What is claimed is:

1. A computer-implemented method for performing a transaction with a merchant, the method comprising:

receiving, by a first server, card information associated with a payment card of a user from the merchant for performing the transaction based on the merchant receiving an indication that the user does not consent to the merchant storing the card information associated with the payment card of the user upon initiation of the transaction, wherein the first server is associated with an alternate identifier service, and wherein the first server comprises a database storing a plurality of alternative identifiers corresponding to a plurality of payment cards;

determining, by the first server, whether an alternate identifier for the card information is stored in the database;

in response to determining that the alternate identifier is not stored in the database, transmitting, by the first server, a request message to a second server, the request message comprising a request to provide a new alternate identifier, wherein the second server is associated with a card issuing network associated with the payment card;

generating, by the second server, the new alternate identifier for the payment card based on the card information;

transmitting, by the second server, a provisioning request message comprising the new alternate identifier to an issuer system;

upon receiving a provisioning approval from the issuer system, transmitting, by the second server, the new alternate identifier to the first server;

upon receiving a second request message from the first server, transmitting, by the second server, a cryptogram value associated with the new alternate identifier to the first server, wherein the cryptogram value is fetched, in real-time, based on receiving the new alternate identifier, and wherein the cryptogram is linked directly to the transaction as an authentication code;

transmitting, by the first server, the new alternate identifier and the cryptogram to the merchant, wherein the cryptogram is provided to the merchant in response to the transaction being routed through the first server, and wherein the merchant transmits the new alternate identifier and the cryptogram to at least one of a payment gateway or an acquirer for authentication;

receiving, by the second server, the new alternate identifier and the cryptogram from the at least one of the payment gateway or the acquirer;

validating, by the second server, the transaction based on the new alternate identifier and the cryptogram value;

transmitting, by the second server, a transaction message including the new alternate identifier and the card information associated with the payment card to the issuer system;

receiving, by the second server, a transaction response from the issuer system, the transaction response indicating completion or rejection of the transaction; and

transmitting, by the second server, the new alternate identifier and the transaction response to the at least one of the payment gateway or the acquirer, wherein the at least one of the payment gateway or the acquirer transmits the new alternate identifier and the transaction response to the merchant, and wherein the merchant uses the new alternate identifier for at least one post-transaction activity associated with the transaction.

2. The computer-implemented method of claim 1, wherein the card information comprises a Primary Account Number (PAN) of the user.

3. The computer-implemented method of claim 1, wherein the transaction is at least one of the following: a guest checkout transaction, a payment transaction, or any combination thereof.

4. The computer-implemented method of claim 1, further comprising:

storing, by the first server, the new alternate identifier for the card information in the memory of the first server upon receiving the new alternate identifier from the second server.

5. A system for performing a transaction with a merchant, the system comprising:

a first server configured to:

receive card information associated with a payment card of a user from the merchant for performing the transaction based on the merchant receiving an indication that the user does not consent to the merchant storing the card information associated with the payment card of the user upon initiation of the transaction, wherein the first server is associated with an alternate identifier service, and wherein the first server comprises a database storing a plurality of alternative identifiers corresponding to a plurality of payment cards;

determine whether an alternate identifier for the card information is stored in the database; and

in response to determining that the alternate identifier is not stored in the database, transmit a request message to a second server, the request message comprising a request to provide a new alternate identifier, wherein the second server is associated with a card issuing network associated with the payment card,

wherein the second server is communicatively coupled to the first server, and wherein the second server is configured to:

generate the new alternate identifier for the payment card based on the card information;

transmit a provisioning request message comprising the new alternate identifier to an issuer system;

upon receiving a provisioning approval from the issuer system, transmit the new alternate identifier to the first server; and

upon receiving a second request message from the first server, transmit a cryptogram value associated with the new alternate identifier to the first server, wherein the cryptogram value is fetched, in real-time, based on receiving the new alternate identifier, and wherein the cryptogram is linked directly to the transaction as an authentication code;

wherein the first server is further configured to:

transmit the new alternate identifier and the cryptogram to the merchant, wherein the cryptogram is provided to the merchant in response to the transaction routed through the first server, and wherein the merchant transmits the new alternate identifier and the cryptogram to at least one of a payment gateway or an acquirer for authentication;

wherein the second server is further configured to:

receive the new alternate identifier and the cryptogram from the at least one of the payment gateway or the acquirer;

validate the transaction based on the new alternate identifier and the cryptogram value;

transmit a transaction message including the new alternate identifier and the card information associated with the payment card to the issuer system;

receive a transaction response from the issuer system, the transaction response indicating completion or rejection of the transaction; and

transmit the new alternate identifier and the transaction response to the at least one of the payment gateway or the acquirer, wherein the at least one of the payment gateway or the acquirer transmits the new alternate identifier and the transaction response to the merchant, and wherein the merchant uses the new alternate identifier for at least one post-transaction activity associated with the transaction.

6. The system of claim 5, wherein the card information comprises a Primary Account Number (PAN) of the user.

7. The system of claim 5, wherein the transaction is one of a guest checkout transaction and a payment transaction.

8. The system of claim 5, wherein the first server is further configured to:

store the new alternate identifier for the card information in the memory of the first server upon receiving the new alternate identifier from the second server.

9. A non-transitory computer readable medium including instructions stored thereon that, when processed by at least one processor, cause a system to perform operations comprising:

receiving, by a first server, card information associated with a payment card of a user from a merchant for performing a transaction based on the merchant receiving an indication that the user does not consent to the merchant storing the card information associated with the payment card of the user upon initiation of the transaction, wherein the first server is associated with an alternate identifier service, and wherein the first server comprises a database storing a plurality of alternative identifiers corresponding to a plurality of payment cards;

determining, by the first server, whether an alternate identifier for the card information is stored in the database;

in response to determining that the alternate identifier is not stored in the database, transmitting, by the first server, a request message to a second server, the request message comprising a request to provide a new alternate identifier, wherein the second server is associated with a card issuing network associated with the payment card;

generating, by the second server, the new alternate identifier for the payment card based on the card information;

transmitting, by the second server, a provisioning request message comprising the new alternate identifier to an issuer system;

upon receiving a provisioning approval from the issuer system, transmitting, by the second server, the new alternate identifier to the first server;

upon receiving a second request message from the first server, transmitting, by the second server, a cryptogram value associated with the new alternate identifier to the first server, wherein the cryptogram value is fetched,

in real-time, based on receiving the new alternate identifier, and wherein the cryptogram is linked directly to the transaction as an authentication code;

transmitting, by the first server, the new alternate identifier and the cryptogram to the merchant, wherein the cryptogram is provided to the merchant in response to the transaction being routed through the first server, and wherein the merchant transmits the new alternate identifier and the cryptogram to at least one of a payment gateway or an acquirer for authentication;

receiving, by the second server, the new alternate identifier and the cryptogram from the at least one of the payment gateway or the acquirer;

validating, by the second server, the transaction based on the new alternate identifier and the cryptogram value;

transmitting, by the second server, a transaction message including the new alternate identifier and the card information associated with the payment card to the issuer system;

receive, by the second server, a transaction response from the issuer system, the transaction response indicating completion or rejection of the transaction; and

transmitting, by the second server, the new alternate identifier and the transaction response to the at least one of the payment gateway or the acquirer, wherein the at least one of the payment gateway or the acquirer transmits the new alternate identifier and the transaction response to the merchant, and wherein the merchant uses the new alternate identifier for at least one post-transaction activity associated with the transaction.

10. The computer-implemented method of claim 1, wherein the at least one post-transaction activity comprises at least one of clearing, settlement, reconciliation, refunding, price calculation, discount calculation, or any combination thereof.

11. The system of claim 9, wherein the at least one post-transaction activity comprises at least one of clearing, settlement, reconciliation, refunding, price calculation, discount calculation, or any combination thereof.

12. The non-transitory computer readable medium of claim 9, wherein the at least one post-transaction activity comprises at least one of clearing, settlement, reconciliation, refunding, price calculation, discount calculation, or any combination thereof.