

TITLE

GENERATIVE ADVERSARIAL NETWORK (GAN) BASED FRAUD DETECTION

TECHNICAL FIELD

[0001] At least some aspects of the present disclosure relate to detecting fraud related to payment transactions, and more particularly, to detecting fraud related to real transaction data based on synthesized transaction data generated using a generative adversarial network.

BACKGROUND

[0002] Various approaches for detecting fraud in payment transactions often rely on historical transaction data. For example, historical transaction data, including data corresponding to non-fraudulent and fraudulent transactions executed across a payment network, may be used to train a fraud detection model to identify features (e.g., patterns) in the historical transaction data indicative of fraudulent transactions. Further, fraud detection rules can be developed based on these features. As additional payment transactions are executed across the payment network, the trained model and/or the fraud detection rules can be applied to the additional transactions to identify potentially fraudulent transactions.

[0003] However, various issues can result from relying on historical transaction data for fraud detection. For example, new types of payment transactions are often developed (e.g., API-based payments, real time payments). Furthermore, malicious actors may create methods for executing new types of fraudulent transactions. Data related to the new types of payment transactions and the new types of fraudulent transactions may not be captured by the historical transaction data. Thus, fraud detection models and/or rules developed based on the historical transaction data may be ineffective at identifying new types of fraudulent transactions. Accordingly, new types of fraudulent transactions may go undetected until historical data related to these fraudulent transactions is collected and used to update the fraud detection model and/or fraud detection rules.

[0004] As another example, only a small fraction of the transactions represented by the historical transaction data may be fraudulent transactions. Thus, large amounts of historical data are often required in order to capture enough fraudulent transactions to train the fraud detection model. Furthermore, significant human intervention is often required to label and processes the historical data. Thus, it can take several months to prepare and implement a fraud detection model. This preparation effort can not only require costly human resources but can also cause the model to be outdated by the time it is implemented.

[0005] As yet another example, various regulations (e.g., General Data Protection Regulation (GDPR)) may prohibit the processing of personal data. Thus, some transaction

data (e.g., personal data) relevant to fraud detection may be excluded from the historical transaction data. Therefore, the historical transaction data may be incomplete and fraud detection models and/or rules developed based on the historical transaction data may be ineffective at identifying various types of fraudulent transactions.

[0006] Accordingly, there is a need for alternate devices, systems, and methods for fraud detection. The present disclosure provides various solutions that implement a generative adversarial network (GAN) for fraud detection.

SUMMARY

[0007] According to one aspect, the present disclosure provides a computer-implemented method. The method can include receiving, by a creator neural network, real transaction data and fraud detection rules. The real transaction data corresponds to real transactions executed across a payment network. The fraud detection rules are for identifying fraudulent transactions. The method can further include, generating, by the creator neural network, synthesized transaction data. The synthesized transaction data corresponds to synthesized transactions that are not actually executed across the payment network. The fraud detection rules can be updated based on the synthesized transaction data.

[0008] According to another aspect, the present disclosure provides a system. The system can include a creator model and an evaluator model. The creator model is to receive real transaction data corresponding to real transactions executed across a payment network, receive fraud detection rules for identifying fraudulent transactions, and generate synthesized transaction data based on the real transaction data and the fraud detection rules. The synthesized transaction data corresponds to synthesized transactions that are not actually executed across the payment network. The evaluator model is to receive the synthesized transaction data and classify at least some of the synthesized transactions as fraudulent transactions.

[0009] According to yet another aspect, the present disclosure provides a computer-implemented method. The computer-implemented method can include receiving, by a transaction service provider server, real transaction data and identifying, by the transaction service provider server, a first fraudulent transaction by applying fraud detection rules to the real transaction data. The method can further include denying, by the transaction service provider server, the first fraudulent transaction. The method can further include generating, by the transaction service provider server, synthesized transaction data based on the real transaction data and generating, by the transaction service provider server, updated fraud

detection rules based on the synthesized transaction data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] In the description, for purposes of explanation and not limitation, specific details are set forth, such as particular aspects, procedures, techniques, etc. to provide a thorough understanding of the present technology. However, it will be apparent to one skilled in the art that the present technology may be practiced in other aspects that depart from these specific details.

[0011] The accompanying drawings, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate aspects of concepts that include the claimed disclosure and explain various principles and advantages of those aspects.

[0012] The apparatuses and methods disclosed herein have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the various aspects of the present disclosure so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

[0013] FIG. 1 is a block diagram of a transaction synthesis system, according to at least one aspect of the present disclosure.

[0014] FIG. 2 is a block diagram of a fraud detection system, according to at least one aspect of the present disclosure.

[0015] FIG. 3 is a block diagram of a payment network system, according to at least one aspect of the present disclosure.

[0016] FIG. 4A is a flow diagram of a method for generating synthesized transaction data, according to at least one aspect of the present disclosure.

[0017] FIG. 4B is a flow diagram of a method for classifying synthesized transaction data, according to at least one aspect of the present disclosure.

[0018] FIG. 5 is a block diagram of a computer apparatus with data processing subsystems or components, according to at least one aspect of the present disclosure.

[0019] FIG. 6 is a diagrammatic representation of an example system that includes a host machine, according to at least one aspect of the present disclosure.

[0020] Corresponding reference characters indicate corresponding parts throughout the

several views. The exemplifications set out herein illustrate various aspects of the present disclosure, in one form, and such exemplifications are not to be construed as limiting the scope of the disclosure in any manner.

DESCRIPTION

[0021] Before explaining various forms of devices, systems, and methods for generative adversarial network (GAN) based fraud detection, it should be noted that the illustrative forms disclosed herein are not limited in application or use to the details of construction and arrangement of components illustrated in the accompanying drawings and description. The illustrative forms may be implemented or incorporated in other forms, variations, and modifications, and may be practiced or carried out in various ways. Further, unless otherwise indicated, the terms and expressions utilized herein have been chosen for the purpose of describing the illustrative forms for the convenience of the reader and are not for the purpose of limitation thereof. Also in the following description, it is to be understood that terms such as “forward,” “rearward,” “left,” “right,” “above,” “below,” “upwardly,” “downwardly,” and the like are words of convenience and are not to be construed as limiting terms.

[0022] As described above, various approaches for detecting fraud in payment transactions often rely on historical transaction data. For example, historical transaction data, including data corresponding to non-fraudulent and fraudulent transactions executed across a payment network, may be used to train a fraud detection model to identify features (e.g., patterns) in the historical transaction data indicative of fraudulent transactions. Furthermore, fraud detection rules can be developed based on these features.

[0023] However, various issues can result from relying on historical transaction data for fraud detection. For example, data related to new types of payment transactions and features indicative of new types of fraudulent transactions may not be captured by the historical transaction data. As another example, only a small fraction of the transactions represented by the historical transaction data may be fraudulent transactions. Thus, large amounts of historical data can be required in order to capture enough fraudulent transactions to train the fraud detection model. As yet another example, various regulations may prohibit the processing of personal data as part of the historical data. Thus, fraud detection models and/or rules developed based on the historical transaction data may be ineffective at identifying the fraudulent transactions. Accordingly, there is a need for alternate devices, systems, and methods for fraud detection.

[0024] The present disclosure provides various devices, systems, and methods that can implement a generative adversarial network (GAN) for fraud detection. For example, in one

aspect, a transaction synthesis system is disclosed. The transaction synthesis system can employ a GAN that includes a creator model (e.g., creator neural network) and an evaluator model (e.g., evaluator neural network). The creator model can receive real transaction data corresponding to real transactions executed across a payment network. Additionally or alternatively, the creator model can receive fraud detection rules for identifying fraudulent transactions. The creator model can generate synthesized transaction data based on the real transaction data and/or the fraud detection rules. The synthesized transaction data can correspond to synthesized transactions that are not actually executed across the payment network. The evaluator model can receive the synthesized transaction data and classify at least some of the synthesized transactions as fraudulent transactions.

[0025] In some aspects, the synthesized transaction data, including data corresponding to the synthesized transactions classified as fraudulent transactions, can be used to update the fraud detection rules. Furthermore, some of the synthesized transactions generated by the creator model can be predictive of future types of fraudulent transactions that have yet to be implemented by malicious actors. Thus, the updated fraud detection rules may be more effective at identifying new types of fraudulent transactions compared to fraud detection rules generated based on historic transaction data alone.

[0026] In some aspects, the creator model can receive the updated fraud detection rules and/or additional real transaction data and generate additional synthesized transaction data. Thus, the transaction synthesis system can employ an iterative feedback loop whereby rules that are updated based on transaction data synthesized by the creator model are then used by the creator model to generate additional synthesized transaction data, enabling further rule updates based on the additional synthesized transaction data. Thus, robust training and validation data can be generated and used to train the creator model and the evaluator model. Accordingly, the evaluator model may be more effective at identifying various types of fraudulent transactions compared to fraud detection models generated based on historic transaction data alone. Furthermore, the synthesized data can be generated to include a larger proportion of fraudulent transactions compared to the relatively small proportion of fraudulent transactions that is often included in historical data. Thus, the evaluator model can be trained to identify fraudulent transactions using a smaller overall data set compared to the large volumes of historical data that is often required for training traditional fraud detection models.

[0027] In some aspects, the creator model includes a large language model. The large language model can format the fraud detection rules such that they can be processed by the creator model to generate synthesized transaction data. Thus, various different types of rules, including, for example, operating regulations, stand in processing rules, and/or risk

rules, can be used to generate the synthesized transaction data with minimal and/or no human intervention.

[0028] In some aspects, an online implementation of the evaluator model can be used to detect fraudulent transactions in real time. As noted above, the feedback loop implemented by the transaction synthesis system can enable the creator model and the evaluator model to generate and use a robust training and validation data set. Furthermore, this training can enable the evaluator model to identify potentially new types of fraudulent transactions (e.g., via the synthesized transaction data) that have yet to be created and implemented by malicious actors. Thus, the evaluator model can be effective at identifying fraudulent transactions included in real transaction data. Accordingly, real transaction data can be sent (e.g., by a transaction processing service provider, by an issuer) to an online implementation of the evaluator model for identifying fraudulent transactions. Furthermore, transactions identified as fraudulent by the online implementation of the evaluator model can be denied (e.g., by the transaction processing service provider, by the issuer, in real time), thereby preventing fraud.

[0029] The devices, systems, and methods provided herein can provide numerous benefits. For example, by generating synthesized transaction data, including data corresponding to fraudulent synthesized transactions, the evaluator model can be trained to more effectively identify fraudulent transactions compared to a fraud detection model trained based on historical transaction data (e.g., large volumes of historical transaction data that include only a small portion of data corresponding to fraudulent transactions).

[0030] As another example, because of the GAN-based approach to generating the synthesized transaction data using real transaction data as well as iteratively updated fraud detection rules, at least some of the synthesized transaction data may have characteristics similar to future types of fraudulent transactions that have yet to be developed. Thus, the evaluator model, which can be trained based on the synthesized transaction data, and/or fraud detection rules, which can be updated based on the synthesized transaction data, can be effective at identifying new types of fraudulent transactions that are not present in the historical transaction data.

[0031] As yet another example, the synthesized transaction data may not include personal information of consumers. Thus, the devices, systems, and methods provided herein can avoid the processing of personal data when training the evaluator model and updating the fraud detection rules, thereby protecting consumer's security and privacy while also complying with various regulatory requirements related to processing personal data.

[0032] As yet another example, devices, systems, and methods can implement the

generation of synthesized transaction data and updated fraud detection rules into a practical application by using the updated fraud detection rules to identify and deny fraudulent transactions (e.g., in real time), thereby preventing fraud.

[0033] FIG. 1 is a block diagram of a transaction synthesis system 100, according to at least one aspect of the present disclosure. The transaction synthesis system 100 can include a creator model 102 and an evaluator model 108. In some aspects, the transaction synthesis system 100 is a generative adversarial network (GAN).

[0034] The creator model 102 can include a neural network. The creator model 102 (e.g., the neural network) can be trained to generate synthesized transaction data 128 from inputs including real transaction data 110, fraud detection rules 114, and/or fraud reporting data 124. The synthesized transaction data 128 generated by the creator model 102 can include data corresponding to transactions that are not actually executed across a payment network.

[0035] The real transaction data 110 can include data corresponding to transactions that have been executed across a payment network. For example, referring briefly to FIG. 3, and also to FIG. 1, the real transaction data 110 can include data corresponding to transactions initiated by a payment device 2006 and an access device 2004 and processed by one or more than one of a payment gateway system 2002, an issuer system 2008, a transaction service provider system 2010, and/or an acquirer system 2012. In some aspects, the real transaction data 110 may be data stored by payment gateway system 2002, an issuer system 2008, a transaction service provider system 2010, and/or an acquirer system 2012 and sent to the transaction synthesis system 100 (e.g., the creator model 102). In some aspects, the real transaction data 110 may be sent to the transaction synthesis system 100 (e.g., the creator model 102) in real time as transactions are being processed across the payment network system 2000.

[0036] Referring again to FIG. 1, in some aspects, the real transaction data 110 can include reference data 112. The reference data 112 can include various identity information related to the real transaction data 110. For example, the reference data 112 can include various fields and/or labels including issuer identifiers, acquirer identifiers, country codes, currency code, merchant codes, etc. corresponding to transactions represented by the real transaction data 110. The reference data 112 can be processed by the creator model 102 to generate the synthesized transaction data 128.

[0037] In some aspects, the transaction synthesis system 100 and/or the creator model 102 can be configured to pre-process the real transaction data 110. For example, the transaction synthesis system 100 can format or otherwise initialize the real transaction data

110 for streamlined processing by the creator model 102 (e.g., the neural network).

[0038] The fraud detection rules 114 can include various rules that may be used to identify potentially fraudulent transactions. For example, in some aspects, the fraud detection rules 114 may be applied to transaction data to identify a risk score for a transaction. If the risk score satisfies a predetermined threshold, then the transaction may be considered as potentially fraudulent. In some aspects, the fraud detection rules 114 may be employed by a fraud detection system (e.g., the fraud detection system 200 (FIG. 2)) to identify potentially fraudulent transactions.

[0039] The fraud detection rules 114 can include risk rules 116, operating regulations 118, stand in processing rules 120, and/or various other rules 122. The risk rules 116 may be rules implemented by a transaction service provider system (e.g., the transaction service provider system 2010 (FIG. 3)) to classify transactions as fraudulent or non-fraudulent. The operating regulations 118 may be rules that govern the interchange of transactions and transaction data across various entities of a payment network (e.g., interchange between the issuer system 2008 and the acquirer system 2012 of the payment network system 2000). The stand in processing rules 120 may be rules that are used for approving or denying transactions by one entity (e.g., a transaction service provider system 2010) on behalf of another entity (e.g., an issuer system 2008). The other rules 122 can include any types of rules implemented by entities operating within a payment network (e.g., payment network system 2000) to verify, authenticate, validate, or otherwise approve or deny transactions. The fraud detection rules 114 can be in any format, including, for example, text, tables, spreadsheets, lists, code, etc.

[0040] In some aspects, the creator model 102 can include a large language model. The large language model can be trained to read and format the fraud detection rules 114 for streamlined processing by the creator model 102 (e.g., the neural network). For example, as noted above the fraud detection rules 114 can be in any format, including, for example, text, tables, spreadsheets, lists, code, etc. The large language model can read any one of these various data formats and reformat the fraud detection rules 114 to be used as an input for generating synthesized transaction data 128 by the creator model 102.

[0041] In some aspects, the creator model 102 can include a randomizer 104 and/or an aggregator 106. The randomizer 104 and/or the aggregator 106 can reduce bias related to the synthesized transaction data 128 generated by the creator model 102. For example, the randomizer 104 can randomly select inputs from the real transaction data 110, the fraud detection rules 114, and/or the fraud reporting data 124 to be applied to the creator model 102 to ensure that various sources of data within the inputs are not over represented when

training the creator model 102. As another example, randomizer 104 can randomize initial weights of the creator model 102. As another example, the aggregator 106 can selectively combine cumulative inputs to be applied to the creator model 102 and/or combine intermediate layer nodes of the creator model 102 to ensure that various sources of data within the inputs are not over represented when training the creator model 102.

[0042] The fraud reporting data 124 can include transaction data for transactions that are confirmed to be fraudulent. For example, the fraud reporting data 124 can include data corresponding to transactions reported as fraudulent by an issuer (e.g., an issuer system 2008) to a transaction service provider (e.g., a transaction service provider system 2010).

[0043] The evaluator model 108 can receive the real transaction data 110 and/or the synthesized transaction data 128 generated by the creator model 102. The evaluator model 108 can include a neural network.

[0044] In some aspects, the evaluator model 108 can be trained to classify input data as either real transaction data 110 or synthesized transaction data 128. Furthermore, the creator model 102 can be trained to generate synthesized transaction data 128 that, when processed by the evaluator model 108, cause the evaluator model 108 to incorrectly classify the synthesized transaction data 128 as real transaction data 110 (e.g., the creator model 102 can be trained to try and fool the evaluator model 108 into thinking that it has received real transaction data 110). Thus, through adversarial training, the creator model 102 becomes better at generating realistic synthesized transaction data 128 and the evaluator model becomes better at differentiating synthesized transaction data 128 from real transaction data 110.

[0045] In some aspects, the evaluator model 108 can be trained to classify transaction data (e.g., real transaction data 110, synthesized transaction data 128) as corresponding to a fraudulent transaction or a non-fraudulent transaction. For example, some of the synthesized transaction data 128 may include data corresponding to synthesized transactions that have features indicative of fraudulent transactions. Further, the synthesized transaction data 128 may include data corresponding to synthesized transactions that have features indicative of non-fraudulent transactions. Accordingly, the evaluator model 108 can be trained to classify each of the synthesized transactions as either fraudulent or non-fraudulent. In one aspect, the evaluator model 108 classifies transactions as fraudulent or non-fraudulent by generating a risk score for each transaction. If a risk score satisfies (e.g., exceeds) a predetermined threshold, then the evaluator model 108 may classify the corresponding transaction as fraudulent. If a risk score does not satisfy (e.g., does not exceed) the predetermined threshold, then the evaluator model 108 may classify the

corresponding transaction as non-fraudulent. Any of the risk scores, classifications, and/or corresponding transaction data that can be processed and/or generated by the evaluator model 108 are represented by the output 130 of FIG. 1.

[0046] The output 130 of the evaluator model 108 can be used to update the fraud detection rules 114. In some aspects, a fraud detection system (e.g., the fraud detection system 200 (FIG. 2)) may receive the output 130 of the evaluator model 108 and generate updated fraud detection rules 114 based on the output 130. For example, as noted above, the output 130 can include synthesized transaction data 128 and classifications indicating that the synthesized transaction data corresponds to fraudulent synthesized transactions. The fraud detection rules 114 can be updated to identify fraudulent transactions that have features similar to those of the fraudulent synthesized transactions.

[0047] As noted above, the creator model 102 can generate synthesized transaction data 128 based on the fraud detection rules 114. Furthermore, as noted above, updated fraud detection rules 114 can be generated based on the output of the evaluator model 108. Thus, the creator model 102 can generate additional synthesized transaction data 128 based on the updated fraud detection rules 114. The transaction synthesis system 100 can therefore employ an iterative process of generating synthesized transaction data 128, updating the fraud detection rules 114 based on synthesized transaction data 128, and applying the updated fraud detection rules 114 to the creator model 102 to generate additional synthesized transaction data 128. This iterative process can be implemented to improve the fraud detection rules 114, the creator model 102 (e.g., the quality of the synthesized transaction data 128 generated by the creator model 102), and the evaluator model 108 (e.g., the quality of the output 130 of the evaluator model 108).

[0048] As noted above, the evaluator model 108 can be trained to classify transaction data (e.g., real transaction data 110, synthesized transaction data 128) as corresponding to a fraudulent transaction or a non-fraudulent transaction. In some aspects, an online implementation of the evaluator model 108 (e.g., evaluator model 208 (FIG. 2)) can be deployed to analyze transaction data for transactions as they are being processed across a payment network (e.g., in real time). Further, based on analyzing the transaction data, the online implementation of the evaluator model 108 can identify fraudulent transactions as they are being processed, enabling various entities of the payment network (e.g., the issuer system 2008, the transaction service provider system 2010, the payment gateway system 2002, the acquirer system 2012) to deny the transactions and/or take another action (e.g., verification) to prevent the potential fraud.

[0049] FIG. 2 is a block diagram of a fraud detection system 200, according to at least

one aspect of the present disclosure. The fraud detection system 200 can receive real transaction data 210 and generate an output 230 based on the real transaction data 210. For example, the real transaction data 210 can correspond to transactions executed across a payment network (e.g., the payment network system 2000). The fraud detection system 200 can receive the real transaction data 210 and generate the output 230 as the corresponding transactions are being processed by the payment network (e.g., in real time).

[0050] The output 230 can comprise a fraud classification and/or a risk score for each transaction represented by the real transaction data 210. For example, the fraud classification can identify the transaction as fraudulent or non-fraudulent. As another example, the risk score can be a numeric probability (e.g. between 0.0 and 1.0) that the transaction is fraudulent. As yet another example, the fraud classification can be based on the risk score, wherein a risk score exceeding a predetermined threshold corresponds to a fraudulent classification for the transaction.

[0051] Various entities of a payment network (e.g., the issuer system 2008, the transaction service provider system 2010, the payment gateway system 2002, the acquirer system 2012) can take action based on the output 230 of the fraud detection system 200. For example, based on the output 230 identifying a transaction as fraudulent and/or including a risk score that exceeds a predetermined threshold, one or more than one entity of a payment network may deny the transaction and/or take another action (e.g., verification) to prevent the potential fraud.

[0052] The fraud detection system 200 can include fraud detection rules 214. The fraud detection rules 214 can be applied to the real transaction data 210 to generate the output 230. The fraud detection rules 214 can be similar to the fraud detection rules 114 (FIG. 1). Thus, any aspects of the fraud detection rules 114 described herein can similarly apply to the fraud detection rules 214. For example, the fraud detection rules 214 can be updated based on the output 130 of the evaluator model 108. As another example, the fraud detection rules 214 can be received by the creator model 102 and processed by the creator model 102 to generate synthesized transaction data 128.

[0053] The fraud detection system 200 can include an evaluator model 208. The evaluator model 208 can be an online implementation of the evaluator model 108 (FIG. 1). The real transaction data 210 can be applied to the evaluator model 208 to generate the output 230. Any of the aspects described herein with respect to the evaluator model 108 can similarly apply to the evaluator model 208.

[0054] In some aspects, the fraud detection system 200 employs both the fraud detection rules 214 and the evaluator model 208 to generate the output 230. In some

aspects, the fraud detection system 200 can include the fraud detection rules 214 without the evaluator model 208. In some aspects, the fraud detection system 200 can include the evaluator model 208 without the fraud detection rules 214.

[0055] FIG. 3 is a diagram of a payment network system 2000 across which transactions may be executed, according to at least one aspect of the present disclosure. As shown in FIG. 3, the payment network system 2000 can include a payment gateway system 2002, an access device 2004, a payment device 2006, an issuer system 2008, a transaction service provider system 2010, an acquirer system 2012, a network 2014, a fraud detection system 2200, and a transaction synthesis system 2100. The payment gateway system 2002, the access device 2004, the payment device 2006, the issuer system 2008, the transaction service provider system 2010, the acquirer system 2012, the fraud detection system 2200, and/or the transaction synthesis system 2100 may interconnect (e.g., establish a connection to communicate) via wired connections, wireless connections, or a combination of wired and wireless connections.

[0056] A “payment network” may refer to an electronic payment system used to accept, transmit, or process transactions made by payment devices for money, goods, or services. The payment network may transfer information and funds among issuers, acquirers, merchants, and payment device users. One illustrative non-limiting example of a payment network is VisaNet, which is operated by Visa, Inc.

[0057] A “system” may refer to one or more computing devices or combinations of computing devices (e.g., processors, servers, client devices, software applications, components of such, and/or the like).

[0058] Referring again to FIG. 3, the access device 2004 may include one or more devices capable of receiving information from and/or transmitting information to the payment gateway system 2002, the payment device 2006, the issuer system 2008, the transaction service provider system 2010, the acquirer system 2012, the fraud detection system 2200, and/or the transaction synthesis system 2100 via the network 2014. The access device 2004 may be any suitable device that provides access to a remote system. The access device 2004 also may be used for communicating with a merchant computer, a transaction-processing computer, an authentication computer, or any other suitable system. The access device 2004 may generally be located in any suitable location, such as at the location of a merchant. The access device 2004 may be in any suitable form. Some examples of the access device 2004 can include POS or point-of-sale devices (e.g., POS terminals), cellular phones, personal digital assistants (PDAs), personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller

machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like. The access device 2004 may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, the payment device 2006. For example, the access device 2004 may include a reader, a processor, and a computer-readable medium. A reader can include a radio frequency (RF) antenna, an optical scanner, a bar code reader, and/or a magnetic stripe readers to interact with the payment device 2006.

[0059] As noted above, in some aspects, the access device 2004 can comprise a point-of-sale (POS) device. The POS device may include one or more than one device, such as a computer, a computer system, a portable electronic device, and/or a peripheral device capable of being used by a merchant to conduct a payment transaction with a user, for example, using the payment device 2006. In some aspects, the POS device may be a component of a merchant system associated with a merchant. In some aspects, the POS device can be configured to receive information from the payment device 2006 via a communication connection (e.g., a near field communication (NFC) connection, a radio-frequency identification (RFID) communication connection, a Bluetooth® communication connection, and/or the like) and/or transmit information to the payment device 2006 via the communication connection.

[0060] A “merchant” may refer to one or more individuals or entities (e.g., operators of retail businesses that provide goods and/or services, and/or access to goods and/or services, to a user (e.g., a customer, a consumer, a customer of the merchant, and/or the like) based on a transaction (e.g., a payment transaction)). As used herein “merchant system” may refer to one or more computer systems operated by or on behalf of a merchant, such as a server computer executing one or more software applications.

[0061] A “user” may include an individual. In some embodiments or aspects, a user may be associated with one or more personal accounts, payment cards, and/or portable electronic devices. The user also may be referred to as a cardholder, account holder, or consumer.

[0062] Referring again to FIG. 3, the payment device 2006 can include any device that may be used to conduct a transaction, such as a financial transaction. For example, a payment device 2006 may be used to provide payment information to a merchant. In some aspects, the payment device 2006 can be a portable computing device. In some aspects, the payment device 2006 can be a payment card and can include a substrate such as a paper, metal, or plastic card, and information that is printed, embossed, encoded, and/or otherwise included at or near a surface of the payment card. The payment device 2006 can be hand-

held and compact so that it can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). The payment device 2006 can be a smart card, a debit device (e.g., a debit card), a credit device (e.g., a credit card), a stored value device (e.g., a stored value card or "prepaid" card), and/or a magnetic stripe or chip card. The payment device 2006 may operate in a contact and/or contactless mode. For example, the payment device 2006 may be an electronic payment device, such as a smart card, a chip card, an integrated circuit card, and/or a near field communications (NFC) card, among others. The payment device 2006 device may include an embedded integrated circuit. The embedded integrated circuit may include a data storage medium (e.g., volatile and/or non-volatile memory) to store information associated with the payment device 2006, such as an account identifier and/or a name of an account holder. The payment device 2006 may interface with the access device 2004 to initiate a transaction.

[0063] Referring still to FIG. 3, the payment gateway system 2002 may include one or more devices capable of receiving information from and/or transmitting information to the access device 2004, the issuer system 2008, the transaction service provider system 2010, the acquirer system 2012, the fraud detection system 2200, and/or the transaction synthesis system 2100 via the network 2014. For example, the payment gateway system 2002 may include a computing device, such as a server (e.g., a transaction processing server), a group of servers, and/or other like devices. The payment gateway system 2002 may refer to an entity and/or a payment processing system operated by or on behalf of such an entity (e.g., a merchant service provider, a payment service provider (PSP), a payment facilitator, a payment facilitator that contracts with an acquirer, a payment aggregator, and/or the like), which provides payment services (e.g., transaction service provider payment services, payment processing services, and/or the like) to one or more merchants.

[0064] Referring still to FIG. 3, the acquirer system 2012 may include one or more devices capable of receiving information from and/or transmitting information to the payment gateway system 2002, the access device 2004, the issuer system 2008, the transaction service provider system 2010 the fraud detection system 2200, and/or the transaction synthesis system 2100 via the network 2014. For example, the acquirer system 2012 may include a computing device, such as a server, a group of servers, and/or other like devices. In some aspects, acquirer system 2012 may be associated with an acquirer. In some aspects, the acquirer system 2012 may be associated with a merchant account of a merchant associated with the access device 2004.

[0065] An "acquirer" may refer to an entity licensed by a transaction service provider and/or approved by a transaction service provider to originate transactions (e.g., payment transactions) using a portable financial device associated with the transaction service

provider. “Acquirer” or “acquirer system” may also refer to one or more computer systems operated by or on behalf of an acquirer, such as a server computer executing one or more software applications (e.g., “acquirer server”). An “acquirer” may be a merchant bank, or in some cases, the merchant system may be the acquirer. The transactions may include original credit transactions (OCTs) and account funding transactions (AFTs). The acquirer may be authorized by the transaction service provider to sign merchants of service providers to originate transactions using a portable financial device of the transaction service provider. The acquirer may contract with payment facilitators to enable the facilitators to sponsor merchants. The acquirer may monitor compliance of the payment facilitators in accordance with regulations of the transaction service provider.

[0066] Referring again to FIG. 3, the transaction service provider system 2010 may include one or more devices capable of receiving information from and/or transmitting information to the payment gateway system 2002, the access device 2004, the issuer system 2008, the acquirer system 2012, the fraud detection system 2200, and/or the transaction synthesis system 2100 via the network 2014. For example, the transaction service provider system 2010 may include a computing device, such as a server (e.g., a transaction processing server), a group of servers, and/or other like devices. In some aspects, the transaction service provider system 2010 may be associated with a transaction service provider. In some aspects, transaction service provider system 2010 may be in communication with a data storage device, which may be local or remote to the transaction service provider system 2010. In some aspects, the transaction service provider system 2010 may be capable of receiving information from, storing information in, transmitting information to, or searching information (e.g., transaction data) stored in a data storage device.

[0067] A “transaction service provider” may refer to an entity that receives transaction authorization requests from merchants or other entities and provides guarantees of payment, in some cases through an agreement between the transaction service provider and an issuer. For example, a transaction service provider may include a payment network, such as Visa®, MasterCard®, American Express®, or any other entity that processes transactions. As used herein, “transaction service provider system” may refer to one or more systems operated by or operated on behalf of a transaction service provider, such as a transaction service provider system executing one or more software applications associated with the transaction service provider. In some non-limiting aspects, a transaction service provider system may include one or more server computers with one or more processors and, in some non-limiting aspects, may be operated by or on behalf of a transaction service provider.

[0068] Referring again to FIG. 3, the issuer system 2008 may include one or more devices capable of receiving information from and/or transmitting information to payment gateway system 2002, the access device 2004, transaction service provider system 2010, the acquirer system 2012, the fraud detection system 2200, and/or the transaction synthesis system 2100 via the network 2014. For example, issuer system 2008 may include a computing device, such as a server, a group of servers, and/or other like devices. In various aspects, the issuer system 2008 may be associated with an issuer institution. For example, the issuer system 2008 may be associated with an issuer institution that issued a credit account, debit account, credit card account, debit card account, and/or the like to a user associated with the payment device 2006.

[0069] The terms “issuer institution,” “portable financial device issuer,” “issuer,” or “issuer bank” may refer to one or more entities that provide one or more accounts (e.g., a credit account, a debit account, a credit card account, a debit card account, and/or the like) to a user (e.g., customer, consumer, and/or the like) for conducting transactions (e.g., payment transactions), such as initiating credit and/or debit payments. For example, an issuer may provide an account identifier, such as a personal account number (PAN), to a user that uniquely identifies one or more accounts associated with the user. The account identifier may be used by the user to conduct a payment transaction. The account identifier may be embodied on a portable financial device, such as a physical financial instrument, e.g., a payment card, and/or may be electronic and used for electronic payments. As used herein “issuer system” or “issuer institution system” may refer to one or more systems operated by or operated on behalf of an issuer. For example, an issuer system may refer to a server executing one or more software applications associated with the issuer. In some non-limiting aspects of the present disclosure, an issuer system may include one or more servers (e.g., one or more authorization servers) for authorizing a payment transaction. An “issuer” can include a payment account issuer. The payment account (which may be associated with one or more payment devices) may refer to any suitable payment account (e.g., credit card account, a checking account, a savings account, a merchant account assigned to a consumer, or a prepaid account), an employment account, an identification account, an enrollment account (e.g., a student account), etc.

[0070] Referring again to FIG. 3, the transaction synthesis system 2100 may include one or more devices capable of receiving information from and/or transmitting information to payment gateway system 2002, the access device 2004, the transaction service provider system 2010, the acquirer system 2012, and/or the fraud detection system 2200 via the network 2014. In some aspects, the transaction synthesis system 2100 may be included in any one or more of the fraud detection system 2200, the issuer system 2008, the transaction

service provider system 2010, and/or the acquirer system 2012. The transaction synthesis system 2100 can receive data corresponding to transactions executed across the payment network system 2000 and/or fraud detection rules (e.g., from the fraud detection system 2200), generate synthesized transaction data, and/or classify real and/or synthesized transaction data as fraudulent or non-fraudulent. Fraud detection rules and/or fraud detection models implemented by the fraud detection system 2200 may be updated based on synthesized transaction data generated by the transaction synthesis system 2100. In some aspects, the transaction synthesis system 2100 is similar to the transaction synthesis system 100 (FIG. 1). Any aspects described herein with respect to the transaction synthesis system 100 can similarly apply to the transaction synthesis system 2100 and vice versa.

[0071] Referring still to FIG. 3, the fraud detection system 2200 may include one or more devices capable of receiving information from and/or transmitting information to payment gateway system 2002, the access device 2004, the transaction service provider system 2010, the acquirer system 2012, and/or the transaction synthesis system 2100 via the network 2014. In some aspects, the fraud detection system 2200 may be included in any one or more of the transaction synthesis system 2100, the issuer system 2008, the transaction service provider system 2010, and/or the acquirer system 2012. The fraud detection system 2200 can receive and analyze data corresponding to transactions executed across the payment network system 2000 to identify potentially fraudulent transactions. The issuer system 2008, the transaction service provider system 2010, and/or the acquirer system 2012 may implement an action (e.g., deny, require further verification) for transactions identified as potentially fraudulent transactions by the fraud detection system 2200. In some aspects, the fraud detection system 2200 is similar to the fraud detection system 200 (FIG. 2). Any aspects described herein with respect to the fraud detection system 200 can similarly apply to the fraud detection system 2200 and vice versa.

[0072] Referring still to FIG. 3, the network 2014 may include one or more wired and/or wireless networks. For example, the network 2014 may include a cellular network (e.g., a long-term evolution (LTE) network, a fourth generation (4G) network, a fifth generation (5G) network, a code division multiple access (CDMA) network, etc.), a public land mobile network (PLMN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), a telephone network (e.g., the public switched telephone network (PSTN)), a private network, an ad hoc network, an intranet, the Internet, a fiber optic-based network, a cloud computing network, and/or the like, and/or a combination of these or other types of networks.

[0073] The number and arrangement of devices, systems, and networks shown in the

payment network system 2000 of FIG. 3 are provided as an example. There may be additional devices, systems, and/or networks; fewer devices, systems, and/or networks, different devices, systems, and/or networks, or differently arranged devices, systems, and/or networks than those shown in FIG. 3. Furthermore, two or more systems shown in FIG. 3 may be implemented within a single system and/or device, or a single system shown in FIG. 3 may be implemented as multiple, distributed devices and/or systems. Additionally or alternatively, a set of devices (*e.g.*, one or more devices) of the payment network system 2000 may perform one or more functions described as being performed by another set of devices of the payment network system 2000.

[0074] FIG. 4A is a flow diagram of a method 400a for generating synthesized transaction data, according to at least one aspect of the present disclosure. In some aspects, the method 400a can be performed by a creator model, such as the creator model 102 of the transaction synthesis system 100 (FIG. 1) and/or a creator model of the transaction synthesis system 2100 (FIG. 3).

[0075] Referring primarily to FIG. 4A, together with FIGS. 1 and 3, according to the method 400a, the creator model 102 receives 402 real transaction data 110 and fraud detection rules 114. The real transaction data 110 can correspond to real transactions executed across the payment network system 2000. The fraud detection rules 114 can be for identifying fraudulent transactions.

[0076] Referring still primarily to FIG. 4A, together with FIGS. 1 and 3, according to the method 400a, the creator model 102 generates 404 synthesized transaction data 128. The synthesized transaction data 128 can correspond to synthesized transactions that are not actually executed across the payment network system 2000. The fraud detection rules 114 can be updated based on the synthesized transaction data 128.

[0077] FIG. 4B is a flow diagram of a method 400b for classifying synthesized transaction data, according to at least one aspect of the present disclosure. In some aspects, the method 400b can be performed by an evaluator model, such as the evaluator model 108 of the transaction synthesis system 100 (FIG. 1) and/or an evaluator model of the transaction synthesis system 2100 (FIG. 3). In some aspects, the method 400b can be implemented in conjunction with the method 400a (FIG. 4A).

[0078] Referring primarily to FIG. 4B, together with FIGS. 1, 3, and 4A, according to the method 400b, the evaluator model 108 receives 406 synthesized transaction data 128. The synthesized transaction data 128 can correspond to synthesized transactions that are not actually executed across the payment network system 2000. The synthesized transaction data 128 may be generated 404 by the creator model 102.

[0079] Referring primarily to FIG. 4B, together with FIGS. 1, 3, and 4A, according to the method 400b, the evaluator model 108 generates 408 risk scores for the synthesized transactions. Further, the evaluator model 108 classifies 410 at least some of the synthesized transactions as fraudulent transactions based on the corresponding risk scores satisfying a predetermined threshold.

[0080] As noted above, the method 400a and the method 400b may be implemented in conjunction with one another. Referring to FIGS. 1, 3, 4A, and 4B, according to some aspects of the method 400a and 400b, the evaluator model 108 receives real transaction data 110 and synthesized transaction data 128. Further, the evaluator model 108 classifies each transaction represented by the real transaction data and the synthesized transaction data as a real transaction or a synthesized transaction.

[0081] According to some aspects, the method 400a and/or the method 400b further comprise training the creator model 102 to cause the evaluator neural model 108 to incorrectly classify synthesized transactions as real transactions.

[0082] Various aspects of the method 400a and/or the method 400b may be performed by a fraud detection system, such as the fraud detection system 200 (FIG. 2) and/or the fraud detection system 2200 (FIG. 3). Referring to FIGS. 2, 3, 4A, and 4B, according to some aspects of the method 400a and 400b, the fraud detection system 200 receives additional real transaction data 210 in real time. The fraud detection system 200 can identify a first real transaction represented by the additional real transaction data 210 as a fraudulent transaction based on the updated fraud detection rules 114, 214. Further, the fraud detection system 200 (and/or another entity of the payment network system 2000) can deny the first real transaction based on identifying the first real transaction as fraudulent.

[0083] According to some aspects of the method 400a and 400b, the fraud detection system 200 receives additional real transaction data 210 in real time. The fraud detection system 200 can include an online implementation of the evaluator model 208. The online implementation of the evaluator model 208 can classify a first real transaction represented by the additional real transaction data 210 as a fraudulent transaction based on the updated fraud detection rules 114, 214. Further, the fraud detection system 200 (and/or another entity of the payment network system 2000) can deny the first real transaction based on identifying the first real transaction as fraudulent.

[0084] According to some aspects of the method 400a and 400b, the real transaction data 110 comprises data corresponding to a transaction confirmed to be fraudulent (e.g., fraud reporting data 124).

[0085] FIG. 5 is a block diagram of a computer apparatus 3000 comprising data

processing subsystems or components, according to at least one aspect of the present disclosure. The subsystems shown in FIG. 5 are interconnected via a system bus 3010. Additional subsystems such as a printer 3018, keyboard 3026, fixed disk 3028 (or other memory comprising computer readable media), monitor 3022, which is coupled to a display adapter 3020, and others are shown. Peripherals and input/output (I/O) devices, which couple to an I/O controller 3012 (which can be a processor or other suitable controller), can be connected to the computer system by any number of means known in the art, such as a serial port 3024. For example, the serial port 3024 or external interface 3030 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus 3010 allows the central processor 3016 to communicate with each subsystem and to control the execution of instructions from system memory 3014 or the fixed disk 3028, as well as the exchange of information between subsystems. The system memory 3014 and/or the fixed disk 3028 may embody a computer readable medium.

[0086] FIG. 6 is a diagrammatic representation of an example computing system 4000 that includes a host machine 4002 within which a set of instructions to perform various aspects of any one or more of the methodologies discussed herein may be executed, such as, for example, the method 400a of FIG. 4A and/or the method 400b of FIG. 4B, according to at least one aspect of the present disclosure. In various aspects, the host machine 4002 operates as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the host machine 4002 may operate in the capacity of a server or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The host machine 4002 may be a computer or computing device, a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a cellular telephone, a portable music player (e.g., a portable hard drive audio device such as an Moving Picture Experts Group Audio Layer 3 (MP3) player), a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

[0087] The example computing system 4000 includes the host machine 4002, running a host operating system (OS) 4004 on a processor or multiple processor(s)/processor core(s) 4006 (e.g., a central processing unit (CPU), a graphics processing unit (GPU), or both), and various memory nodes 4008. The host OS 4004 may include a hypervisor 4010 which is able to control the functions of and/or communicate with a virtual machine ("VM") 4012

running on machine readable media. The VM 4012 also may include a virtual CPU or vCPU 4014. The memory nodes 4008 may be linked or pinned to virtual memory nodes or vNodes 4016. When the memory node 4008 is linked or pinned to a corresponding vNode 4016, then data may be mapped directly from the memory nodes 4008 to the corresponding vNode 4016.

[0088] All the various components shown in host machine 4002 may be connected with and to each other, or communicate to each other via a bus (not shown) or via other coupling or communication channels or mechanisms. The host machine 4002 may further include a video display, audio device or other peripherals 4018 (e.g., a liquid crystal display [LCD], alpha-numeric input device(s) including, e.g., a keyboard, a cursor control device, e.g., a mouse, a voice recognition or biometric verification unit, an external drive, a signal generation device, e.g., a speaker,) a persistent storage device 4020 (also referred to as disk drive unit), and a network interface device 4022. The host machine 4002 may further include a data encryption module (not shown) to encrypt data. The components provided in the host machine 4002 are those typically found in computer systems that may be suitable for use with aspects of the present disclosure and are intended to represent a broad category of such computer components that are known in the art. Thus, the example computing system 4000 can be a server, minicomputer, mainframe computer, or any other computer system. The computer may also include different bus configurations, networked platforms, multi-processor platforms, and the like. Various operating systems may be used including UNIX, LINUX, WINDOWS, QNX ANDROID, IOS, CHROME, TIZEN, and other suitable operating systems.

[0089] The disk drive unit 4024 also may be a Solid-state Drive (SSD), a hard disk drive (HDD) or other includes a computer or machine-readable medium on which is stored one or more sets of instructions and data structures (e.g., data/instructions 4026) embodying or utilizing any one or more of the methodologies or functions described herein. The data/instructions 4026 also may reside, completely or at least partially, within the main memory node 4008 and/or within the processor(s) 4006 during execution thereof by the host machine 4002. The data/instructions 4026 further may be transmitted or received over a network 4028 via the network interface device 4022 utilizing any one of several well-known transfer protocols (e.g., Hyper Text Transfer Protocol (HTTP)).

[0090] The processor(s) 4006 and memory nodes 4008 also may comprise machine-readable media. The term "computer-readable medium" or "machine-readable medium" should be taken to include a single medium or multiple medium (e.g., a centralized or distributed database and/or associated caches and servers) that store the one or more sets of instructions. The term "computer-readable medium" shall also be taken to include any

medium that is capable of storing, encoding, or carrying a set of instructions for execution by the host machine 4002 and that causes the host machine 4002 to perform any one or more of the methodologies of the present application, or that is capable of storing, encoding, or carrying data structures utilized by or associated with such a set of instructions. The term "computer-readable medium" shall accordingly be taken to include, but not be limited to, solid-state memories, optical and magnetic media, and carrier wave signals. Such media may also include, without limitation, hard disks, floppy disks, flash memory cards, digital video disks, random access memory (RAM), read-only memory (ROM), and the like. The example aspects described herein may be implemented in an operating environment comprising software installed on a computer, in hardware, or in a combination of software and hardware.

[0091] One skilled in the art will recognize that Internet service may be configured to provide Internet access to one or more computing devices that are coupled to the Internet service, and that the computing devices may include one or more processors, buses, memory devices, display devices, input/output devices, and the like. Furthermore, those skilled in the art may appreciate that the Internet service may be coupled to one or more databases, repositories, servers, and the like, which may be utilized to implement any of the various aspects of the disclosure as described herein.

[0092] The computer program instructions also may be loaded onto a computer, a server, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions that execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0093] Suitable networks may include or interface with any one or more of, for instance, a local intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide Area Network), a MAN (Metropolitan Area Network), a virtual private network (VPN), a storage area network (SAN), a frame relay connection, an Advanced Intelligent Network (AIN) connection, a synchronous optical network (SONET) connection, a digital T1, T3, E1 or E3 line, Digital Data Service (DDS) connection, DSL (Digital Subscriber Line) connection, an Ethernet connection, an ISDN (Integrated Services Digital Network) line, a dial-up port such as a V.90, V.34 or V.34bis analog modem connection, a cable modem, an ATM (Asynchronous Transfer Mode) connection, or an FDDI (Fiber Distributed Data Interface) or CDDI (Copper Distributed Data Interface) connection. Furthermore, communications may also include links to any of a variety of wireless networks, including WAP (Wireless Application Protocol), GPRS (General Packet Radio Service), GSM (Global System for

Mobile Communication), CDMA (Code Division Multiple Access) or TDMA (Time Division Multiple Access), cellular phone networks, GPS (Global Positioning System), CDPD (cellular digital packet data), RIM (Research in Motion, Limited) duplex paging network, Bluetooth radio, or an IEEE 802.11-based radio frequency network. The network 4028 can further include or interface with any one or more of an RS-232 serial connection, an IEEE-1394 (Firewire) connection, a Fiber Channel connection, an IrDA (infrared) port, a SCSI (Small Computer Systems Interface) connection, a USB (Universal Serial Bus) connection or other wired or wireless, digital or analog interface or connection, mesh or Digi® networking.

[0094] In general, a cloud-based computing environment is a resource that typically combines the computational power of a large grouping of processors (such as within web servers) and/or that combines the storage capacity of a large grouping of computer memories or storage devices. Systems that provide cloud-based resources may be utilized exclusively by their owners or such systems may be accessible to outside users who deploy applications within the computing infrastructure to obtain the benefit of large computational or storage resources.

[0095] The cloud is formed, for example, by a network of web servers that comprise a plurality of computing devices, such as the host machine 4002, with each server 4030 (or at least a plurality thereof) providing processor and/or storage resources. These servers manage workloads provided by multiple users (e.g., cloud resource customers or other users). Typically, each user places workload demands upon the cloud that vary in real-time, sometimes dramatically. The nature and extent of these variations typically depends on the type of business associated with the user.

[0096] It is noteworthy that any hardware platform suitable for performing the processing described herein is suitable for use with the technology. The terms “computer-readable storage medium” and “computer-readable storage media” as used herein refer to any medium or media that participate in providing instructions to a CPU for execution. Such media can take many forms, including, but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media include, for example, optical or magnetic disks, such as a fixed disk. Volatile media include dynamic memory, such as system RAM. Transmission media include coaxial cables, copper wire, and fiber optics, among others, including the wires that comprise one aspect of a bus. Transmission media can also take the form of acoustic or light waves, such as those generated during radio frequency (RF) and infrared (IR) data communications. Common forms of computer-readable media include, for example, a flexible disk, a hard disk, magnetic tape, any other magnetic medium, a CD-ROM disk, digital video disk (DVD), any other optical medium, any other physical medium with patterns of marks or holes, a RAM, a PROM, an EPROM, an EEPROM, a FLASH EPROM,

any other memory chip or data exchange adapter, a carrier wave, or any other medium from which a computer can read.

[0097] Various forms of computer-readable media may be involved in carrying one or more sequences of one or more instructions to a CPU for execution. A bus carries the data to system RAM, from which a CPU retrieves and executes the instructions. The instructions received by system RAM can optionally be stored on a fixed disk either before or after execution by a CPU.

[0098] Computer program code for carrying out operations for aspects of the present technology may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++, or the like and conventional procedural programming languages, such as the "C" programming language, Go, Python, or other programming languages, including assembly languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[0099] Examples of the devices, systems, and methods according to various aspects of the present disclosure are provided below in the following numbered clauses. An aspect of any of the devices(s), method(s), and/or system(s) may include any one or more than one, and any combination of, the numbered clauses described below.

[0100] Clause 1: A computer-implemented method, comprising: receiving, by a creator neural network, real transaction data and fraud detection rules, wherein the real transaction data corresponds to real transactions executed across a payment network, and wherein the fraud detection rules are for identifying fraudulent transactions; and generating, by the creator neural network, synthesized transaction data, wherein the synthesized transaction data corresponds to synthesized transactions that are not actually executed across the payment network, and wherein the fraud detection rules are updated based on the synthesized transaction data.

[0101] Clause 2: The computer-implemented method of Clause 1, further comprising: receiving, by an evaluator neural network, the synthesized transaction data; generating, by the evaluator neural network, risk scores for the synthesized transactions; and classifying, by the evaluator neural network, at least some of the synthesized transactions as fraudulent transactions based on the corresponding risk scores satisfying a predetermined threshold,

wherein the fraud detection rules are updated based on the synthesized transaction data and the risk scores.

[0102] Clause 3: The computer-implemented method of Clause 2, further comprising: receiving, by the evaluator neural network, the real transaction data; and classifying, by the evaluator neural network, each transaction represented by the real transaction data and the synthesized transaction data as a real transaction or a synthesized transaction.

[0103] Clause 4: The computer-implemented method of Clause 3, further comprising: training the creator neural network to cause the evaluator neural network to incorrectly classify synthesized transactions as real transactions.

[0104] Clause 5: The computer-implemented method of any of Clause 2-4, further comprising: receiving, by a fraud detection system, additional real transaction data in real time; identifying, by the fraud detection system, a first real transaction represented by the additional real transaction data as a fraudulent transaction based on the updated fraud detection rules; and denying, by the fraud detection system, the first real transaction.

[0105] Clause 6: The computer-implemented method of any of Clause 2-4, further comprising: receiving, by a fraud detection system, additional real transaction data in real time, wherein the fraud detection system comprises an online implementation of the evaluator neural network; classifying, by the online implementation of the evaluator neural network, a first real transaction represented by the real transaction data as a fraudulent transaction; and denying, by the fraud detection system, the first real transaction.

[0106] Clause 7: The computer-implemented method of any of Clauses 2-6, wherein the real transaction data comprises data corresponding to a transaction confirmed to be fraudulent.

[0107] Clause 8: A system, comprising: a creator model to: receive real transaction data corresponding to real transactions executed across a payment network; receive fraud detection rules for identifying fraudulent transactions; and generate synthesized transaction data based on the real transaction data and the fraud detection rules, wherein the synthesized transaction data corresponds to synthesized transactions that are not actually executed across the payment network; and an evaluator model to: receive the synthesized transaction data; and classify at least some of the synthesized transactions as fraudulent transactions.

[0108] Clause 9: The system of Clause 8, wherein the creator model comprises: a large language model to generate formatted fraud detection rules based on the fraud detection rules, wherein the creator model generates the synthesized transaction data based on the

real transaction data and the formatted fraud detection rules.

[0109] Clause 10: The system of any of Clauses 8-9, wherein the fraud detection rules comprise operating regulations, stand in processing rules, or risk rules, or a combination thereof.

[0110] Clause 11: The system of any of Clauses 8-10, wherein the creator model further comprises: a randomizer to reduce bias related to the synthesized transaction data generated by the creator model; and an aggregator to reduce bias related to the synthesized transaction data generated by the creator model.

[0111] Clause 12: The system of any of Clauses 8-11, further comprising a fraud detection system comprising the fraud detection rules, wherein the fraud detection system is to: update the fraud detection rules based on the synthesized transaction data; and send the updated fraud detection rules to the creator model; and wherein the creator model is to: generate additional synthesized transaction data based on the updated fraud detection rules.

[0112] Clause 13: The system of Clause 12, wherein the fraud detection system is to: receive additional real transaction data corresponding to additional real transactions; apply the fraud detection rules to the additional real transaction data; identify a first real transaction of the additional real transactions as fraudulent; and deny the first real transaction.

[0113] Clause 14: The system of any of Clauses 8-11, further comprising a fraud detection system, wherein the fraud detection system comprises an online implementation of the evaluator model.

[0114] Clause 15: The system of Clause 14, wherein the fraud detection system is to: receive additional real transaction data corresponding to additional real transactions; apply the additional real transaction data to the online implementation of the evaluator model to identify a first real transaction of the additional real transactions as fraudulent; and deny the first real transaction.

[0115] Clause 16: The system of any of Clauses 8-15, wherein the evaluator model is to: generate risk scores for the synthesized transactions; and classify the at least some of the synthesized transactions as fraudulent transactions based on the corresponding risk scores satisfying a predetermined threshold.

[0116] Clause 17: A computer-implemented method, comprising: receiving, by a transaction service provider server, real transaction data; identifying, by the transaction service provider server, a first fraudulent transaction by applying fraud detection rules to the real transaction data; denying, by the transaction service provider server, the first fraudulent transaction; generating, by the transaction service provider server, synthesized transaction

data based on the real transaction data; and generating, by the transaction service provider server, updated fraud detection rules based on the synthesized transaction data.

[0117] Clause 18: The computer-implemented method of Clause 17, wherein generating the synthesized transaction data based on the real transaction data comprises applying, by the transaction service provider server, the real transaction data to a generative adversarial network.

[0118] Clause 19: The computer-implemented method of any of Clauses 17-18, further comprising: receiving, by a transaction service provider server, additional real transaction data; identifying, by the transaction service provider server, a second fraudulent transaction by applying the updated fraud detection rules to the additional real transaction data; and denying, by the transaction service provider server, the second fraudulent transaction.

[0119] Clause 20: The computer-implemented method of Clause 19, the method further comprising: generating, by the transaction service provider server, additional synthesized transaction data based on the additional real transaction data; and generating, by the transaction service provider server, further updated fraud detection rules based on the additional synthesized transaction data.

[0120] Further, it is understood that any one or more of the following-described forms, expressions of forms, examples, can be combined with any one or more of the other following-described forms, expressions of forms, and examples.

[0121] While several forms have been illustrated and described, it is not the intention of Applicant to restrict or limit the scope of the appended claims to such detail. Numerous modifications, variations, changes, substitutions, combinations, and equivalents to those forms may be implemented and will occur to those skilled in the art without departing from the scope of the present disclosure. Moreover, the structure of each element associated with the described forms can be alternatively described as a means for providing the function performed by the element. Also, where materials are disclosed for certain components, other materials may be used. It is therefore to be understood that the foregoing description and the appended claims are intended to cover all such modifications, combinations, and variations as falling within the scope of the disclosed forms. The appended claims are intended to cover all such modifications, variations, changes, substitutions, modifications, and equivalents.

[0122] As used herein, a “server” may include one or more computing devices which can be individual, stand-alone machines located at the same or different locations, may be owned or operated by the same or different entities, and may further be one or more clusters of distributed computers or “virtual” machines housed within a datacenter. It should be

understood and appreciated by a person of skill in the art that functions performed by one “server” can be spread across multiple disparate computing devices for various reasons. As used herein, a “server” is intended to refer to all such scenarios and should not be construed or limited to one specific configuration. Further, a server as described herein may, but need not, reside at (or be operated by) a merchant, a payment network, a financial institution, a healthcare provider, a social media provider, a government agency, or agents of any of the aforementioned entities. The term “server” also may refer to or include one or more processors or computers, storage devices, or similar computer arrangements that are operated by or facilitate communication and processing for multiple parties in a network environment, such as the Internet, although it will be appreciated that communication may be facilitated over one or more public or private network environments and that various other arrangements are possible. Further, multiple computers, *e.g.*, servers, or other computerized devices, *e.g.*, point-of-sale devices, directly or indirectly communicating in the network environment may constitute a “system,” such as a merchant’s point-of-sale system. Reference to “a server” or “a processor,” as used herein, may refer to a previously recited server and/or processor that is recited as performing a previous step or function, a different server and/or processor, and/or a combination of servers and/or processors. For example, as used in the specification and the claims, a first server and/or a first processor that is recited as performing a first step or function may refer to the same or different server and/or a processor recited as performing a second step or function.

[0123] As used herein, a “server computer” may describe a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. The server computer may be associated with an entity such as a payment processing network, a wallet provider, a merchant, an authentication cloud, an acquirer or an issuer. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers. In some embodiments or aspects, the server computer may provide and/or support payment network cloud service.

[0124] Reference to “a device,” “a server,” “a processor,” and/or the like, as used herein, may refer to a previously recited device, server, or processor that is recited as performing a previous step or function, a different server or processor, and/or a combination of servers and/or processors. For example, as used in the specification and the claims, a first server or

a first processor that is recited as performing a first step or a first function may refer to the same or different server or the same or different processor recited as performing a second step or a second function.

[0125] One or more components may be referred to herein as “configured to,” “configurable to,” “operable/operative to,” “adapted/adaptable,” “able to,” “conformable/conformed to,” etc. Those skilled in the art will recognize that “configured to” can generally encompass active-state components and/or inactive-state components and/or standby-state components, unless context requires otherwise.

[0126] Those skilled in the art will recognize that, in general, terms used herein, and especially in the appended claims (e.g., bodies of the appended claims) are generally intended as “open” terms (e.g., the term “including” should be interpreted as “including but not limited to,” the term “having” should be interpreted as “having at least,” the term “includes” should be interpreted as “includes but is not limited to,” etc.). It will be further understood by those within the art that if a specific number of an introduced claim recitation is intended, such an intent will be explicitly recited in the claim, and in the absence of such recitation no such intent is present. For example, as an aid to understanding, the following appended claims may contain usage of the introductory phrases “at least one” and “one or more” to introduce claim recitations. However, the use of such phrases should not be construed to imply that the introduction of a claim recitation by the indefinite articles “a” or “an” limits any particular claim containing such introduced claim recitation to claims containing only one such recitation, even when the same claim includes the introductory phrases “one or more” or “at least one” and indefinite articles such as “a” or “an” (e.g., “a” and/or “an” should typically be interpreted to mean “at least one” or “one or more”); the same holds true for the use of definite articles used to introduce claim recitations.

[0127] The term “substantially,” “about,” or “approximately” as used in the present disclosure, unless otherwise specified, means an acceptable error for a particular value as determined by one of ordinary skill in the art, which depends in part, on how the value is measured or determined. In certain aspects, the term “substantially,” “about,” or “approximately” means within 1, 2, 3, or 4 standard deviations. In certain aspects, the term “substantially,” “about,” or “approximately” means within 50%, 20%, 15%, 10%, 9%, 8%, 7%, 6%, 5%, 4%, 3%, 2%, 1%, 0.5%, or 0.05% of a given value or range.

[0128] In addition, even if a specific number of an introduced claim recitation is explicitly recited, those skilled in the art will recognize that such recitation should typically be interpreted to mean at least the recited number (e.g., the bare recitation of “two recitations,” without other modifiers, typically means at least two recitations, or two or more recitations).

Furthermore, in those instances where a convention analogous to “at least one of A, B, and C, etc.” is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., “a system having at least one of A, B, and C” would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). In those instances where a convention analogous to “at least one of A, B, or C, etc.” is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., “a system having at least one of A, B, or C” would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). It will be further understood by those within the art that typically a disjunctive word and/or phrase presenting two or more alternative terms, whether in the description, claims, or drawings, should be understood to contemplate the possibilities of including one of the terms, either of the terms, or both terms unless context dictates otherwise. For example, the phrase “A or B” will be typically understood to include the possibilities of “A” or “B” or “A and B.”

[0129] With respect to the appended claims, those skilled in the art will appreciate that recited operations therein may generally be performed in any order. Also, although various operational flow diagrams are presented in a sequence(s), it should be understood that the various operations may be performed in other orders than those which are illustrated, or may be performed concurrently. Examples of such alternate orderings may include overlapping, interleaved, interrupted, reordered, incremental, preparatory, supplemental, simultaneous, reverse, or other variant orderings, unless context dictates otherwise. Furthermore, terms like “responsive to,” “related to,” or other past-tense adjectives are generally not intended to exclude such variants, unless context dictates otherwise.

[0130] It is worthy to note that any reference to “one aspect,” “an aspect,” “an exemplification,” “one exemplification,” and the like means that a particular feature, structure, or characteristic described in connection with the aspect is included in at least one aspect. Thus, appearances of the phrases “in one aspect,” “in an aspect,” “in an exemplification,” and “in one exemplification” in various places throughout the specification are not necessarily all referring to the same aspect. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more aspects.

[0131] As used herein, the singular form of “a,” “an,” and “the” include the plural references unless the context clearly dictates otherwise.

[0132] Any patent application, patent, non-patent publication, or other disclosure material referred to in this specification and/or listed in any Application Data Sheet is

incorporated by reference herein, to the extent that the incorporated materials is not inconsistent herewith. As such, and to the extent necessary, the disclosure as explicitly set forth herein supersedes any conflicting material incorporated herein by reference. Any material, or portion thereof, that is said to be incorporated by reference herein, but which conflicts with existing definitions, statements, or other disclosure material set forth herein will only be incorporated to the extent that no conflict arises between that incorporated material and the existing disclosure material.

[0133] In summary, numerous benefits have been described which result from employing the concepts described herein. The foregoing description of the one or more forms has been presented for purposes of illustration and description. It is not intended to be exhaustive or limiting to the precise form disclosed. Modifications or variations are possible in light of the above teachings. The one or more forms were chosen and described in order to illustrate principles and practical application to thereby enable one of ordinary skill in the art to utilize the various forms and with various modifications as are suited to the particular use contemplated. It is intended that the claims submitted herewith define the overall scope.

CLAIMS

What is claimed is:

1. A computer-implemented method, comprising:
receiving, by a creator neural network, real transaction data and fraud detection rules, wherein the real transaction data corresponds to real transactions executed across a payment network, and wherein the fraud detection rules are for identifying fraudulent transactions; and
generating, by the creator neural network, synthesized transaction data, wherein the synthesized transaction data corresponds to synthesized transactions that are not actually executed across the payment network, and wherein the fraud detection rules are updated based on the synthesized transaction data.
2. The computer-implemented method of Claim 1, further comprising:
receiving, by an evaluator neural network, the synthesized transaction data;
generating, by the evaluator neural network, risk scores for the synthesized transactions; and
classifying, by the evaluator neural network, at least some of the synthesized transactions as fraudulent transactions based on the corresponding risk scores satisfying a predetermined threshold, wherein the fraud detection rules are updated based on the synthesized transaction data and the risk scores.
3. The computer-implemented method of Claim 2, further comprising:
receiving, by the evaluator neural network, the real transaction data; and
classifying, by the evaluator neural network, each transaction represented by the real transaction data and the synthesized transaction data as a real transaction or a synthesized transaction.
4. The computer-implemented method of Claim 3, further comprising:
training the creator neural network to cause the evaluator neural network to incorrectly classify synthesized transactions as real transactions.
5. The computer-implemented method of Claim 2, further comprising:
receiving, by a fraud detection system, additional real transaction data in real time;
identifying, by the fraud detection system, a first real transaction represented by the additional real transaction data as a fraudulent transaction based on the updated fraud detection rules; and

denying, by the fraud detection system, the first real transaction.

6. The computer-implemented method of Claim 2, further comprising:
 - receiving, by a fraud detection system, additional real transaction data in real time, wherein the fraud detection system comprises an online implementation of the evaluator neural network;
 - classifying, by the online implementation of the evaluator neural network, a first real transaction represented by the real transaction data as a fraudulent transaction; and
 - denying, by the fraud detection system, the first real transaction.
7. The computer-implemented method of Claim 1, wherein the real transaction data comprises data corresponding to a transaction confirmed to be fraudulent.
8. A system, comprising:
 - a creator model to:
 - receive real transaction data corresponding to real transactions executed across a payment network;
 - receive fraud detection rules for identifying fraudulent transactions; and
 - generate synthesized transaction data based on the real transaction data and the fraud detection rules, wherein the synthesized transaction data corresponds to synthesized transactions that are not actually executed across the payment network; and
 - an evaluator model to:
 - receive the synthesized transaction data; and
 - classify at least some of the synthesized transactions as fraudulent transactions.
9. The system of Claim 8, wherein the creator model comprises:
 - a large language model to generate formatted fraud detection rules based on the fraud detection rules, wherein the creator model generates the synthesized transaction data based on the real transaction data and the formatted fraud detection rules.
10. The system of Claim 9, wherein the fraud detection rules comprise operating regulations, stand in processing rules, or risk rules, or a combination thereof.
11. The system of Claim 9, wherein the creator model further comprises:
 - a randomizer to reduce bias related to the synthesized transaction data generated by the creator model; and

an aggregator to reduce bias related to the synthesized transaction data generated by the creator model.

12. The system of Claim 11, further comprising a fraud detection system comprising the fraud detection rules, wherein the fraud detection system is to:

update the fraud detection rules based on the synthesized transaction data; and
send the updated fraud detection rules to the creator model; and

wherein the creator model is to:

generate additional synthesized transaction data based on the updated fraud detection rules.

13. The system of Claim 12, wherein the fraud detection system is to:

receive additional real transaction data corresponding to additional real transactions;
apply the fraud detection rules to the additional real transaction data;
identify a first real transaction of the additional real transactions as fraudulent; and
deny the first real transaction.

14. The system of Claim 11, further comprising a fraud detection system, wherein the fraud detection system comprises an online implementation of the evaluator model.

15. The system of Claim 14, wherein the fraud detection system is to:

receive additional real transaction data corresponding to additional real transactions;
apply the additional real transaction data to the online implementation of the evaluator model to identify a first real transaction of the additional real transactions as fraudulent; and
deny the first real transaction.

16. The system of Claim 8, wherein the evaluator model is to:

generate risk scores for the synthesized transactions; and
classify the at least some of the synthesized transactions as fraudulent transactions based on the corresponding risk scores satisfying a predetermined threshold.

17. A computer-implemented method, comprising:

receiving, by a transaction service provider server, real transaction data;
identifying, by the transaction service provider server, a first fraudulent transaction by applying fraud detection rules to the real transaction data;
denying, by the transaction service provider server, the first fraudulent transaction;

generating, by the transaction service provider server, synthesized transaction data based on the real transaction data; and

generating, by the transaction service provider server, updated fraud detection rules based on the synthesized transaction data.

18. The computer-implemented method of Claim 17, wherein generating the synthesized transaction data based on the real transaction data comprises applying, by the transaction service provider server, the real transaction data to a generative adversarial network.

19. The computer-implemented method of Claim 18, further comprising:
receiving, by a transaction service provider server, additional real transaction data;
identifying, by the transaction service provider server, a second fraudulent transaction by applying the updated fraud detection rules to the additional real transaction data; and
denying, by the transaction service provider server, the second fraudulent transaction.

20. The computer-implemented method of Claim 19, the method further comprising:
generating, by the transaction service provider server, additional synthesized transaction data based on the additional real transaction data; and
generating, by the transaction service provider server, further updated fraud detection rules based on the additional synthesized transaction data.