CLAIMS

WHAT IS CLAIMED IS:

1. A computer-implemented method for real-time automated teller machine (ATM) fraud detection and prevention, the method comprising: generating, with at least one processor, at least one predetermined ATM activity threshold at least partly by a machine learning model trained on historic transaction data for a plurality of payment devices; receiving, with at least one processor, transaction data of a plurality of transactions completed by at least one ATM, the transaction data received in real-time during transaction processing at a transaction service provider system; storing, with at least one processor, the transaction data in a distributed cache for aggregation and recall of the transaction data; receiving, with at least one processor, a transaction request for a user transaction at a first ATM of the at least one ATM using a payment device, the transaction request comprising a payment device identifier; in response to receiving the transaction request, and before completion of the user transaction at the first ATM: modifying, with at least one processor, a profile of ATM activity stored in the distributed cache and associated with the payment device identifier, the profile comprising metrics comprising at least ATM transaction value data and ATM transaction count data, wherein modifying the profile of ATM activity comprises aggregating at least one of the metrics of the profile based on the user transaction; comparing, with at least one processor, at least one metric of the profile of ATM activity to the at least one predetermined ATM activity threshold; and in response to determining that the at least one metric satisfies the at least one predetermined ATM activity threshold, activating, or causing the activation of, with at least one processor, a fraud prevention operation before the user transaction is completed at the first ATM, the fraud prevention operation comprising at least one of the following: declining the user transaction, disabling a transaction account associated with the payment device identifier, communicating an alert to an issuer, or any combination thereof; retraining, with at least one processor, the machine learning model based at least partly on the transaction data received in real-time during processing of the transaction data, to produce an updated machine learning model; regenerating, with at least one processor, the at least one predetermined ATM activity threshold at least partly by the updated machine learning model, to produce at least one updated predetermined ATM activity threshold; receiving, with at least one processor, a new transaction request for a new user transaction at a second ATM of the at least one ATM; comparing, with at least one processor, at least one metric of the profile of ATM activity to the at least one updated predetermined ATM activity threshold; and in response to determining that the at least one metric satisfies the at least one updated predetermined ATM activity threshold, activating, or causing the activation of, with at least one processor, a second fraud prevention operation for the new user transaction.

2. The computer-implemented method of claim 1, wherein the first ATM is communicatively connected to the distributed cache and programmed and/or configured to aggregate the transaction data with data from the user transaction during processing of the user transaction.

3. The computer-implemented method of claim 2, wherein (i) comparing the at least one metric to the at least one predetermined ATM activity threshold and (ii) activating, or causing the activation of, the fraud prevention operation, are executed by the first ATM in real-time with processing the user transaction.

4. The computer-implemented method of claim 1, wherein the machine learning model is regularly updated based on the transaction data received in real-time during processing of the

transaction data, and wherein the at least one predetermined ATM activity threshold is regenerated at regular intervals at least partly by the machine learning model.

5. The computer-implemented method of claim 1, wherein the at least one metric further comprises ATM transaction time data, and wherein the fraud prevention operation is activated in response to determining a count of ATM transactions associated with the payment device identifier in a time period satisfies the at least one predetermined ATM activity threshold comprising an upper threshold count of transactions.

6. The computer-implemented method of claim 1, wherein the at least one metric further comprises ATM transaction location data, and wherein the fraud prevention operation is activated in response to determining a count of ATM transactions associated with the payment device identifier in a geographic region satisfies the at least one predetermined ATM activity threshold comprising an upper threshold count of transactions in the geographic region.

7. The computer-implemented method of claim 1, wherein the at least one metric further comprises ATM transaction time data and ATM transaction location data, and wherein the fraud prevention operation is activated in response to determining a time interval between a first ATM transaction of the payment device and a second ATM transaction of the payment device satisfies the at least one predetermined ATM activity threshold comprising a lower threshold time interval, the lower threshold representative of an unlikely or impossible travel time between a location of the first ATM transaction and a location of the second ATM transaction.

8. A system for real-time automated teller machine (ATM) fraud detection and prevention, the system comprising: a distributed cache; and a server including at least one processor for executing program instructions, the server being programmed and/or configured to: generate at least one predetermined ATM activity threshold at least partly by a machine learning model trained on historic transaction data for a plurality of payment devices; receive transaction data of a plurality of transactions completed by at least one ATM, the transaction data received in real-time during transaction processing at a transaction service provider system; store the transaction data in the distributed cache for aggregation and recall of the transaction data; receive a transaction request for a user transaction at a first ATM of the at least one ATM using a payment device, the transaction request comprising a payment device identifier; in response to receiving the transaction request, and before completion of the user transaction at the first ATM: modify a profile of ATM activity stored in the distributed cache and associated with the payment device identifier, the profile comprising metrics comprising at least ATM transaction value data and ATM transaction count data, wherein, when modifying the profile of ATM activity, the server is programmed and/or configured to aggregate at least one of the metrics of the profile based on the user transaction; compare at least one metric of the profile of ATM activity to the at least one predetermined ATM activity threshold; and in response to determining that the at least one metric satisfies the at least one predetermined ATM activity threshold, activate, or cause the activation of, a fraud prevention operation before the user transaction is completed at the first ATM, the fraud prevention operation comprising at least one of the following: declining the user transaction, disabling a transaction account associated with the payment device identifier, communicating an alert to an issuer, or any combination

thereof; retrain the machine learning model based at least partly on the transaction data received in real-time during processing of the transaction data, to produce an updated machine learning model; regenerate the at least one predetermined ATM activity threshold at least partly by the updated machine learning model, to produce at least one updated predetermined ATM activity threshold; receive a new transaction request for a new user transaction at a second ATM of the at least one ATM; compare at least one metric of the profile of ATM activity to the at least one updated predetermined ATM activity threshold; and in response to determining that the at least one metric satisfies the at least one updated predetermined ATM activity threshold, activate, or cause the activation of, a second fraud prevention operation for the new user transaction.

9. The system of claim 8, wherein the machine learning model is regularly updated based on the transaction data received in real-time during processing of the transaction data, and wherein the at least one predetermined ATM activity threshold is regenerated at regular intervals at least partly by the machine learning model.

10. The system of claim 8, wherein the at least one metric further comprises ATM transaction time data, and wherein the fraud prevention operation is activated in response to determining a count of ATM transactions associated with the payment device identifier in a time period satisfies the at least one predetermined ATM activity threshold comprising an upper threshold count of transactions.

11. The system of claim 8, wherein the at least one metric further comprises ATM transaction location data, and wherein the fraud prevention operation is activated in response to determining a count of ATM transactions associated with the payment device identifier in a geographic region satisfies the at least one predetermined ATM activity threshold comprising an upper threshold count of transactions in the geographic region.

12. The system of claim 8, wherein the at least one metric further comprises ATM transaction time data and ATM transaction location data, and wherein the fraud prevention operation is activated in response to determining a time interval between a first ATM transaction of the payment device and a second ATM transaction of the payment device satisfies the at least one predetermined ATM activity threshold comprising a lower threshold time interval, the lower threshold representative of an unlikely or impossible travel time between a location of the first ATM transaction and a location of the second ATM transaction.

13. A computer program product for real-time automated teller machine (ATM) fraud detection and prevention, the computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, cause the at least one processor to: generate at least one predetermined ATM activity threshold at least partly by a machine learning model trained on historic transaction data for a plurality of payment devices; receive transaction data of a plurality of transactions completed by at least one ATM, the transaction data received in real-time during transaction processing at a transaction service provider system; store the transaction data in a distributed cache for aggregation and recall of the transaction data; receive a transaction request for a

user transaction at a first ATM of the at least one ATM using a payment device, the transaction request comprising a payment device identifier; in response to receiving the transaction request, and before completion of the user transaction at the first ATM: modify a profile of ATM activity stored in the distributed cache and associated with the payment device identifier, the profile comprising metrics comprising at least ATM transaction value data and ATM transaction count data, wherein the program instructions that cause the at least one processor to modify the profile of ATM activity cause the at least one processor to aggregate at least one of the metrics of the profile based on the user transaction; compare at least one metric of the profile of ATM activity to at least one predetermined ATM activity threshold; and in response to determining that the at least one metric satisfies the at least one predetermined ATM activity threshold, activate, or cause the activation of, a fraud prevention operation before the user transaction is completed at the first ATM, the fraud prevention operation comprising at least one of the following: declining the user transaction, disabling a transaction account associated with the payment device identifier, communicating an alert to an issuer, or any combination thereof; retrain the machine learning model based at least partly on the transaction data received in real-time during processing of the transaction data, to produce an updated machine learning model; regenerate the at least one predetermined ATM activity threshold at least partly by the updated machine learning model, to produce at least one updated predetermined ATM activity threshold; receive a new transaction request for a new user transaction at a second ATM of the at least one ATM; compare at least one metric of the profile of ATM activity to the at least one updated predetermined ATM activity threshold; and in response to determining that the at least one metric satisfies the at least one updated predetermined ATM activity threshold, activate, or cause the activation of, a second fraud prevention operation for the new user transaction.

14. The computer program product of claim 13, wherein the machine learning model is regularly updated based on the transaction data received in real-time during processing of the transaction data, and wherein the at least one predetermined ATM activity threshold is regenerated at regular intervals at least partly by the machine learning model.

15. The computer program product of claim 13, wherein the at least one metric further comprises ATM transaction time data, and wherein the fraud prevention operation is activated in response to determining a count of ATM transactions associated with the payment device identifier in a time period satisfies the at least one predetermined ATM activity threshold comprising an upper threshold count of transactions.

16. The computer program product of claim 13, wherein the at least one metric further comprises ATM transaction location data, and wherein the fraud prevention operation is activated in response to determining a count of ATM transactions associated with the payment device identifier in a geographic region satisfies the at least one predetermined ATM activity threshold comprising an upper threshold count of transactions in the geographic region.

17. The computer program product of claim 13, wherein the at least one metric further comprises ATM transaction time data and ATM transaction location data, and wherein the fraud prevention operation is activated in response to determining a time interval between a first ATM transaction of the payment device and a second ATM transaction of the payment

device satisfies the at least one predetermined ATM activity threshold comprising a lower threshold time interval, the lower threshold representative of an unlikely or impossible travel time between a location of the first ATM transaction and a location of the second ATM transaction.