the like) by another system, another device, another group of systems, or another group of devices, separate from or including merchant system 108, such as issuer system 104 (e.g., one or more devices of issuer system 104), a third customer device 106, transaction service provider system 102, acquirer system 110, a third party system, a government system, and/or the like. In some non-limiting embodiments or aspects, document verification system 402a, identity token system 402b, registry 402c, and/or any combination thereof may be implemented as a single system. Additionally or alternatively, at least one of (e.g., each of) document verification system 402a, identity token system 402b, and/or registry 402c may be implemented as a separate system (e.g., separate from the others).

[0128] As shown in FIG. 4A, at 422, implementation 400 may include logging into a secure mobile application. For example, sponsor device 406a may log into the secure mobile application, e.g., via a strong authentication technique, as described herein.

[0129] In some non-limiting embodiments or aspects, as shown in FIG. 4B, a sponsoring user sponsor device 406a may include a secure mobile application. Additionally or alternatively, sponsor device 406a may log into the secure mobile application via a strong authentication technique, as described herein. For example, a sponsoring user may provide (e.g., input and/or the like) authentication data (e.g., data~~e~~ required by the strong authentication technique) to sponsor device 406a, which may use the authentication data to log into the secure mobile application.

[0130] With continued reference to FIG. 4A, at 424, implementation 400 may include authenticating and/or requesting a unique identifier. For example, sponsor device 406a may authenticate with (e.g., log into and/or the like), e.g., identity token system 402b, a secure mobile application associated therewith, and/or the like, as described herein. Additionally or alternatively, sponsor device 406a may request a unique identifier (e.g., first unique identifier), e.g., from identity token system 402b, as described herein.

[0131] In some non-limiting embodiments or aspects, as shown in FIG. 4D, sponsor device 406a associated with a sponsoring user may request a unique identifier (e.g., first unique identifier), e.g., from identity token system 402b, as described herein. In some non-limiting embodiments or aspects, sponsor device 406a may request the unique identifier before capturing an image of the enrolling user. Additionally or alternatively, sponsor device 406a may request the unique identifier after capturing the image of the enrolling user.

[0132] With continued reference to FIG. 4A, at 426, implementation 400 may include communicating a unique identifier. For example, identity token system 402b may communicate a unique identifier (e.g., a first unique identifier) to sponsor device 406a, as described herein.

registry 702c may be the same as or similar to registry 402c, registry 502c, registry 602c, transaction service provider system 102, and/or the like. In some non-limiting embodiments or aspects, relying party system 708 may be the same as or similar to relying party system 408, relying party system 508, relying party system 608, merchant system 108, and/or the like. In some non-limiting embodiments or aspects, identity token system 702b and registry 702c may be implemented as a single system. Additionally or alternatively, identity token system 702b and registry 702c may be implemented as separate systems.

[0161] As shown in FIG. 7, at 722, implementation 700 may include performing a transaction. For example, enrollee device 706b may initiate a transaction with relying party system 708, as described herein.

[0162] As shown in FIG. 7, at 724, implementation 700 may include waiting for a period of time (e.g., a selectable period of time, a preselected period of time, a predetermined period of time, a dynamic period of time, and/or the like). For example, relying party system 708 may wait for a period of time associated with a time it takes for a transaction to settle, as described herein.

[0163] As shown in FIG. 7, at 726, implementation 700 may include communicating event data associated with an event. For example, relying party system 708 may communicate the event data to identity token system 702b, as described herein. In some non-limiting embodiments or aspects, the event data may include negative event data associated with at least one negative event, as described herein. For example, the negative event data may include at least one of complaint data associated with a complaint, an indication (e.g., fraud indication and/or the like) associated with a fraudulent transaction, any combination thereof, and/or the like, as described herein.

[0164] As shown in FIG. 7, at 728, implementation 700 may include adjusting at least one trust score based on the event data. For example, identity token system 702b may adjust the trust score associated with the enrolling user associated with enrollee device 706b by degrading (e.g., reducing and/or the like) the trust score, as described herein.

[0165] Referring now to FIGS. 8A-8D, FIGS. 8A-8D are diagrams of an exemplary implementation of a tree 800 according to a non-limiting embodiment relating to process 300 shown in FIG. 3. As shown in FIGS. 8A-8D, tree 800 may include first node 806a, second node 806b, third node 806c, fourth node 806d, fifth node 806e, sixth node 806f, seventh node 806g, eighth node 806h, ninth node 806i, and/or tenth node 806j. In some non-limiting embodiments or aspects, tree 800 may be implemented (e.g., generated and/or the like) by an identity token system (e.g., identity token system 402b, identity token system 502b, identity token system 602b, identity token system 702b, transaction service provider system 102, and/or the like).

trust score) may be upgraded (e.g., increased) based on the new edge connecting sixth node 806f to second node 806b, as described herein. In some non-limiting embodiments or aspects, the sixth trust score associated with node 806f may now exceed the fifth trust score associated with fifth node 806e.

[0171] As shown in FIG. 8D, additional edges may be generated in tree 800 connecting seventh node 806g to eighth node 806h, ninth node 806i, and tenth node 806j (e.g., based on newly enrolling users being sponsored by the user associated with seventh node 806g), as described herein. Additionally or alternatively, an additional edge may be generated connecting tenth node 806j to ninth node 806i (e.g., based on the user associated with tenth node 806j sponsoring the user associated with ninth node 806i), as described herein. In some non-limiting embodiments or aspects, an eighth trust score associated with eighth node 806h, a ninth trust score associated with ninth node 806i, and a tenth trust score associated with tenth node 806j may be determined, as described herein. For example, each of the eighth trust score, ninth trust score, and tenth trust score may be lower than the seventh trust score.

[0172] In some non-limiting embodiments or aspects, event data associated with one of the nodes may be received, as described herein. For example, negative event data associated with ninth node 806i may be received, as described herein. In some non-limiting embodiments the trust score associated with ninth node 806i may be adjusted (e.g., degraded and/or the like) based on the event data. Additionally or alternatively, the trust score associated with each node (e.g., seventh node 806g, tenth node 808j, and/or the like) connected by one of the edges to ninth node 806i may be adjusted (e.g., degraded and/or the like) based on the event data. In some non-limiting embodiments or aspects, the trust score associated with at least some nodes ~~node~~ (e.g., eighth node 806h, fifth node 806e, and/or the like) indirectly connected to ninth node 806i may be adjusted (e.g., degraded and/or the like) based on the event data. For example, the trust score associated with eighth node 806h, which is connected to (e.g., sponsored by) seventh node 806g by an edge, may also be adjusted based on the adjustment of the trust score of seventh node 806g. Additionally or alternatively, the trust score associated with fifth node 806e, which is connected to (e.g., has sponsored) seventh node 806g by an edge, may also be adjusted based on the adjustment of the trust score of seventh node 806g. In some non-limiting embodiments or aspects, the number of indirect connections (e.g., hops and/or the like) away from the node associated with the event data (e.g., ninth node 806i and/or the like) for which trust scores will be adjusted may be configurable (e.g., selectable, preselected, predetermined, dynamic, and/or the like). Additionally or alternatively, a weight factor for the adjustment of the respective trust score of a respective node may be configurable (e.g., selectable, preselected, predetermined, dynamic, and/or the like) based on the number of indirect connections (e.g., hops and/or the like) away from the node associated with the event data (e.g., ninth node 806i and/or the like).