CLAIMS

What is claimed is:

1. A transaction card, comprising:

a plurality of interfaces;

a processor; and

a memory storing instructions which when executed by the processor, cause the processor to:

detect, by a quality assurance applet executing on the processor, a transaction attempt via an interface of the plurality of interfaces;

determine, by the quality assurance applet, data associated with the transaction attempt, the data comprising a timestamp associated with the transaction attempt, and an interface type of the interface on which the transaction attempt was detected;

store, by the quality assurance applet, the data associated with the transaction attempt in the memory;

detect, by the quality assurance applet, a read for the data by a computing device made via the interface of the plurality interfaces;

generate, by the quality assurance applet, encrypted data from the data associated with the transaction attempt stored in the memory, the encrypted data generated based on a cryptographic algorithm, a customer identifier, and a private key; and

provide, by the quality assurance applet, the encrypted data to the computing device via the interface on which the read was detected.

2. The transaction card of claim 1, wherein the interface on which the transaction attempt is detected is one of a contact interface or a contactless interface, the contact interface comprising a magstripe interface or an EMV interface, and the contactless interface comprising a near-field communication (NFC) interface.

3. The transaction card of claim 1, wherein the quality assurance applet is configured as a default applet on the transaction card to enable detection of the transaction attempt.

4. The transaction card of claim 1, wherein the data associated with the transaction attempt further comprises a transaction identifier to identify the transaction attempt, and a transaction terminal identifier to identify a transaction terminal.

5. The transaction card of claim 4, wherein the detection of the transaction attempt includes receiving at least a portion of the data from the transaction terminal, the portion of the data comprising the timestamp, the interface type, or combination thereof.

6. The transaction card of claim 1, wherein the data associated with the transaction attempt is stored with other data corresponding with other transaction attempts.

7. The transaction card of claim 6, wherein the encrypted data further comprises other data corresponding to the other transaction attempts, and the processor to provide the encrypted data including the data and the other data to the computing device as a batch communication.

8. The transaction card of claim 1, wherein the interface on which the read is detected, and the encrypted data is provided is a near-field communication (NFC) interface, and the encrypted data is provided in one or more NFC Data Exchange Format (NDEF) messages.

9. A transaction system comprising:

a processor;

storage comprising a data store; and

a memory storing instructions which when executed by the processor, cause the processor to:

receive, via an interface coupled with the processor, data associated with a plurality of transaction attempts performed with a transaction card associated with a user account, the data comprising entries associated with ~~the~~ transaction attempts, each entry for each transaction attempt including a timestamp for a corresponding transaction attempt, and an interface type for the transaction attempt;

store the data in the data store;

determine interface information for one or more interfaces of the transaction card based on the data, the interface information to indicate anomalies and interface usage statistics associated with the one or more interfaces; and

cause an action based on the interface information.

10. The system of claim 9, wherein the data is encrypted and received from the transaction card via a computing device communicatively coupled via the interface.

11. The system of claim 9, wherein each entry associated with each of the transaction attempts includes a transaction identifier, and a point-of-sale (POS) identifier to identify a POS terminal.

12. The system of claim 9, the processor to:

compare timestamps of consecutive transaction attempts in the data;

determine that a difference between the timestamps is within a reattempt transaction threshold;

determine an interface type associate with a first in-time transaction attempt of the consecutive transaction attempts; and

indicate a failed transaction attempt in an entry corresponding to the first in-time transaction attempt.

13. The system of claim 9, wherein the usage statistics indicate a number of failed transaction attempts correspond with an interface of the transaction card.

14. The system of claim 9, wherein the usage statistics indicate a number of transaction attempts utilizing a contact interface and a number of transaction attempts utilizing a contactless interface.

15. The system of claim 14, wherein the usage statistics indicate whether each of the transaction attempts for the contact interface and the contactless interface was successful or not successful.

16. The system of claim 9, the processor to:

receive additional data associated with a plurality of transaction cards and user accounts;

store the additional data in the data store;

determine interface information for the plurality of transaction cards based on the data; and

determine an anomaly associated with a POS terminal based on the interface information for the plurality of transaction cards.

17. The system of claim 16, wherein the action comprises sending a device associated with the POS terminal an indication of the anomaly.

18. The system of claim 9, wherein the action comprises sending a user associated with the user account a replacement transaction card, communicating a text message to a device associated with the user account, or sending instructions to perform a contactless interface transaction to the device associated, or combination thereof.

19. A computer-implemented method, comprising:

detecting, by a quality assurance applet executing on a processor, a transaction attempt via one of a plurality of interfaces;

receiving, by the quality assurance applet, data associated with the transaction attempt, the data comprising a timestamp associated with the transaction attempt, and an interface type of the one of the plurality of interfaces;

storing, by the quality assurance applet, the data in a storage structure of a memory;

detecting, by the quality assurance applet, a read for the data by a computing device made via a Near-Field Communication (NFC) interface of the plurality interfaces;

encrypting, by the quality assurance applet, the data associated with the transaction attempt utilizing a cryptographic algorithm, a customer identifier, and a private key; and

causing communication, by the quality assurance applet, of the data to the computing device via the NFC interface.

20. The computer-implemented method of claim 19, wherein the interface on which the transaction attempt is detected is one of a contact interface or a contactless interface, the contact interface comprising a magstripe interface or an EMV interface, and the contactless interface comprising the NFC interface.