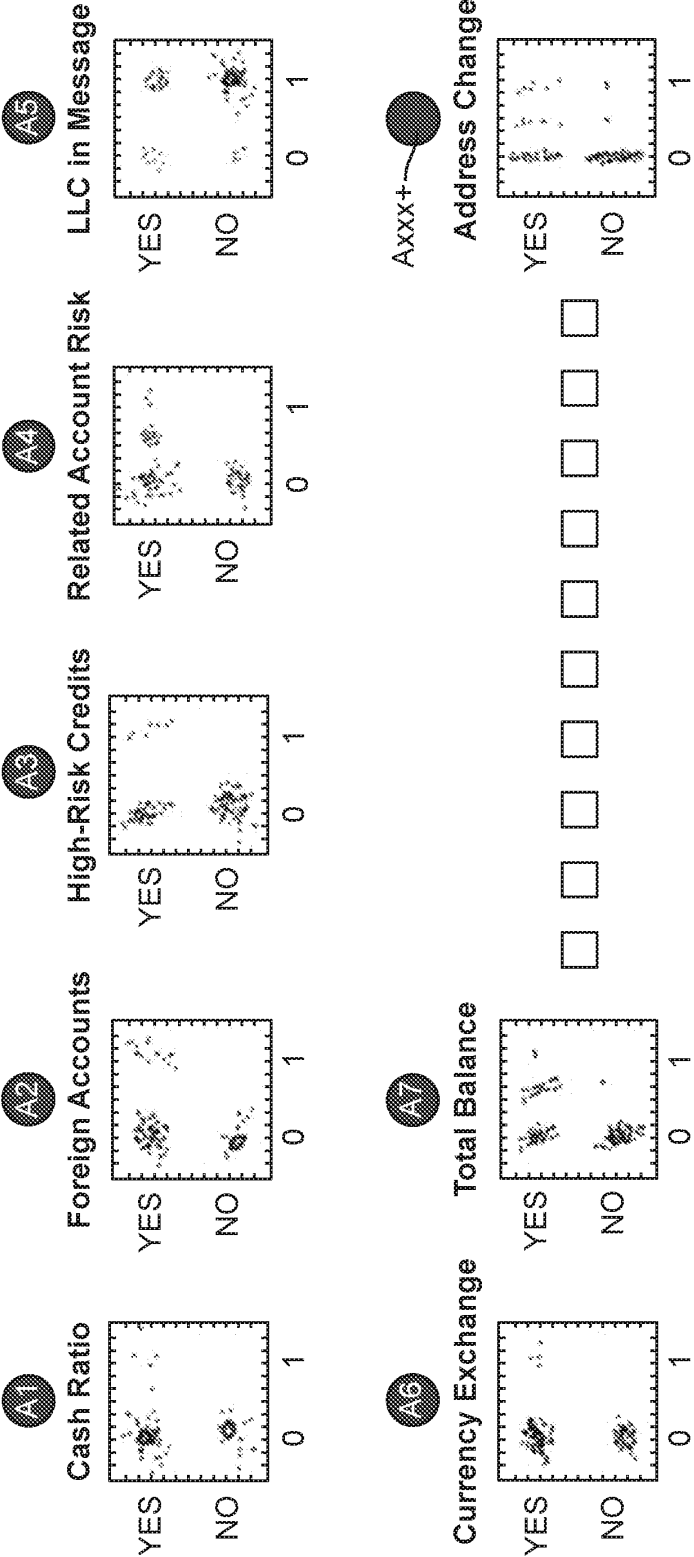


FIG. 11

SUBSTITUTE SHEET (RULE 26)

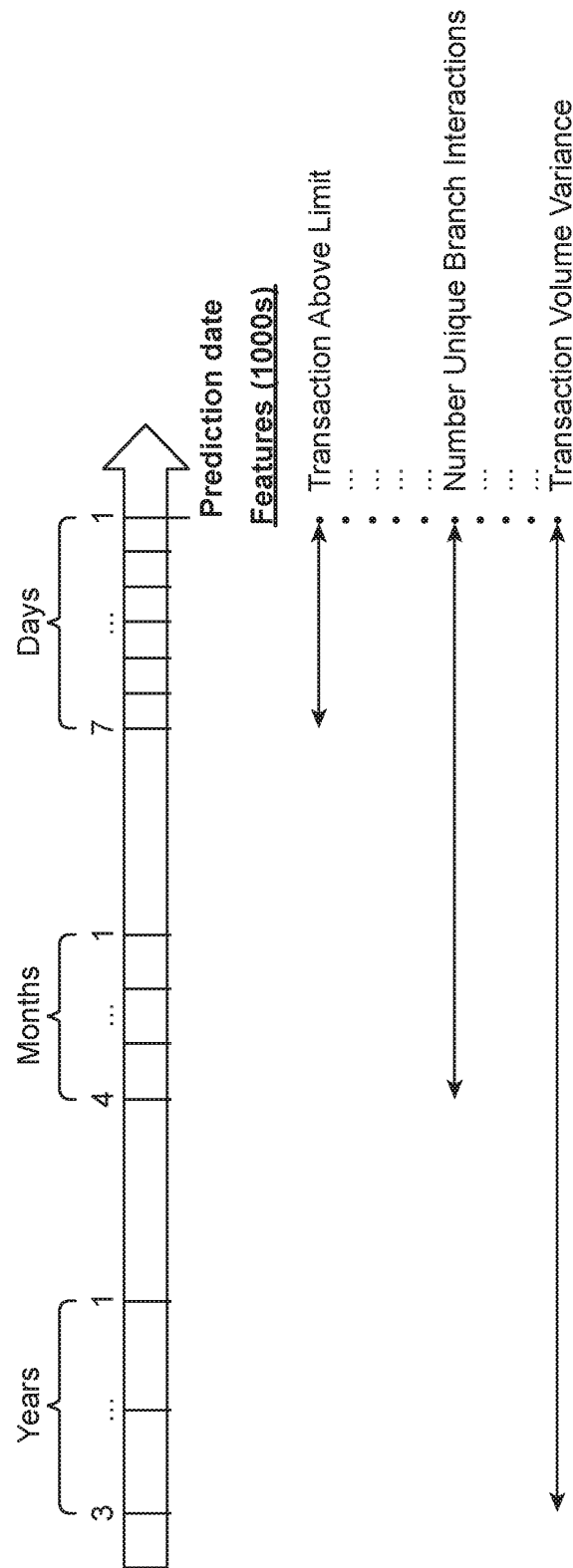


FIG. 12

SUBSTITUTE SHEET (RULE 26)

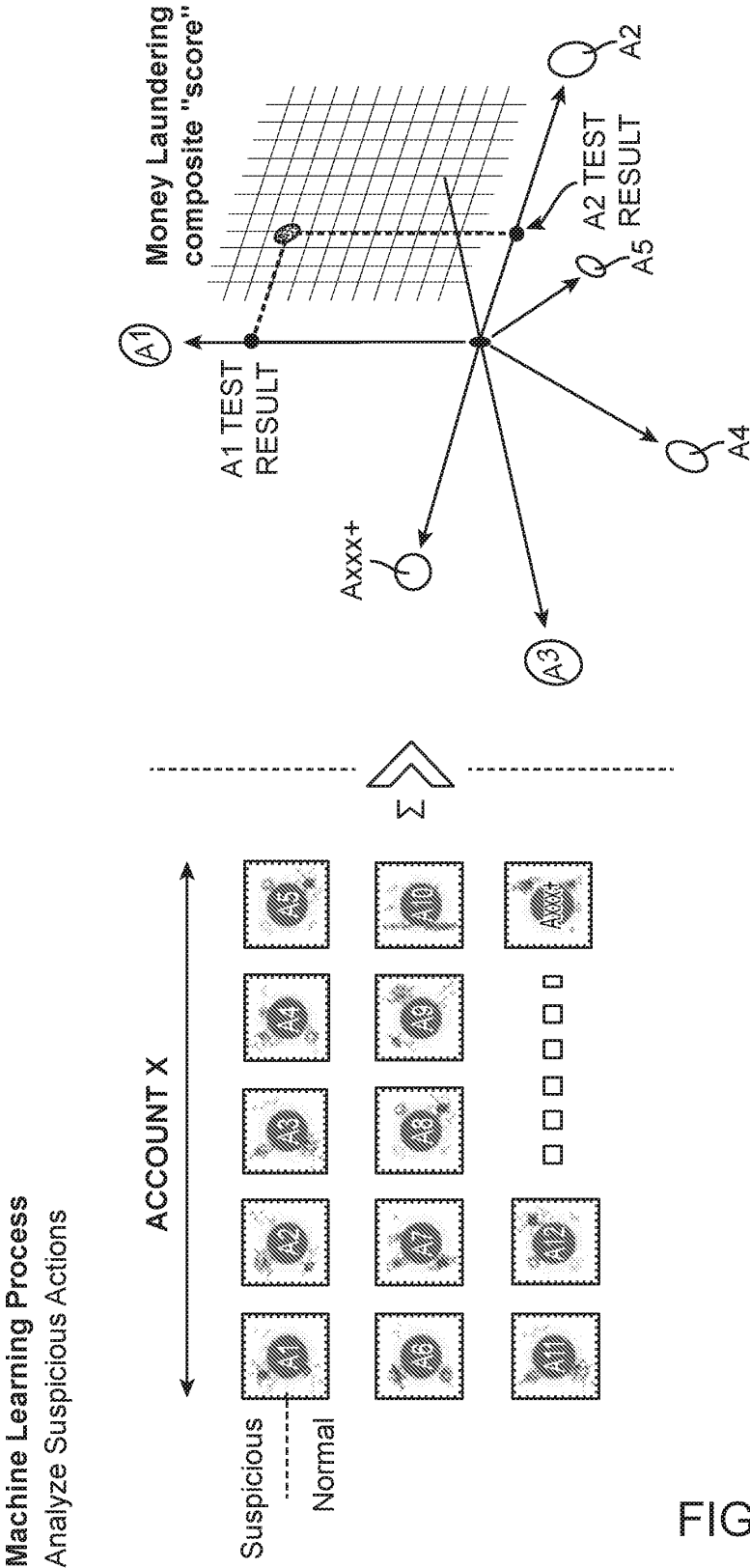


FIG. 13

Machine Learning Process
Machine Learning-Based Lead Classification

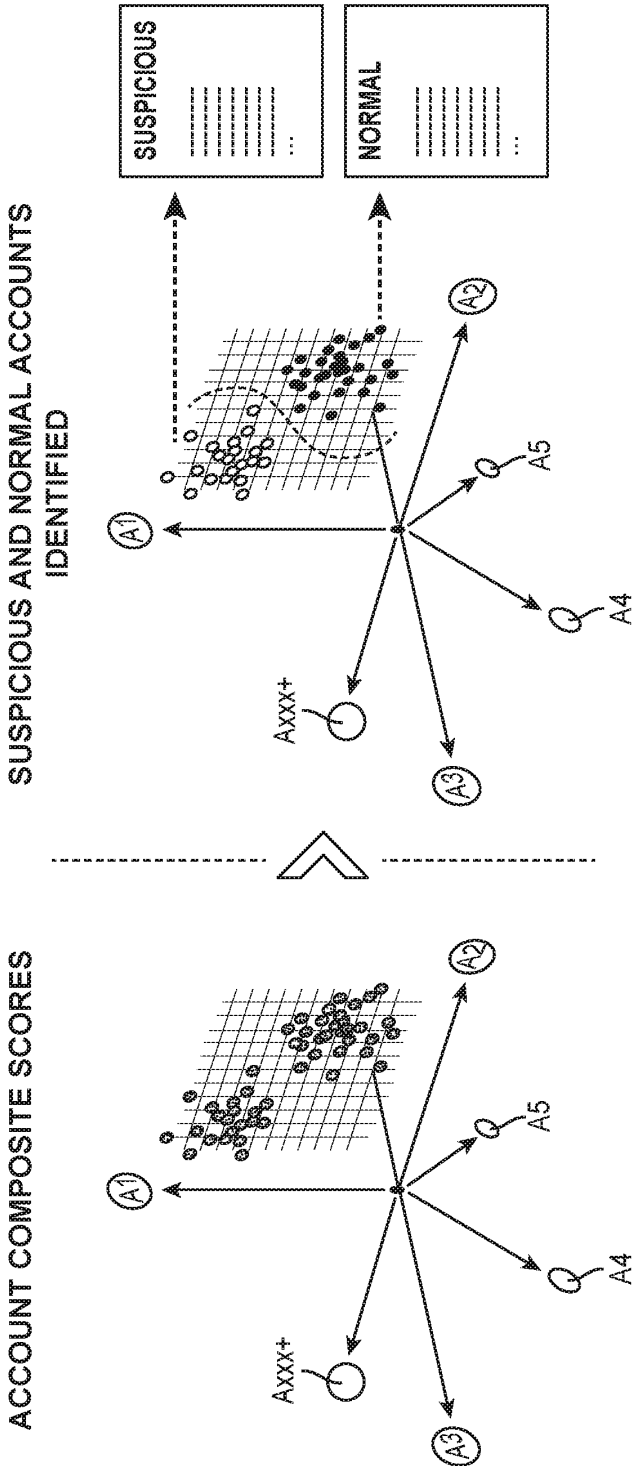


FIG. 14A

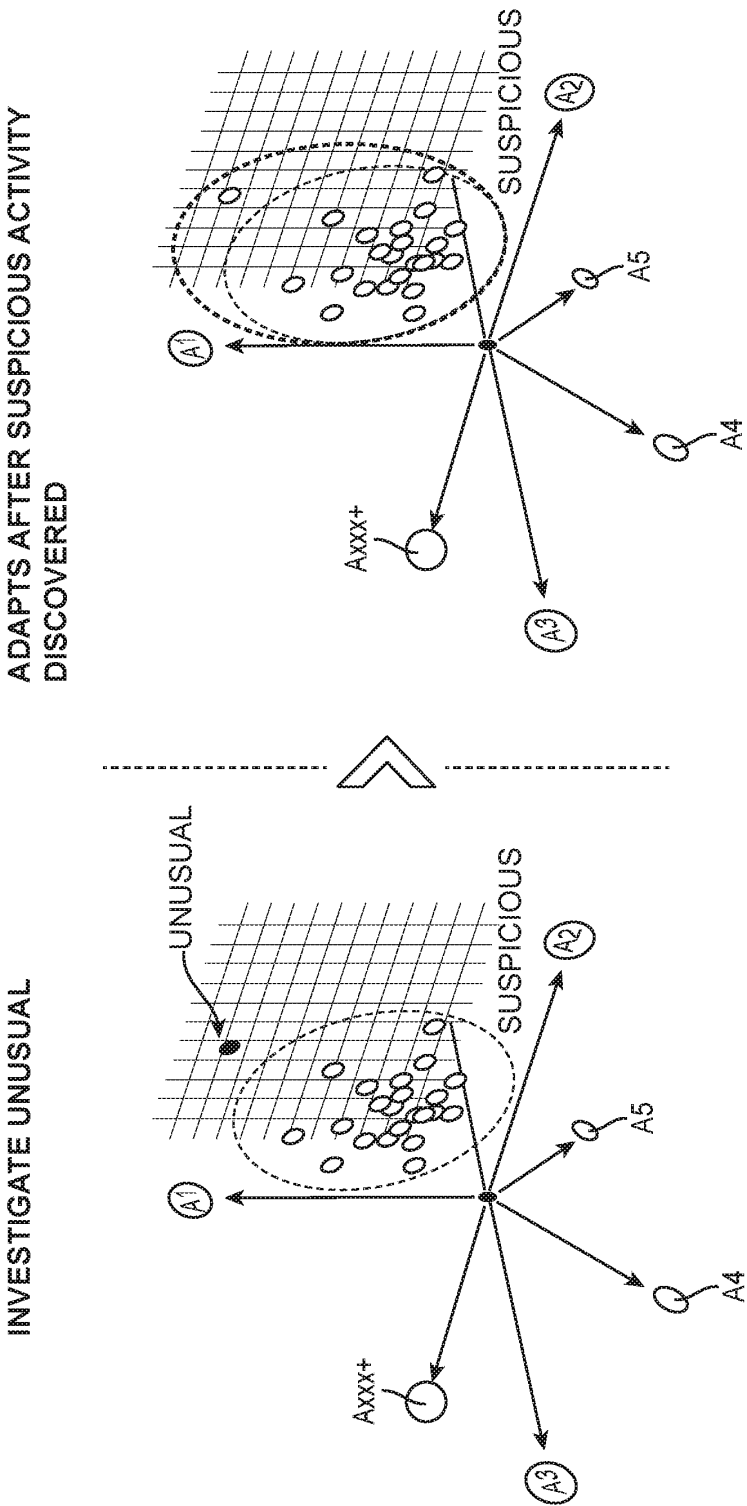


FIG. 14B

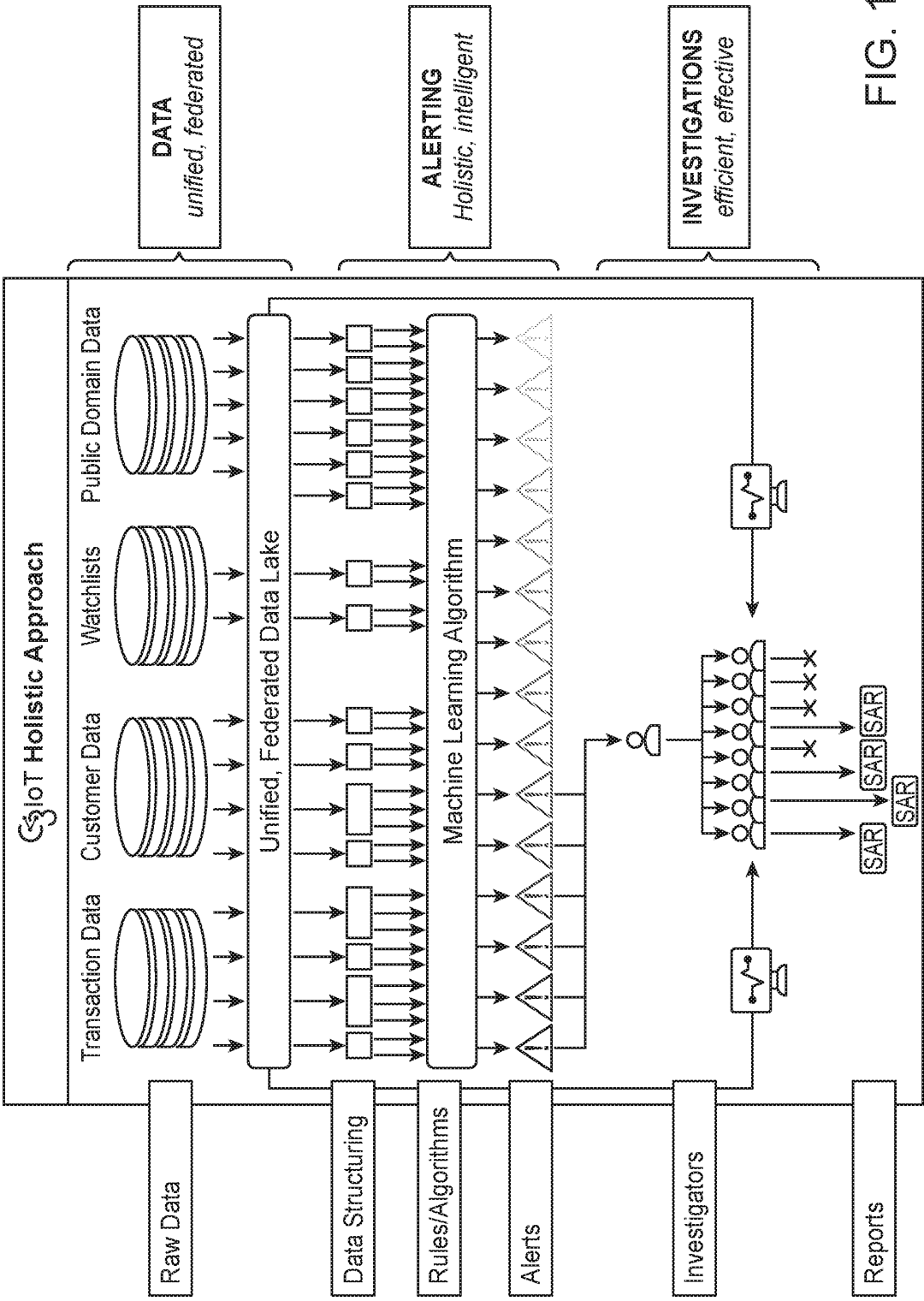


FIG. 14C

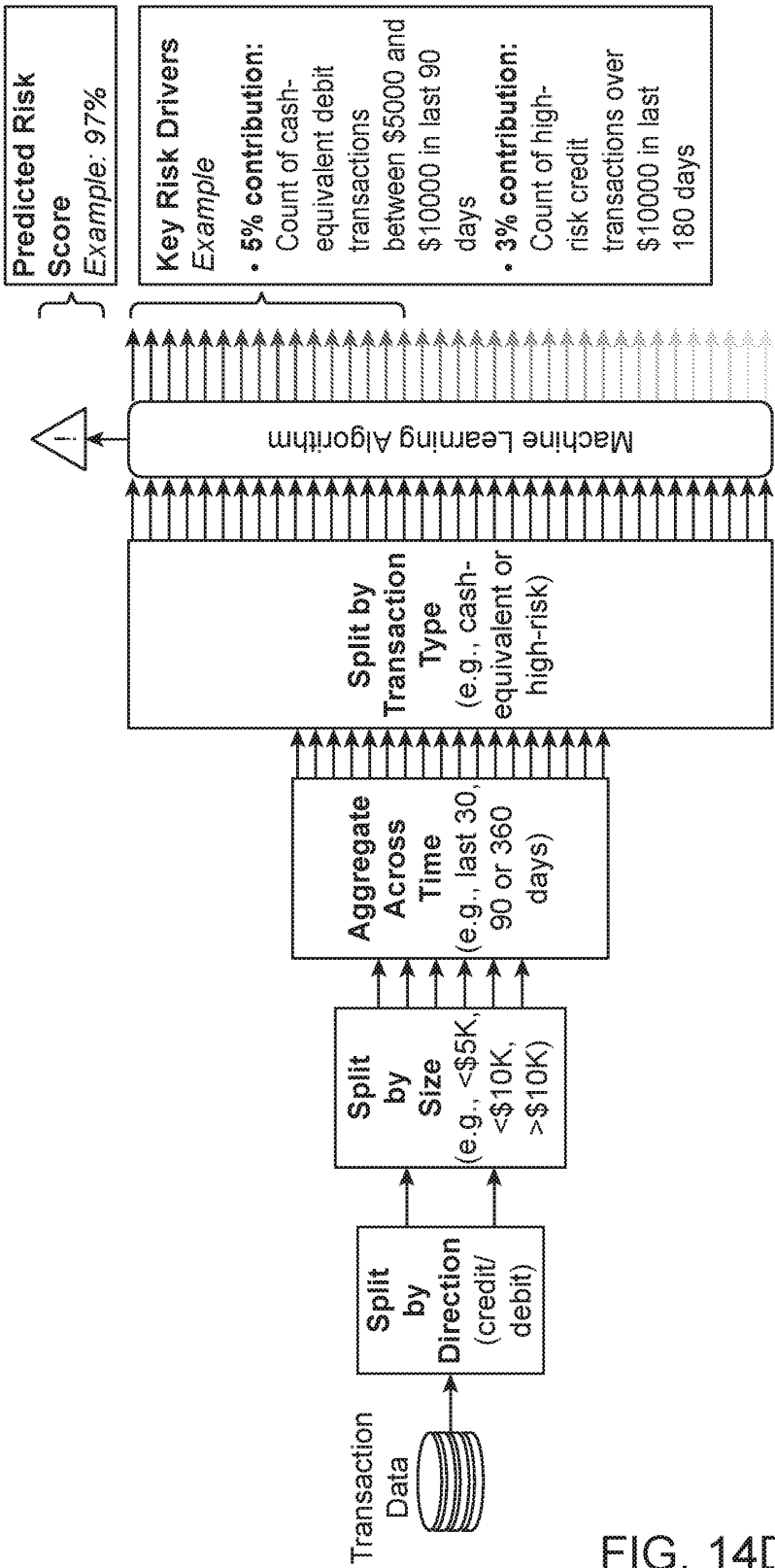


FIG. 14D

Feature Class	Description	Examples
Party Attributes	Attributes or characteristics of the client including both internal and externally available data	- Adverse media score for fraudulent activity - Party is domiciled in high-risk country - Party is Private Investment Company - Party is politically exposed person
Party Behaviors	Behavior of parties as demonstrated through transactions, wires, or other actions that leave a digital trace	- Ratio of deposits/withdrawals last 360 days - Value of ATM deposits >5K, <10K last 7 days - Activity in dormant account last 2 days - Count of transactions using currency from risky country
Anomalies	Abnormal transaction patterns relative to stated business; abnormal patterns relative to historical benchmark; abnormal patterns relative to stated income	- Cash-equivalent transactions relative to peers last 7 days - Burst in beneficiary activity last 2 days - High-risk transactions relative to historical last 30 days - High-risk country transactions relative to peers last 180 days
Associations	Proximity to known money launderers; similar transaction patterns to known money launderers; associations with high-risk businesses or countries	- Shortest graph path to known illicit organization - Sum value of wires where counterparty didn't disclose name - Number of 2nd degree connections with >1 shared nodes - Number of related parties
Segmentation	Segmentation based on country, transaction behavior, business sector, legal entity type, shared accounts, high-frequency relationships	- Behavior-based AI segmentation - Profile information, KYC based AI segmentation - Network and associations based segmentation % of segment that is known illicit organization

FIG. 14E

Feature Class	Description	Examples
Suspicious Information	Customer provides suspicious or incomplete information	- Client affiliated with consulate - Client is non-profit organization
Recordkeeping Avoidance	Customer behavior is designed to avoid reporting thresholds or requirements	- Redaction to party address info last 180 days - Count of transactions <10K last 7 days
Funds Transfers	Customer conducts suspicious transfers	- Cash/total ratio last 30 days - Suspicious payment instruction last 2 days
Inconsistent Behavior	Customer behavior relative to expected behavior	- Transaction value/income ratio last 360 days - Wire count relative to peers last 30 days
Cross-border Transactions	Customer has ties to or conducts transactions with high-risk geographies	- Number of unique countries last 180 days - Value with high-risk countries last 7 days
Shell Company Activity	Customer or account operates on behalf of unknown beneficiary	- Address is P.O. box - Number of parties at same address
Other	Other red flags including suspicious lending, insurance or other activity	- Loan scheduled balance net actual balance - Surrendered insurance contract last 30 days

FIG. 14F

Feature Class	Description	Examples
Placement	Introduction of illicit funds into formal financial services	◦ Count scheduled net count actual loan payment ◦ Client is non-profit organization
Layering	Movement of funds to obfuscate trail to funds' origin	◦ Redaction to party address info last 180 days ◦ Count of transactions <10K last 7 days
Integration	Transactions to create appearance of legality for sources of funds	◦ Client affiliated with cash-intense business ◦ Scheduled/actual loan payment discrepancies

FIG. 14G

Feature Class	Description	Examples
Transaction Monitoring	Suspicious activity or transaction monitoring systems	◦ Avg. party/counterparty distance last 30 days ◦ Value of transfers to risky country last 2 days
Know Your Customer	Know your customer or client due diligence systems	◦ Associated with terrorist org in social media ◦ Party is citizen of high-risk country
Watch List	Watch list filtering for politically exposed or other relevant persons	◦ Associated with terrorist org in social media ◦ Known politically exposed person

FIG. 14H

Potential Typology	Feature	Contribution	Value
	Count Of Foreign Accounts	0.332	2.0
High-risk Associations	Count Of Credits Of Related Party Transactions Between 5000 And 10000 In Last 180 Days	0.249	1.0
	Count Of Foreign Personal Investment Co Accounts	0.248	3.0
	Account Holder Has Global Risk Rating 2	0.206	1.0
Unusual Fund Transfer	Count Of High-Risk Debit Transactions Between 10000 And 100000 In Last 180 Days	0.192	23.0
Cross-Border Transactions	Sum Of Count Of All Transactions Message Contains Panama In Last 180 Days	0.188	1.0
	Sum Of All Transactions Originating From Country With Risk Rating 1 In Last 180 Days	-0.147	520,405
	Total Balance	0.142	1,204,532
Lack of Transparency	Account Holder Added Industry Code In Last 90 Days	0.118	0.0
Tax Evasion	Sum Of Value Of All Transactions Message Contains Tax In Last 180 Days	-0.108	0.0
Unusual Fund Transfer	Change In Avg Count Of Debit Transactions In Last 180 Days Compared To Previous 180 Days	-0.102	0.174
	Account Holder Is Operating Company	0.097	0.0
Activity Inconsistency	Sum Of Value Of All Transactions Message Contains Company In Last 180 Days	0.093	405,000
	Sum Of Count Of All Transactions Message Contains Chip In Last 2 Days	0.084	12,500
Unusual Fund Transfer	Count Of Debit Transactions Between 10000 And 100000 In Last 180 Days	-0.062	2.0
Unusual Fund Transfer	Stddev Count Of High-Risk Debit Transactions In Last 180 Days	0.051	0.083
Lack of Transparency	Sum Of Value Of All Transactions Message Contains Lic In Last 180 Days	0.011	0.0
Lack of Transparency	Count Of All Transactions With Counterparty In Different Financial Institution In Last 2 Days	-0.004	1.0

FIG. 14I

Example Potential Typologies
◦ Lack of Transparency ◦ Cross-Border Transactions ◦ Structuring ◦ Flow Through of Funds ◦ Unusual Fund Transfer ◦ High-risk Associations ◦ Activity Inconsistency ◦ Tax Evasion

Categories of Feature Contributions
◦ Account Holder Characteristics and Changes ◦ Balances ◦ Structuring Activity ◦ Flow Through of Funds ◦ Direct Geographic Risk and Associated Risk ◦ Natural Language Processing ◦ Transaction Activity Changes ◦ Related Party Characteristics

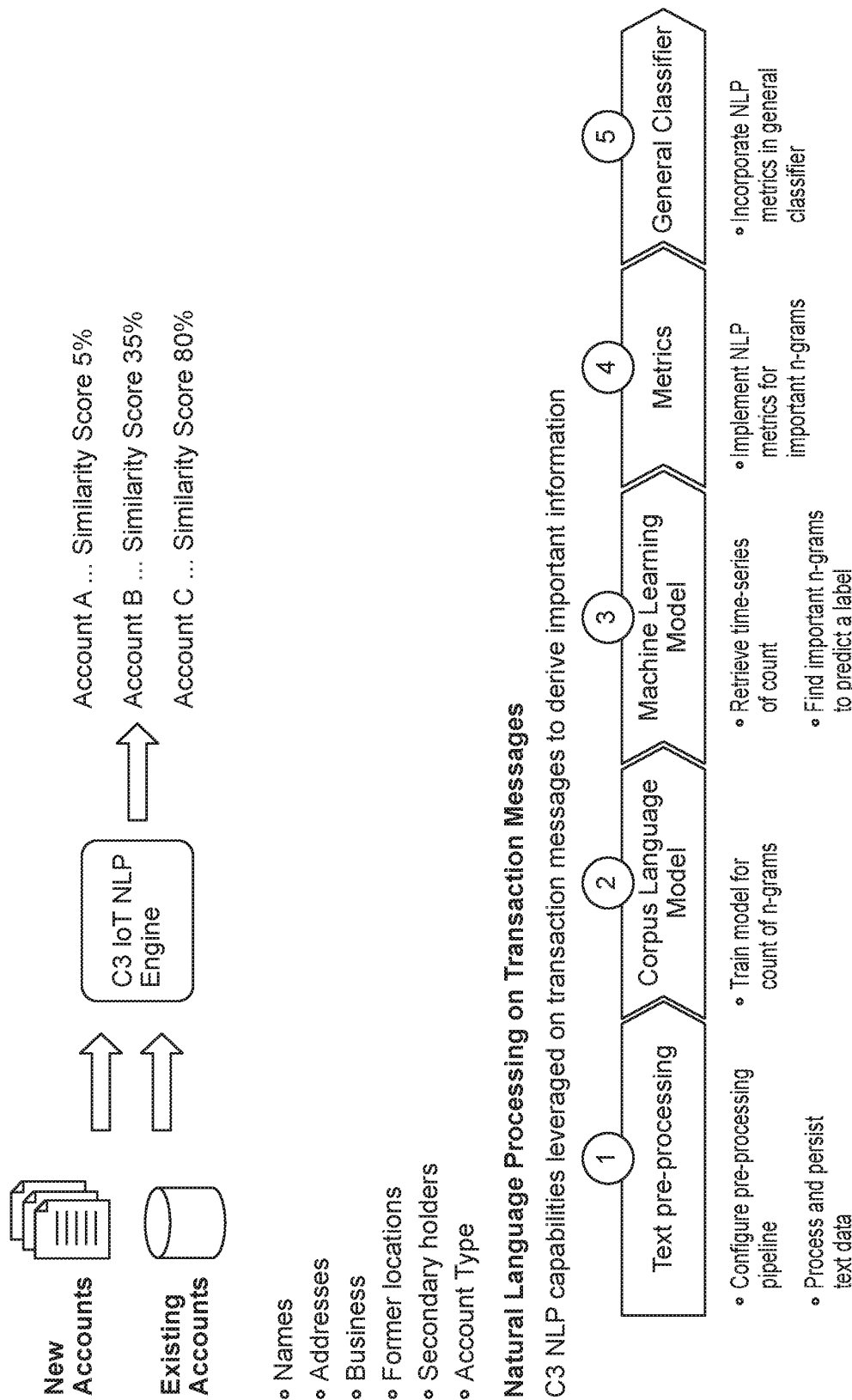


FIG. 15

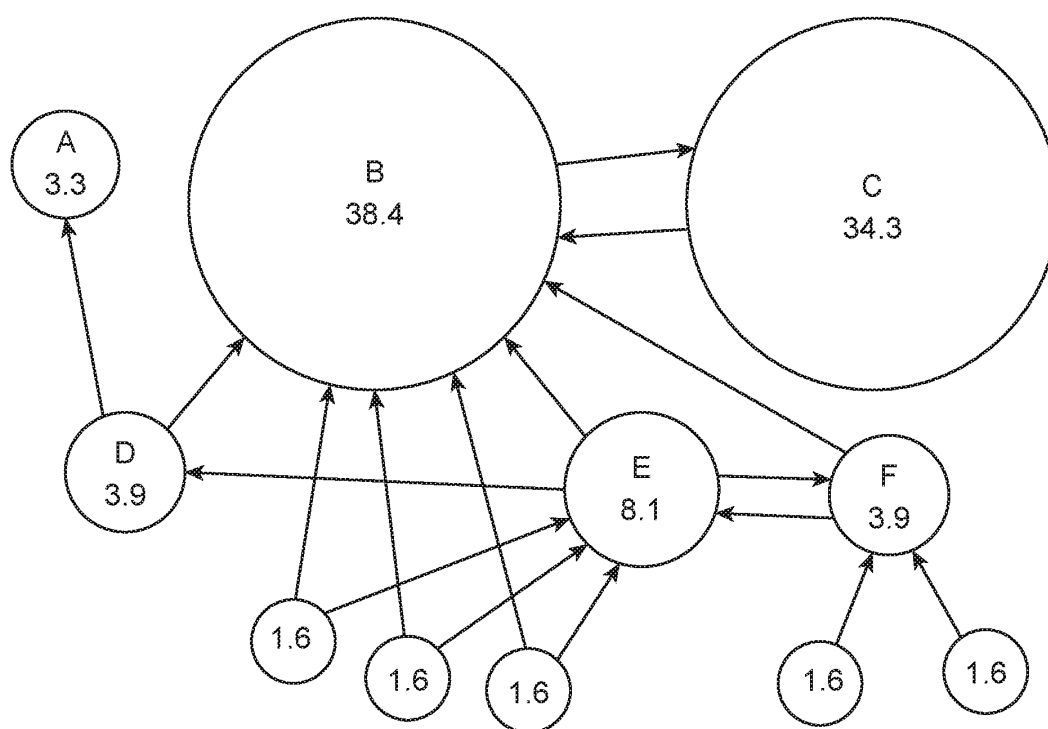


FIG. 16

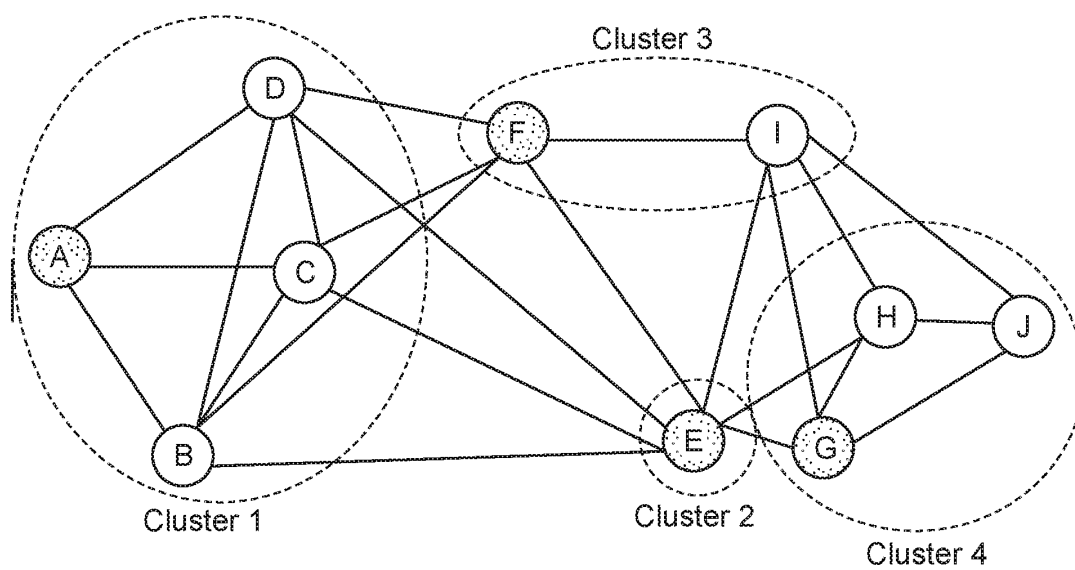


FIG. 17

C3 ANTI MONEY LAUNDERING ANALYTICS

ANALYTICS CLASS	DESCRIPTION	ANALYTICS
PLACEMENT	◦ Review large transactions for new or modified accounts ◦ Flag suspicious account holders or falsified identification	◦ New transaction ◦ Suspicious account change ◦ Suspicious identification ◦ Large transaction after account change
LAYERING	◦ Identify size and speed of transaction that may indicate layering	◦ Small transactions after large ◦ Consistent transactions in time
FOREIGN EXCHANGE	◦ Identify currency exchange with suspicious entities associated with high crime of terrorist activities ◦ Correlate transactions with moves in forex markets ◦ Identify suspicious transactions using SWIFT	◦ Known terrorist connections ◦ Transactions without forex discrimination ◦ Inconsistent currency exchange
STRUCTURING	◦ Identify structuring of transactions at multiple locations to avoid federal reporting limits ◦ Identify number of transactions below limits required to show identification	◦ Number of unique transaction locations ◦ Transactions below reporting limits ◦ Transactions below ID limits ◦ No account changes ◦ Unique tellers ◦ Transactions of similar size
SUSPICIOUS ACTORS	◦ Identify transactions with suspicious entities (terrorist regimes, criminal connections) ◦ Correlate depositors with criminal backgrounds ◦ Identify transactions inconsistent with stated occupations	◦ Terrorist backed entities ◦ Criminal connection ◦ High transactions ◦ Transactions inconsistent with occupation ◦ Degree of closeness with terrorist activity
TRANSACTION	◦ Review cash rations by transaction and aggregate ◦ Identify multiple deposits of similar size ◦ Track transactions spatially and temporally ◦ Flag various but consistent usage of non-conventional monetary instruments ◦ Align transaction speed with account changes ◦ Track transactions within retail, correspondent banking, securities and insurance across business ◦ Identify unusual withdrawals ◦ Align speed of withdrawals relative to deposits	◦ Cash ratio ◦ Deposit variance ◦ Graph of transactions in space and time ◦ Opt-out customer ◦ Cash ratio aligned with account change ◦ Unique monetary instruments ◦ Unusual withdrawal size ◦ Unique transaction locations ◦ Currency exchange ◦ Retail transactions ◦ Time between transactions ◦ Transaction above threshold ◦ Unique account members
ACCOUNT	◦ Identify suspicious accounts with many account holders at same address ◦ Identify connections with blacklisted or suspicious foreign entities ◦ Identify gaps or missing account data relative to population ◦ Reference account data with third party database like criminal or business organizations ◦ Verify account information with government AML sources like (MoLIN) ◦ Identify unusual use of business account ◦ Correlate types of businesses at risk for money laundering	◦ Number account holders at address ◦ Blacklist ◦ Unusual business ◦ Criminal ties ◦ Gaps in account data ◦ Missing account information ◦ Removed account information ◦ International account connections ◦ Suspicious foreign entity connection

FIG. 18

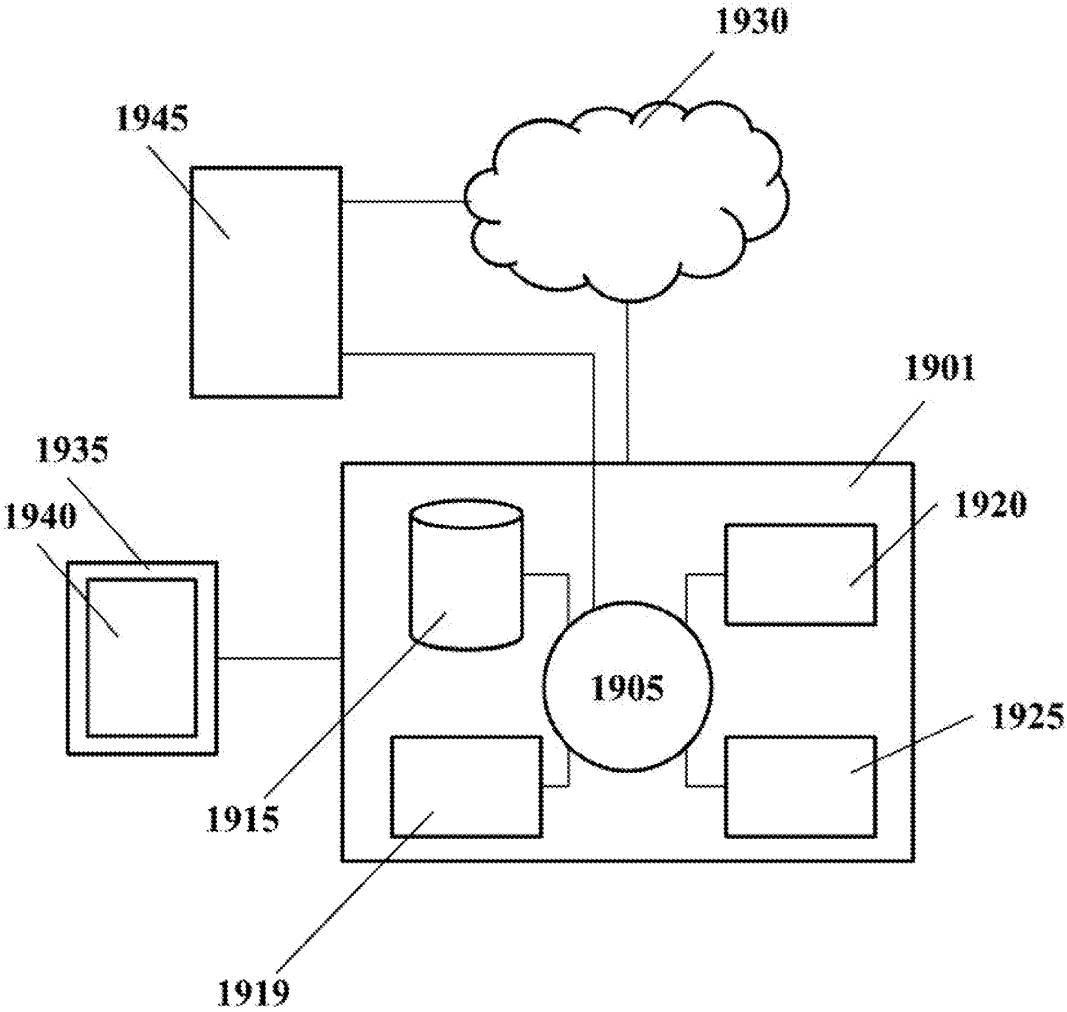


FIG. 19