3-D Secure

This guide covers the following:

- 3-D Secure Overview
- 3-D Secure 2
- Out-of-Scope Transactions and SCA Exemptions
- Chargeback Liability Shift
- Rules for MITs
- Use Cases
- Enable and Configure 3-D Secure
- 3-D Secure Integrations
- Test 3-D Secure

3-D Secure Overview

Terminology

- 3-D Secure (3DS) — an advanced authentication solution
- 3-D Secure 2 (3DS 2) — the new global specification for 3DS
- CIT — Customer-Initiated Transaction
- MIT — Merchant-Initiated Transaction
- MOTO — Mail Order and Telephone Order transaction
- PSD2 — Revised Payment Services Directive
  (For more information, refer to our 3-D Secure 2 FAQs page.)
- SCA — Strong Customer Authentication
  (For more information, refer to our 3-D Secure 2 FAQs page.)
- TRA — Transaction Risk Analysis

What is 3-D Secure?

3-D Secure is an advanced authentication solution implemented to reduce eCommerce fraud by verifying a cardholder's identity in real time. Each of the major card brands has a 3-D Secure offering:

- American Express Safekey®
- Discover ProtectBuy® (covers Discover and Diners Club)
- Mastercard SecureCode®
- Visa Secure®

This additional layer of security helps prevent unauthorized use of cards and protects eCommerce merchants and issuers from exposure to fraud.

Supported Cards
Supported Countries
Supported Currencies
Supported Languages
Testing Your Integration

Back to Top

3-D Secure 2

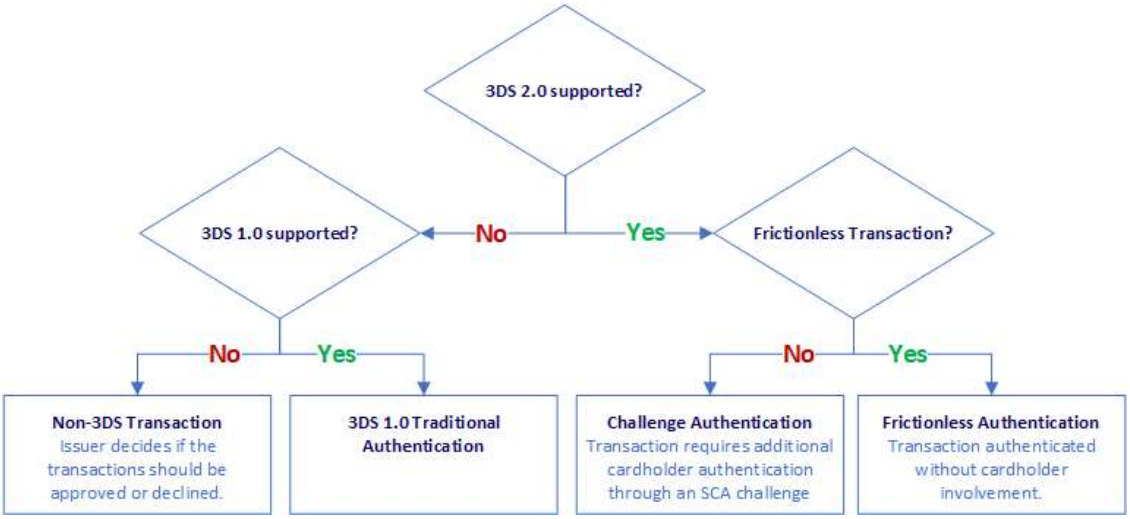
What is 3-D Secure 2?

3-D Secure 2 (3DS 2) is the new global specification for card payment security developed by EMVCo. It is designed to deliver frictionless payment authentication across a range of devices, including mobile devices. Unlike previous versions of 3DS, it allows for more seamless integration with merchants' e-commerce customer experiences. 3DS 2 is being deployed across Europe. For details on the implementation date click here.

The use of 3-D Secure 2 satisfies the PSD2 requirement for SCA.

- For specific details on the 3-D Secure 2 specification, refer to the specification.
- For answers to questions related to BlueSnap and 3-D Secure 2, PSD2, and SCA, refer to our 3-D Secure 2 FAQs page.
- For specific use cases regarding how 3-D Secure 2, PSD2, and SCA are implemented at BlueSnap, refer to the Use Cases.

3-D Secure 2 Authentication Flow and Fallback Workflow



Back to Top

Out-of-Scope Transactions and SCA Exemptions

The intent of PSD2 is to make SCA a requirement for all online transactions; however, there are some transactions that are considered out of scope and there are some exemptions.

Out-of-Scope Transactions

Anonymous Transactions

Transactions through anonymous payment instruments are not subject to the SCA mandate, for example anonymous prepaid cards.

Inter-regional Transactions

Inter-regional Transactions are usually exempt. An Inter-regional Transactions is one in which the issuer or the acquirer of the card is not based in the EEA (European Economic Area). For example, accepting payments in Europe from non-European shoppers is not in the scope of PSD2.

Merchant-Initiated Transaction (MIT)

Most subscription or recurring transactions with a fixed amount (same amount each time) are exempt after the initial transaction; only the initial transaction requires SCA.

Some subscriptions have a variable charge based on usage. These types of transactions are usually considered *merchant-initiated transactions*. These are exempt from PSD2 and SCA requirements.

Payments made with a card on file when the customer is not present in the checkout flow may qualify as *merchant-initiated transactions*. These payments fall outside the scope of SCA but ultimately the issuing bank must decide if SCA is needed for the transaction.

BlueSnap will work with merchants to apply this out-of-scope exemption for applicable transactions.

> 👍 **API**
>
> In the API, MIT transactions are indicated using: `"transactionInitiator":"MERCHANT"` . For more information, refer to these examples.

Mail Order and Telephone Orders (MOTO) Transaction

MOTO transactions are exempt from SCA in all cases. The MOTO transactions are not considered to be "electronic" payments, so are out of the scope of the regulation.

BlueSnap works with merchants to apply this out-of-scope exemption for applicable transactions.

> 👍 **API**
>
> In the API, MOTO transactions are indicated using `"transactionOrderSource":"MOTO"` . For more information, refer here.

SCA Exemptions

Low Value Transactions

Transactions under 30 EUR are exempt from SCA. The issuing bank must track the amount of each payment made. If the total amount attempted on a single card without SCA is greater than 100 EUR, or for every 5 transactions on a single card, SCA is required.

BlueSnap automatically applies this exemption for applicable transactions.

Transaction Risk Analysis (TRA)

The TRA exemption allows for certain remote transactions to be exempted from SCA provided a robust risk analysis is performed.

BlueSnap automatically applies this exemption for applicable transactions.

Trusted Beneficiaries

Customers can assign merchants to a list of *Trusted Beneficiaries* that is maintained by their bank. These trusted merchants are exempt from PSD2 for SCA. This allows customers who regularly shop with a business to shop without providing SCA after the business is added to the list.

Payee-Initiated

Payee-initiated transactions are exempt. A payee-initiated transaction occurs when the payer's consent for a direct debit transaction is given in the form of an electronic mandate with the involvement of its PSP. For example, SEPA is a payee-initiated transaction.

Secure Corporate Payments

Payments made through dedicated corporate processes and protocols (for example, lodge cards, central travel accounts, and virtual cards) that are initiated by business entities, are not available to consumers, and that already offer high levels of protection from fraud may be exempt from SCA.

Back to Top

Chargeback Liability Shift

In addition to preventing unauthorized card use, 3DS can shift liability for fraud chargebacks from the merchant to the card issuer in these situations:

- **Situation 1:** Shopper successfully verifies their identity, passing SCA authentication.
- **Situation 2:** An issuer who perceives the transaction to be low risk authenticates without requiring SCA from the shopper.
  In Situation 2, the shopper never sees a pop-up window requesting SCA during checkout, making the 3DS-flow entirely transparent to them.

Note: In order for a liability shift to occur, the region where the authentication takes place must support 3DS liability shifts. The following table outlines this support.

Region	Support date
Canada, Latin America, and the Caribbean	August 15, 2019
Asia Pacific, Central Europe, Middle East, and Africa	April 15, 2020
Rest of Europe	March 1, 2020
United States	August 15, 2020

Fraud Liability Summary

Transaction Type	SCA Required?	Issuer Challenged	Fraud Liability
CIT	Yes	Yes	Issuer
CIT	Yes	No	Issuer
CIT	No; Low Value Exemption	No	Issuer
CIT	No; Transaction Risk Analysis (TRA) Exemption	No	Merchant

Transaction Type	SCA Required?	Issuer Challenged	Fraud Liability
CIT	No; Secure Corporate Payment Exemption	No	Issuer
CIT	No; White Listing Exemption	No	Issuer
CIT	No; Inter-regional Exemption	No	Merchant
MOTO	No	No	Merchant
MIT	No	No	Merchant

> 📘 **Chargebacks may still occur**
>
> You may still receive fraud chargebacks for transactions authenticated using 3DS. However, these chargebacks are considered invalid. If you receive a chargeback on an authenticated 3DS transaction you should dispute the chargeback through BlueSnap's chargeback management services.

Back to Top

Rules for MITs

1. Merchants must store the Network Transaction ID of the CIT that established the agreement, for future MITs.
2. An MIT can only occur ***after*** an initial CIT has been performed to establish a customer agreement.
3. MITs must be properly indicated as MITs to ensure they are treated as out of scope of SCA.
4. Merchants should only request MIT authorization when the goods are available and ready to be shipped.
5. "*Grandfathering*" can be applied to an MIT if the transaction is performed based on an agreement made prior to the implementation of PSD2. Refer to the Use Cases for details.
6. When setting up an agreement to process future MITs, the merchant can only authenticate and authorize for the amount needed on the day the agreement is signed. Authorizing any additional amount unnecessarily only impacts the cardholder's "open to buy" limit.

Back to Top

Use Cases

MIT, MOTO, and CIT examples

MIT and MOTO are out-of-scope transactions. When properly flagged, these transactions should not require SCA by issuers.

Use Case 1: Create a new subscription and then submit on-going subscription payments as MITs

You must perform the following 3 steps to establish a customer/merchant agreement and to submit the initial and recurring subscription charges.

1. The merchant authenticates the shopper for the amount due immediately.
2. After the cardholder is successfully authenticated, merchant authorizes for the amount due that day. If no amount is due that day, the merchant should perform a zero-amount authorization. The merchant obtains and stores the initial transaction ID, known as the Network Transaction ID, for future MITs.
3. When the next payment is due, the merchant initiates the payment as an MIT by sending the auth-capture request with the Network Transaction ID and flagging it as an MIT. (In the API, this is done using: `"transactionInitiator":"MERCHANT"`. For more information, refer to these examples.)

Use Case 2: Cardholder calls in to establish stored credentials for future MITs

Sometimes a cardholder establishes an agreement with a merchant over the phone, by mail, or email. In those cases, the initial transaction is MOTO transaction. All subsequent transactions made under that agreement should **not** be flagged as MOTO; they are MITs unless they too are made by phone, by mail, or email. The detailed steps are:

1. The cardholder provides the card information by phone, email, or mail order.
2. The merchant sends MOTO transaction authorization with the amount (or zero-amount); no SCA is required. (In the API, this is done using `"transactionOrderSource:MOTO"`. For more information, refer here.)
3. The merchant obtains and stores the Network Transaction ID from step 2 for future MITs.
4. The merchant initiates an MIT for subsequent payments, the merchant sends the MIT flag and the Network Transaction ID in the authorization request to issuer. (The Network Transaction ID links the MIT to the initial MOTO transaction.)

Use Case 3: Cardholder calls in to establish stored credentials for future MOTO and CIT

1. The cardholder provides the stored credentials via MOTO and the merchant saves the card on file. No SCA is required for the MOTO transaction.
2. The cardholder comes back again to make a purchase using the stored credentials; the transaction must be flagged correctly based on the channel:

- If the cardholder makes a purchase by phone, mail, or email, the transaction should be flagged as MOTO and no SCA is required. The merchant directly sends the transaction as a MOTO authorization request. (In the API, MOTO transactions are indicated using `"transactionOrderSource:MOTO"`. For more information, refer here.)
- If the cardholder makes a purchase through the merchant's website, the transaction should be flagged as an ecommerce transaction and requires SCA.

Note: The SCA requirement for a transaction with stored credentials is determined by **how the transaction is processed** *not* by how the stored credentials were initially established.

- MITs and MOTO transactions are out of scope for PSD2.
- CITs usually require SCA.

Use Case 4: Use of Network Transaction ID in subscription and various MITs and how to use *Grandfathering* to process MITs performed based on agreements made prior to the implementation of PSD2.

The Network Transaction ID is a data field returned either during account verification or the initial CIT related to subsequent MITs. When included in future MIT authorization requests, the Network Transaction ID lets the issuer know that the MIT is a subsequent payment for a subscription and is related to the initial CIT.

A merchant using their own subscription management engine must store the Network Transaction ID on their end for Visa and MasterCard transactions. The Network Transaction ID should be included in all future MITs for Mastercard and Visa transactions. American Express transactions do not require the Network Transaction ID; merchants can flag the subsequent MITs as a recurring transaction.

The merchant and cardholder have an existing agreement established prior to the implementation of PSD2. The merchant does not need to re-establish a new agreement with their customer.

- For merchants not using BlueSnap's subscription functionality:
  - If you do not have a Network Transaction ID (NTI), pass the parameter "transactionInitiator":"MERCHANT" in the API request.
  - If you receive a Network Transaction ID (NTI) from us, save the NTI and pass it to us for all subsequent MIT transactions.
- For American Express, the merchant must flag the transaction as MIT.

(To flag a transaction as MIT in the API, use `"transactionInitiator":"MERCHANT"`. For more information, refer to these examples.)

Use Case 5: Renew a subscription after it expires

- If the new subscription uses the same stored card and the same address, the merchant can use the old Network Transaction ID and continue flagging subsequent transactions as MIT.
- If the new subscription uses a new card or a new address, the merchant must put the cardholder through SCA.

Use Case 6: Submit an order using MOTO or a merchant-managed virtual terminal

This is a MOTO transaction and needs to be flagged as a MOTO transaction; no SCA is required. For subsequent transactions, the merchant flags the order as MIT with the Network Transaction ID obtained from the original MOTO transaction.

> 👍 **In the API**
>
> MOTO transactions are indicated using `"transactionOrderSource:MOTO"`. For more information, refer here.
>
> MIT transactions are indicated using: `"transactionInitiator":"MERCHANT"`. For more information, refer to these examples.

Use Case 7: Customer agreement changes

Sometimes, a merchant or customer may need to change the payment terms of the ongoing agreement. SCA is always recommended in those situations; however, the merchant may opt not to authenticate if certain conditions apply:

- For merchant-driven changes to payment terms, SCA is not required provided that the original agreement terms and
  conditions and other cardholder communications clearly covered the eventuality of such changes.
- For customer-driven changes, if the customer requests a change to pricing and terms, pauses an agreement, or stops and restarts an agreement, SCA is not required provided that the agreement terms and conditions clearly covered the eventuality of such changes **and** the merchant has the necessary risk management in place.

Use Case 8: Cardholder changes the delivery address

If a cardholder goes into their merchant account and updates the delivery address for an order, SCA is not required by regulation. However, it is recommended that SCA be performed if the customer changes the delivery address linked to an in-process order as this represents a risk of fraud.

Use Case 9: Payment credentials updated by account updater

The merchant received updated payment credentials from the Issuer. SCA is not required; however, under Visa rules this must be addressed through terms and conditions and other cardholder communications.

Use Case 10: Creating a vaulted shopper and then creating recurring transactions on this returning shopper

1. The cardholder provides the credentials to be stored and the merchant authenticates the shopper. This is true whether the initial transaction is for $0 (to simply vault the shopper) or for a purchase. SCA is required for this CIT transaction.
2. The cardholder comes back again to make a purchase using the stored credentials; the transaction must be flagged correctly based on the channel:

- If the cardholder makes a purchase by phone, mail, or email, the transaction should be flagged as MOTO and no SCA is required. The merchant directly sends the transaction as a MOTO authorization request. (In the API, MOTO transactions are indicated using `"transactionOrderSource:MOTO"`. For more information, refer here.)
- If the cardholder makes a purchase through the merchant's website, the transaction should be flagged as an ecommerce transaction and requires SCA.

Note: The SCA requirement for a transaction with stored credentials is determined by **how the transaction is processed** *not* by how the stored credentials were initially established.

- MITs and MOTO transactions are out of scope for PSD2.
- CITs usually require SCA.

Back to Top

Enable and Configure 3-D Secure

To get started, contact Merchant Support to request that BlueSnap enable 3DS for your account. After it has been enabled, you can activate and configure it in 3-D Secure settings below.

3-D Secure settings

In your BlueSnap Console to the **3D Secure Rules** section under **Settings > Fraud Settings**.

Enable 3-D Secure

After 3-D Secure has been enabled for your account, activate it by selecting this option.

> 📘 **Important**
>
> Enabling 3-D Secure on your account initiates an authentication request to the issuer for every customers regardless of where they are located. The **issuing bank** must decide if SCA is needed for the transaction.
>
> - If the issuer requires authentication, then the shopper is presented with an SCA challenge.
> - If issuer does not require authentication, then the shopper experiences the same flow as if 3-D Secure is not enabled.

Process failed 3DS transactions

If this option is enabled, if a transaction fails 3-D Secure authentication, it is still processed.

> ❗ **Use Caution when enabling this option**

Exclude countries for 3DS

This lets you include and exclude specific countries 3-D Secure verification. Select the countries from either list and click the arrow to move them to the other list. You can select a single country, multiple countries, or all countries. When a country is in the Exclude list, transactions from that country do not go through the 3-D Secure authentication process.

3-D Secure Integrations

Payment API

BlueSnap's Payment API provides built-in support for 3-D Secure. Complete implementation details are available in this 3-D Secure API Guide.

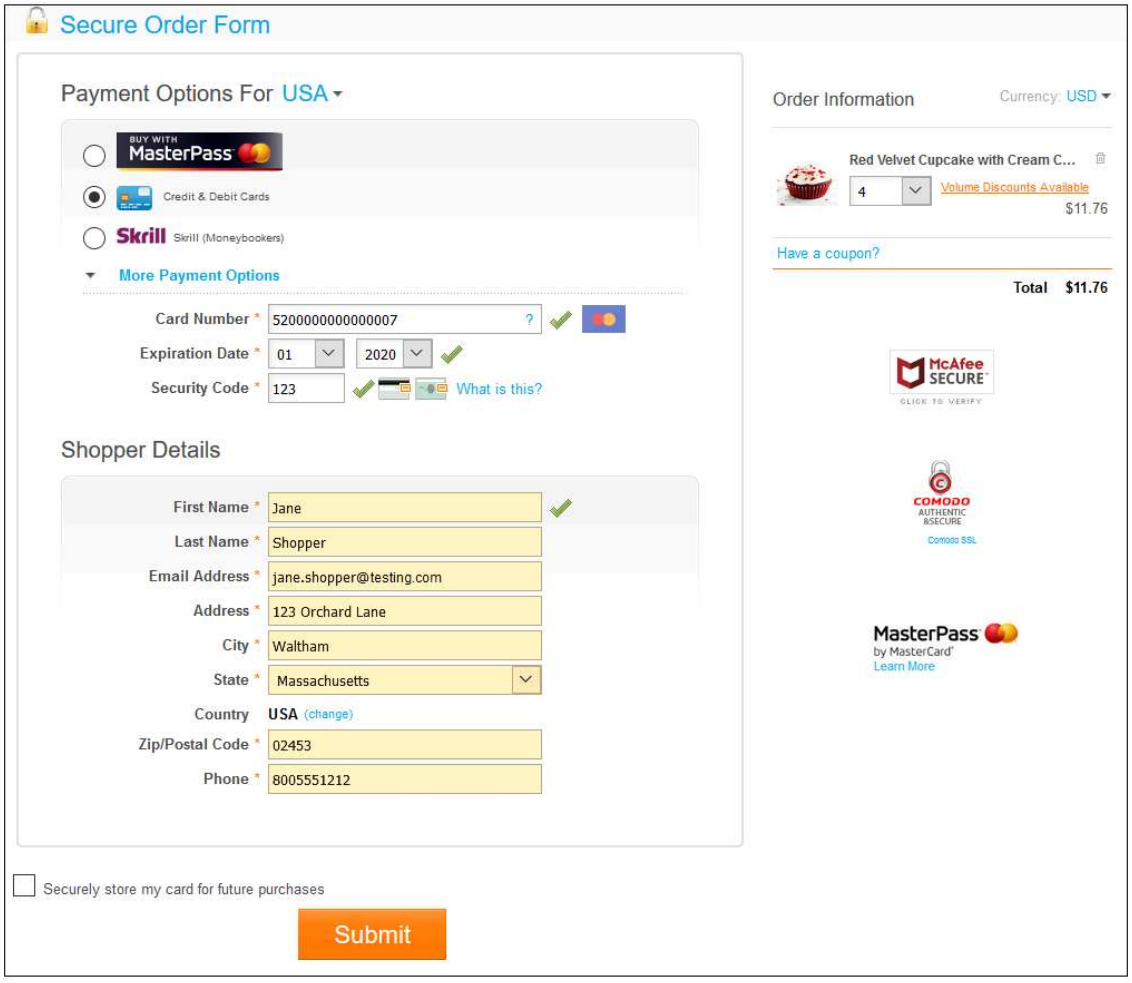
Hosted Pages

BlueSnap's Hosted Pages provide out-of-the-box support for 3-D Secure. Simply ensure that 3-D Secure is enabled.

The shopper experience

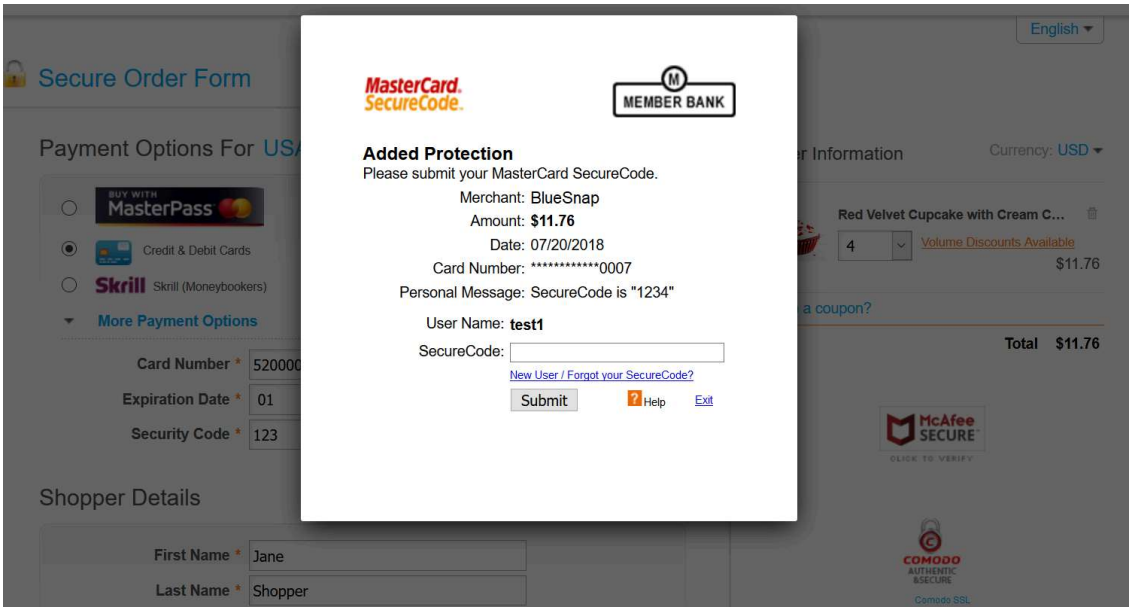
The following steps outline the general 3-D Secure flow with images taken from a BlueSnap Hosted Page.

Step 1: Shopper enters card information and submits payment form

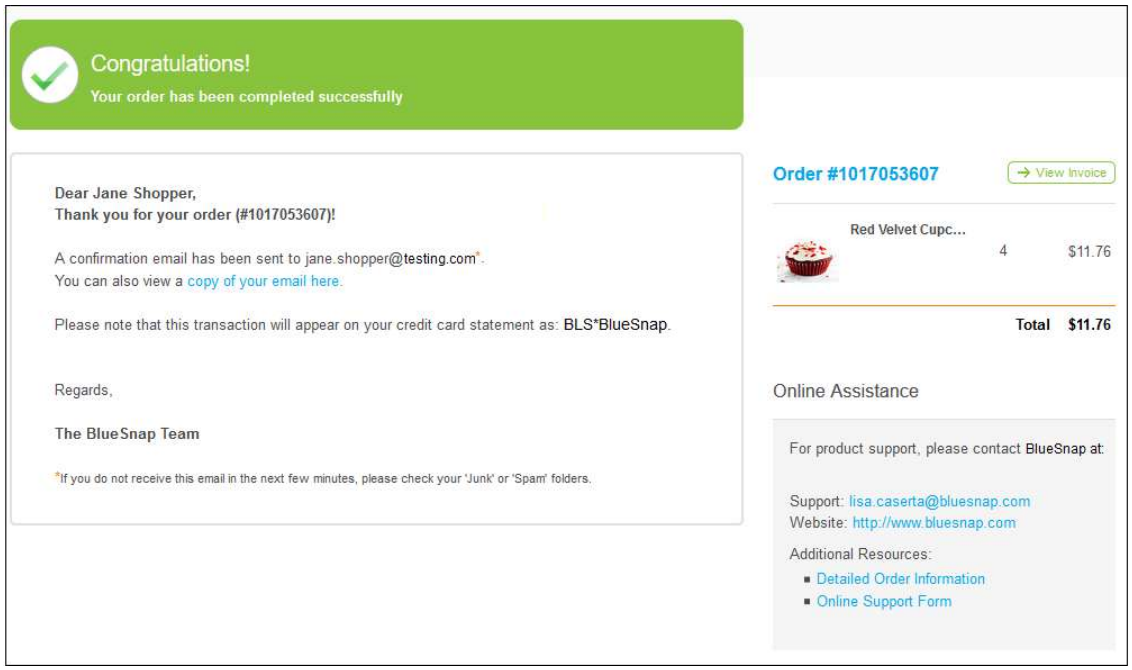


Step 2: If shopper verification is required, a popup prompts the shopper to enter a password

A lookup is performed during checkout to determine if the issuer requires identity verification from the shopper. If required, a popup like the one below prompts the shopper to enter a password, which is typically a one-time code sent via text message.



Step 3: Confirmation page opens



Embedded Checkout

If you are using BlueSnap's Embedded Checkout, you don't need to do any coding. BlueSnap processes these transactions using the same 3-D Secure flow.

Virtual Terminal

- If you are using BlueSnap's Virtual Terminal, you don't need to do any coding. BlueSnap processes these transactions as MOTO and identifies the out-of-scope transactions for you, and therefore do not need to do any coding.
- If you are using your own self-developed virtual terminal, when you submit the transactions to BlueSnap, these transactions need to be flagged as MOTO, so we can submit the authorization request as MOTO to processors, and the transactions do not require SCA.

Subscriptions

- If you are using the BlueSnap Subscription Engine or our merchant-managed subscription feature, BlueSnap manages all subscription transactions. You do not need to do any

coding, BlueSnap handles the exemptions and the out-of-scope transactions for you.

- If you handle your own **subscriptions** (that is, you are sending straight auth-capture requests ***not*** using the BlueSnap Subscription Engine or our merchant-managed subscription feature), follow the information in the Use Cases for details on how to continue your existing subscriptions.

Back to Top

Test 3-D Secure 2

You can test 3-D Secure 2 using our test page. This button opens a new tab with a checkout page to test 3-D Secure 2. Use any of the cards numbers below to test various 3-D Secure 2 results.

Test 3DS Transactions

> ❗ **Test Cards**
>
> The following cards are only valid on a system with 3DS 2 enabled. The test system (accessed through the button above) does have 3DS 2 enabled.
>
> - If you want to use these cards on your system, you need to have 3DS 2 enabled. To have 3DS 2 enabled on your system, contact an Implementation Specialist.
> - If these cards do not work, try the 3DS 1.0 cards listed here.

Visa	Mastercard	Authentication Result
4000000000001091	5200000000001096	Successful with challenge
4000000000001000	5200000000001005	Successful without challenge
4000000000001109	5200000000001104	Failed with challenge
4000000000001018	5200000000001013	Failed without challenge
4000000000001059	5200000000001054	Unavailable

> 👍 **Card Data**
>
> - **Expiration Date**
> - The expiration **month** is always January.
> - The expiration **year** is the current year plus 3 years.
> For example: In 2019, the Expiration Date value is 01/2022.
> - **Security Code** (CVV): any 3-digit code
> - **Challenge**: If challenged
> - The user name (**test1**) is prefilled.
> - The password is `1234`

Back to Top

Updated 13 days ago