How Card Payments Happen

Sagar Udasi

May 14, 2024

Have you ever stopped to wonder what happens when you tap your credit card or enter your card details online? It all seems so instantaneous - a quick swipe or a few clicks, and your purchase is confirmed. In this article, we will explore the journey your payment information takes, from the moment you initiate a purchase to the final transfer of funds. We will meet the key players involved, from the merchant website and your bank to the invisible network that facilitates the entire process. So, let's get started!

1 Key Players Of the Card Payment

Let's meet the essential participants in the card payment process.

1. **Customer:** This is you, the one initiating the purchase. You could be using a physical credit card, debit card, or entering your card details on a website or mobile app.
2. **Merchant Website (MW):** This is the online platform where you make your purchase. Examples include online stores like Amazon, travel booking platforms, or even the website of your favorite local restaurant offering online ordering.
3. **Payment Gateway (PG):** Think of the PG as the secure middleman. It receives your encrypted payment data from the merchant website and routes it to the appropriate network for authorization. Popular payment gateways include Stripe, PayPal, and Authorize.Net.
4. **Acquiring Bank:** This is the bank that has a business relationship with the merchant. It handles receiving the authorization response and settlement of funds from the issuing bank.
5. **Card Network:** The card network acts as the invisible highway for your payment information. It acts as a bridge between the issuing and acquiring banks, facilitating communication and authorization checks. Visa, Mastercard, American Express, and Discover are some of the major card networks.
6. **Issuing Bank:** This is your bank, the one that issued your credit or debit card. It receives the authorization request from the card network, verifies your account details and available funds, and ultimately approves or declines the transaction.

One thing which I always struggled understanding was, *what's the use of Payment Gateway and Card Network?*

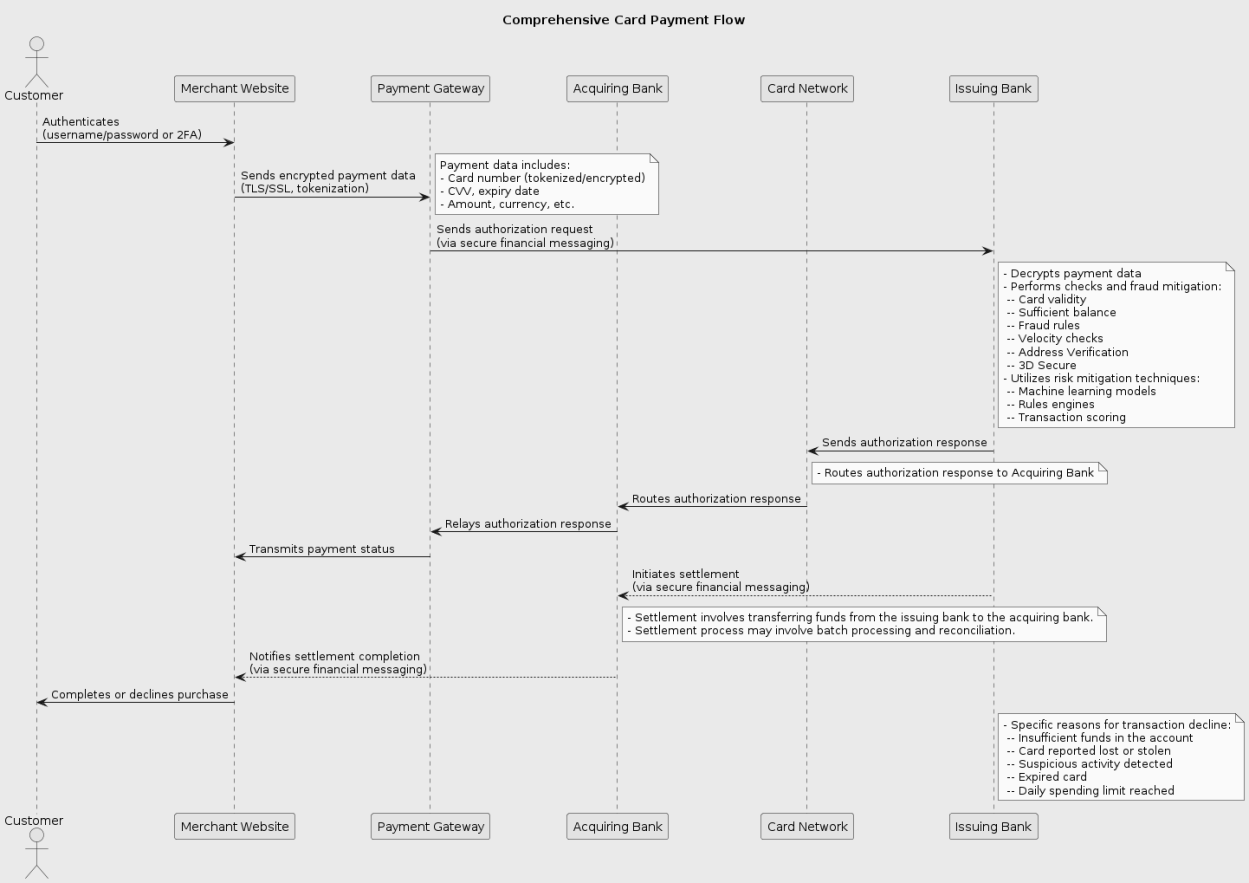
It's because of the Payment Gateway that merchants don't need to establish individual connections with every issuing bank, simplifying setup and maintenance. Merchants would need to manage their own security measures, potentially increasing the risk of data breaches. Gateways can integrate various payment methods (credit cards, debit cards, e-wallets, netbanking, UPI) into a single platform. If they are absent, customers might be restricted to fewer payment methods, hindering the shopping experience.

Every bank has its own protocols and direct communication between the banks could lead of compatibility problems and transaction failures. If banks handle transactions and settlements among themselves, transactions

might get limited to the specific region or country. Card networks provide a standardized communication protocol for authorization requests and responses between issuing and acquiring banks, regardless of their location. Because of their presence as the centralized source, international transactions become easy as the bank has now to just deal with the network provider. Now because all transactions are routed through the card network, we can have a centralized fraud detection system, identifying suspicious activity across different institutions. If there are multiple players communicating among themselves, the chances of fraud increases dramatically. Card networks offer standardized processes for handling disputes between merchants and customers, ensuring a fair and efficient resolution process without distrubing the bank in the process.

2 The Card Payment Process

The flow of the payment process is shown in the following figure:



2.1 Customer Authenticates on Merchant Website

Before initiating the payment, the merchant website should know who is paying. That's why it first asks the customer to authenticate themselves. Authentication is the process of verifying the identity of a user, service, or system by validating the credentials provided. One can authenticate themselves on websites by one of the two ways:

- Using username and password
- Using account of the third-party service provider like Google, Facebook, GitHub, etc.

The first method is one of the most common forms of authentication, where the user provides a unique username (or email address) and a corresponding password. The merchant website then verifies these credentials against a database of authorized users. If the provided credentials match, the user is authenticated and granted access.

In the second method, instead of using their username and password, users authenticate with the service provider (e.g., Google, Facebook, GitHub) and authorize the third-party application to access specific resources on their behalf. This is also called as **OAuth2.0** authorization. It works through the following steps:

1. The user initiates the authentication flow by accessing the third-party application.
2. The application redirects the user to the service provider's authentication page.
3. The user authenticates with the service provider (e.g., Google) using their credentials.
4. The service provider asks the user to grant permission to the third-party application to access specific resources (e.g., email, contacts, profile information).
5. If the user grants permission, the service provider issues an access token to the third-party application.
6. The third-party application can then use the access token to access the authorized resources from the service provider on behalf of the user.

Sometimes you may require to provide **OTP** *(One Time Password)* as well even after authenticating yourself correctly. This is called **Two-Factor Authentication (2FA)**. Two-factor authentication is an additional layer of security that requires users to provide a second form of verification in addition to their username and password. This second factor can be something the user possesses (e.g., a hardware token or mobile device), something they know (e.g., a one-time code or personal identification number), or something they inherently are (e.g., a biometric like a fingerprint or facial recognition). 2FA provides an extra level of assurance that the user is who they claim to be, making it more difficult for unauthorized individuals to gain access, even if they have obtained the user's password.

Once the customer is authenticated, they provide their **card details** to the merchant website. The details include card number, CVV, expiry date, amount, currency, and other info like card holder's name and address. *But why are exactly these details asked?*

2.1.1 Card Number

Consider a fictional 16-digit card number: **4567 8901 2345 6775**.

It has four major parts.

1. **Major Industry Identifier (MII)**: The very first digit identifies the broad category of the issuing institution. For instance, '4' indicates Visa and '5' signifies Mastercard.
2. **Issuer Identification Number (IIN)**: The first six digits (including the MII) make up the IIN, also called the Bank Identification Number (BIN). This unique code identifies the specific bank that issued the card. Here, '4567 89' is assigned to the bank (let's call it "First National Bank").
3. **Individual Account Identification Number**: The next nine digits '01 2345 677' represent your unique account number within First National Bank.
4. **Check Digit**: The last digit isn't part of the account information. It's a mathematically derived check digit calculated using an algorithm called **Luhn Modulo 10**. This digit helps identify typos or errors in the card number during transactions. The last digit '5' is the check digit, calculated using the Luhn algorithm based on the previous 15 digits.

Here's how the Luhn's algorithm works:

- Starting from the rightmost digit (excluding the check digit), double the value of every second digit. If the result is greater than 9, subtract 9 from the result.
- Sum all the digits, including both the unchanged digits and the doubled digits (with adjustments if needed).
- The last 16th digit should be such that, when added to the sum should give a number which is divisible by 10.

Consider the 15 digits of the card: 4567 8901 2345 677.

- Doubling every second digit gives: (8)5(12)7 (16)9(0)1 (4)3(8)5 (12)7(14). We substract 9 from those which are two-digits. We get, (8)5(3)7 (7)9(0)1 (4)3(8)5 (3)7(5)
- Sum of all digits -> $8 + 5 + 3 + 7 + 7 + 9 + 0 + 1 + 4 + 3 + 8 + 5 + 3 + 7 + 5 = 75$
- The last digit must be '**5**', so that $75 + 5 = 80$, which is divisble by 10.

2.1.2 CVV

CVV or **Card Verification Value** adds an extra layer of security for online transactions. Unlike the card number, the CVV isn't printed on receipts or statements, so it's an indicator that the person placing the order has the physical card in hand.

Unlike your card number, the CVV isn't used for everyday transactions where you physically swipe your card. Its primary function is to add security for online purchases where the merchant doesn't have access to the physical card. By requesting the CVV during checkout, the merchant can verify that the person placing the order has the card and potentially reduce the risk of fraudulent transactions. Your CVV is a confidential code and should be treated with the same care as your PIN.

The CVV code is unique to your specific card and isn't directly linked to your card number. It's generated by a special algorithm considering your card details and expiry date. This makes it more difficult for someone to guess your CVV even if they have your card number. If your card gets lost or stolen, you'll receive a new card with a new CVV code. This adds another layer of security by rendering any stolen CVV codes useless.

2.1.3 Expiry Date

Expiry date ensures the card you're using is valid and hasn't expired. Expired cards can't be used for transactions. The actual reason by card network companies ask you to put the expiry date is twofold. Firstly, knowing the expiry date allows you to stay ahead and request a replacement card from your bank before the current one becomes invalid. Secondly, for the merchants, it reduces the risk of chargebacks that occur when a transaction is made on an expired card. Chargebacks can be a hassle for merchants, involving reversing the transaction and potentially incurring fees.

2.1.4 Amount

Amount tells the bank and the merchant exactly how much money needs to be transferred for your purchase.

2.1.5 Currency

Currency specifies the type of money you're paying with. It avoids any confusion if the merchant deals in multiple currencies.

2.1.6 Card Holder's Name

This verifies that the card being used matches the person making the purchase. It helps prevent unauthorized use of the card.

2.2 Merchant sends encrypted payment data to the Payment Gateway

Whatever data merchant has received from the customer, they have to transfer it to the payment gateway. It uses two levels of security here: **TLS/SSL** and **Tokenization**.

2.2.1 TLS/SSL

TLS/SSL stands for **Transport Layer Security/Secure Sockets Layer.** It creates a secure tunnel between the merchant's website and the payment gateway, encrypting the data in transit to prevent eavesdropping by unauthorized parties.

Of course, "tunnel" is a metaphor used to describe TLS/SSL in simpler terms. Here's a more technical explanation of what happens:

1. **Handshake** When you visit a website secured with TLS/SSL (indicated by a padlock symbol in the address bar), a handshake process establishes a secure connection.
    - The website (server) sends its public key certificate to your browser (client).
    - Your browser verifies the certificate's authenticity with a trusted Certificate Authority (CA).
    - The browser generates a secret session key and encrypts it with the server's public key, sending it back.
    - Only the server's private key can decrypt the session key, creating a shared secret for the connection.
2. **Encryption and Decryption**
    - All communication between the browser and the server is encrypted using the established session key. This means the data is scrambled into an unreadable format.
    - Only the browser and server, with their respective private keys, can decrypt the data and understand its content.
3. **Data Integrity**
    - TLS/SSL also ensures data integrity, meaning the information isn't altered during transmission. This is achieved using message authentication codes (MACs) that get attached to the data. Any tampering with the data would invalidate the MAC, alerting both parties.

Think of it like this:

- Imagine two people (*browser* and *server*) wanting to exchange confidential messages.
- TLS/SSL acts like a secure room with a locked door (*public key encryption*).
- Each person has a unique key (*private key*) that only opens their own lock.
- They share a secret message (*session key*) in the locked room ensuring only they can understand it.
- Additionally, a tamper-proof seal (*MAC*) is placed on the message to ensure it hasn't been altered.

2.2.2 Tokenization

Tokenization, in the context of online payments, refers to the process of replacing sensitive data, like a credit card number, with a unique identifier called a token. This token can be used to process the transaction without exposing the actual card number to the merchant or the payment gateway.

During an online purchase, when you enter your card details, they are sent to the payment gateway. The payment gateway doesn't store your actual card number. Instead, it interacts with a tokenization service (often provided by the card network or a third-party provider). The tokenization service creates a unique token that acts as a substitute for your card number. This token can be alphanumeric or a combination of letters and numbers, with no inherent value on its own. The tokenization service securely stores the mapping between the token and the actual card number. Tokenization is helpful because:

- **Enhanced Security:** By replacing card numbers with tokens, tokenization significantly reduces the risk of data breaches. Even if a hacker gains access to the merchant's or payment gateway's systems, they wouldn't be able to use the stolen tokens for fraudulent purchases.
- **Improved Convenience:** Once a card is tokenized, you don't need to re-enter your entire card number for subsequent purchases from the same merchant (if they offer token storage). This creates a smoother and faster checkout experience.

2.3 Payment Gateway sends authorization request to the Issuing Bank

Payment gateway sends authorization request to the issuing bank via secure financial messaging channel. Secure financial messaging refers to specialized protocols and technologies used to transmit sensitive financial information between banks and other financial institutions. These protocols ensure the confidentiality, integrity, and authenticity of the data during communication. It uses the following two standards:

- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS):** As explained earlier, TLS/SSL creates a secure tunnel for encrypted data exchange.
- **ISO 8583:** An international standard message format specifically designed for financial transactions. It defines the structure and content of messages exchanged between banks.

The issuing bank then decrypts the message received from the payment gateway and gets the data sent by the merchant website. On that data, it performs several fraud mitigation checks. These checks include:

- **Card Validity:** Verifies if the card number is valid and hasn't been reported lost or stolen. This check helps prevent unauthorized use of stolen cards. If this check fails, a fraudster who finds a lost or stolen card could potentially use it for unauthorized purchases.
- **Sufficient Balance:** Ensures the cardholder's account has enough funds to cover the transaction amount. This prevents fraudulent purchases exceeding the available balance. Skipping this check could allow a fraudster to exploit a compromised card and make large, unauthorized purchases before the cardholder notices.
- **Fraud Rules:** Issuing banks develop rules based on historical fraud patterns. These rules consider factors like transaction location, time, type of merchant, and purchase amount. A transaction violating multiple rules might be flagged for further investigation. Without fraud rules, a series of small, unusual purchases from a different country might go unnoticed, allowing a fraudster to gradually drain the account.
- **Velocity Checks:** Analyze the frequency and volume of transactions. Sudden spikes in purchase activity, especially from geographically unusual locations, could indicate suspicious behavior. An attacker might steal card details and use them to make a rapid sequence of small purchases online, potentially going unnoticed without velocity checks.

- **Address Verification (AVS):** Compares the cardholder's billing address provided during checkout with the address on file at the issuing bank. This helps identify potential misuse of stolen cards. If AVS is bypassed, a fraudster could use a stolen card number and a fake billing address to complete a purchase.
- **3D Secure (3DS):** An authentication protocol that adds an extra layer of security for online transactions. It requires cardholders to verify their identity with a password or one-time code before the transaction is authorized. Omitting 3D Secure makes online transactions more vulnerable to unauthorized use, especially if the card details are stolen through phishing attacks.

The issuing bank employs various techniques to assess and manage the overall risk of a transaction. These techniques include:

- **Machine Learning Models:** Advanced algorithms analyze historical transaction data and identify patterns associated with fraudulent behavior. This allows for dynamic risk scoring and real-time fraud detection. Machine learning models can identify unusual spending patterns for a specific cardholder, flagging suspicious activity that might be missed by static rules.
- **Rules Engines:** Automated systems apply pre-defined rules based on various factors like transaction amount, location, merchant category, and cardholder behavior. Transactions exceeding risk thresholds might be flagged for review. A rule engine could automatically decline transactions exceeding a certain amount for a specific card type, preventing large-scale fraudulent purchases.
- **Transaction Scoring:** Assigns a risk score to each transaction based on various checks and risk factors. Transactions with high scores might be declined or require additional verification. Transaction scoring helps prioritize fraud review, allowing investigators to focus on high-risk transactions first.

These techniques work together to create a multi-layered defense against fraud. By combining traditional checks with advanced analytics, issuing banks can significantly reduce the risk of fraudulent transactions and protect their cardholders.

2.4 Issuing Bank sends authorization response to the Card Network

After performing various checks and fraud mitigation (as explained previously), the issuing bank makes a decision:

- **Authorization Approved:** If all checks pass and the transaction seems legitimate, the issuing bank sends an authorization response indicating approval. This response might include additional details like an authorization code.
- **Authorization Declined:** If any check fails, or the issuing bank suspects fraud, it sends a decline response with a reason code explaining the denial.

2.5 Card Network routes this authorization response to the Acquiring Bank

The issuing bank typically doesn't have a direct connection to the acquiring bank that processes the transaction for the merchant. The card network acts as an intermediary, receiving the authorization response from the issuing bank. Based on the issuing bank's response (approved or declined) and the specific network rules, the card network routes the authorization response to the acquiring bank.

2.6 Acquiring Bank relays this response to Payment Gateway

After receiving the authorization response from the issuing bank (whether approved or declined), the acquiring bank acts as a messenger. It relays this information back to the payment gateway (PG) that initially sent the authorization request. The acquiring bank doesn't make the authorization decision itself. Its role is to facilitate the communication between the merchant and the issuing bank. By relaying the response, the acquiring bank ensures the PG receives the latest update on the transaction status.

2.7 Payment Gateway transmits payment status to Merchant Website

Upon receiving the authorization response from the acquiring bank, the payment gateway now has the final verdict from the issuing bank. The PG translates this response into a user-friendly format (e.g., "Transaction approved" or "Transaction declined") and transmits it back to the merchant website (MW). The merchant website is the point of interaction for the customer. They are waiting to know whether their purchase has been successful. The PG acts as the intermediary, informing the merchant website of the authorization status so they can update the customer's order status and display an appropriate message (e.g., "Payment successful, your order is confirmed" or "Payment declined, please try again").

This flow of information ensures both the customer and the merchant receive timely updates on the transaction status. In case of any delays or errors during communication, the customer might experience a lag in receiving the final outcome, leading to a less than ideal shopping experience. This specific authorization flow doesn't involve the transfer of funds yet. The actual settlement (transfer of funds) happens later as a separate process.

2.8 Actual Funds Transfer

Once the issuing bank approves the transaction, it initiates the settlement process. This involves transferring the authorized funds from the cardholder's account to the acquiring bank that represents the merchant. Similar to the authorization request, the settlement message is sent via secure financial messaging protocols like ISO 8583 or dedicated settlement networks. The message typically includes details like: transaction amount, merchant identifier, cardholder information (masked) and transaction reference number.

The acquiring bank receives the settlement message from the issuing bank. Settlements may not happen in real-time for all transactions. Acquiring banks might accumulate authorized transactions over a period and process them in batches for efficiency. Reconciliation involves verifying that the total amount received from the issuing bank matches the total authorized transaction amounts for the corresponding batch. Any discrepancies are investigated and resolved.

Once the settlement process is complete, the acquiring bank credits the merchant's account with the authorized funds, minus any processing fees they might charge.

2.9 Merchant and Customer Notification

The acquiring bank informs the merchant website about the successful completion of the settlement process, indicating that the funds are now available. Based on the settlement notification and any internal policies, the merchant website can finalize the purchase for the customer (e.g., ship the product, deliver the service) or decline it if there are any unforeseen issues. The merchant website updates the customer about the purchase status (completed or declined) based on the settlement outcome.

3 Conclusion

The next time you buy that must-have gadget online or treat yourself to a takeout dinner, remember – there's a whole team working behind the scenes to make sure your purchase goes through safely. This intricate process might seem invisible, but it's what keeps your hard-earned cash secure. As technology continues to race forward, you can rest assured that these payment systems are constantly evolving to stay ahead of the game, ensuring a smooth and secure experience for every swipe, tap, or click!
