



infobip

**Be PSD2 Compliant:
2FA for Strong
Customer Authentication**

TABLE OF CONTENTS

1. What You Need to Know About PSD2	3
How will PSD2 impact your business?	4
2. What Do You Need to Become PSD2 Compliant?	5
Two-factor authentication (2FA) - deliver OTPs to authenticate customers	5
Why you need 2FA	6
PSD2 won't impact revenue	7
Client success story	8
3. The Infobip Advantage	9
Users can choose the 2FA channels they prefer	9
Generate your own OTPs and deliver with Infobip	9
How our 2FA works	10
4. How to Setup 2FA	11
2FA setup for OTPs generated by Infobip	11
Application Setup	11
Message Template Setup	11
Send and verify OTPs	12
Send OTP	12
Verify OTP	12
Integrating Infobip 2FA	12

Summary

The EU Payment Services Directive (PSD2) is here and it's changing the online payments environment in the European Union (EU). This whitepaper covers what PSD2 means for businesses, and how you can make your business compliant. You will also discover how we provide two-factor authentication (2FA), and how you can build a system that complies with Strong Customer Authentication (SCA) requirements. We'll share an example of how a fintech startup used 2FA to grow, and outline how you can integrate with us to achieve similar success.

1. What You Need to Know About PSD2

PSD2 introduces new laws aimed at improving innovation, reinforcing consumer protection, and enhancing the security of online payments and account access in the EU. PSD2 is a continuation of the original Payment Services Directive (PSD), adopted by the EU in 2007, which established a single EU market for payments. The directive from 2007 helped make cross-border payments between EU member states as convenient and secure as transactions in a member state.

PSD2 expands on the existing legislation by allowing bank customers to grant third-parties access to retrieve information from their bank accounts in order to initiate payments directly from their accounts. For security reasons, this will require SCA.

SCA is a PSD2 requirement that, among others, ensures electronic payments are performed with multifactor authentication to increase security. This requirement takes effect on **September 14th, 2019.**

Making systems compliant with PSD2 directives requires investment – and not meeting PSD2 requirements means that your business may not be able to process transactions on the EU common market. So, how serious is this? According to a survey by the open banking platform, [Tink](#), 41% of banks missed the March 14th deadline to provide testing environments for third-party service providers.

41%

of banks missed the March 14th deadline to provide testing environments for third-party service providers.

How much is this worth?

[57 billion transactions](#) worth €44 trillion were processed by retail payment systems in the EU in 2017.

How will PSD2 impact your business?

Once the SCA requirement takes effect on September 14th, online payments and checkout processes will need to meet at least two of the following criteria in order to accept payments:

At least two of the following criteria need to be followed



Ask for a password or OTP
something the customer knows



Require a mobile phone
something the customer has



Use a fingerprint or facial recognition
something the customer is

2. What Do You Need to Become PSD2 Compliant?

Two-factor authentication (2FA) - deliver OTPs to authenticate customers

Two-Factor Authentication (2FA) combines two of the required elements outlined by SCA: something the customer knows and something the customer has. Specifically, a **one-time PIN (OTP)** and a **mobile phone**.

SCA requires a clear link between authentication and financial events. This means customers authorizing payments need to be able to clearly identify how much they are paying, and who they are making that payment to. This is not possible with offline authentication models, like tokens.

The simplest way of providing 2FA is over SMS. Text messages can be delivered to any type of phone wherever your customer may be. In addition to this, SMS is easy to integrate and easy to scale. The message content can contain the information required to comply with PSD2 dynamic linking of financial and authentication events, as well, so that customers know what they're authorizing. 2FA channels are:



There have been concerns about the security of SMS as an authentication channel. However, the US-based [National Institute of Standards and Technology](#) reversed its recommendation to not use SMS as a 2FA channel in 2017. **SMS is now a compliant out-of-band authenticator.**

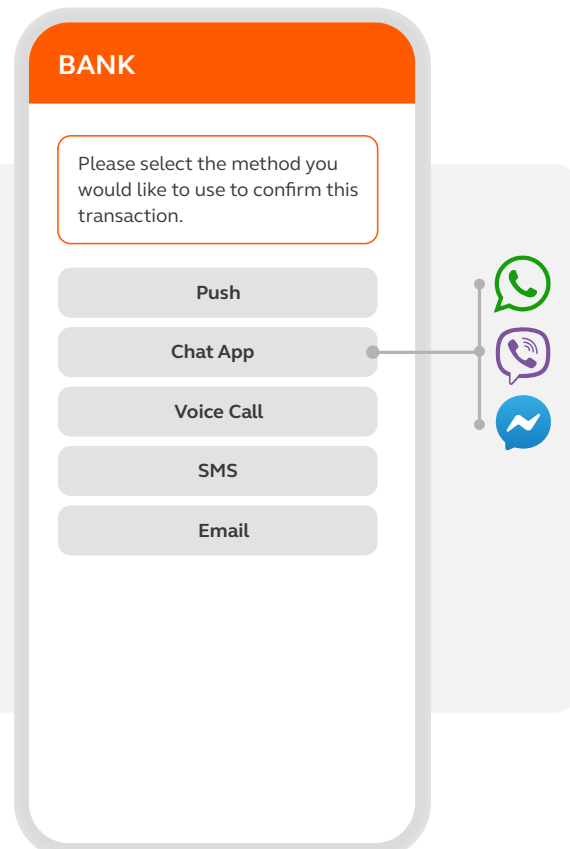
[Calls](#) are another option for providing 2FA over a more traditional channel that can reach customers on all devices, wherever they may be in the world with the highest delivery rate. This channel can contain all the required information about the transaction to comply with PSD2.

Transactions or logins can also be authorized within an app using push for authentication. This works by sending the app user a [push notification](#) that prompts them to either confirm or reject the action – a transaction or login.

Using push to authorize transactions offers several benefits. One of the main benefits is providing customers the ability to approve or deny authorization for transactions in real time, without having to manually enter a PIN. Security is also improved, since the flow used for push authentication involves only the business, 2FA provider and customer - minimizing the potential of man-in-the-middle attacks.

2FA is best offered over the channel customers prefer –

and you can give them the option to choose which authentication channel best meets their needs. Doing this makes authentication more convenient for customers, which should help improve conversion rates.



Why you need 2FA

Having measures in place to protect customers from online fraud is important to any business operating in the digital economy. This protects your customers and their data, as well as your business. In the UK, [four in ten](#) businesses suffered at least one cyber attack in the 12 months preceding April 2018. Breaches like this cost EU customers €1.44 billion in 2012, according to [Europol](#).



In the UK, [four in ten](#) businesses suffered at least one **cyber attack** in the 12 months preceding April 2018.

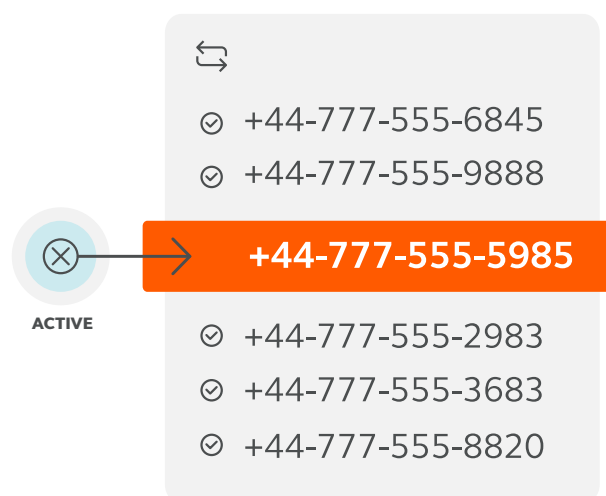
In addition to this, if your business provides online transactions in the EU, then you need to comply with PSD2 regulations for strong customer authentication. **This means that all online transactions in the EU worth €30 EUR or higher will have to be authorized by customers as of September 14th 2019.** Transactions that are not compliant with SCA will be rejected by payment service providers.

PSD2 won't impact revenue

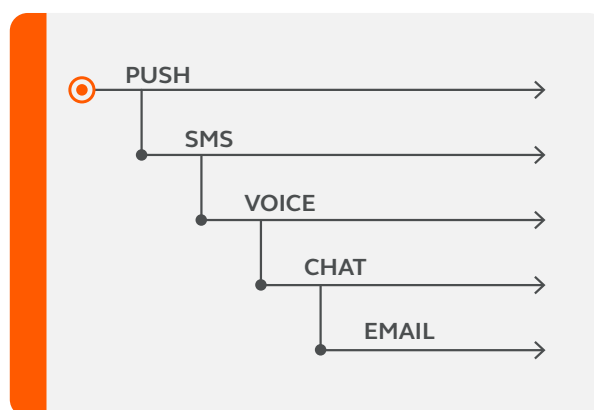
The requirements PSD2 introduces for authenticating transactions has businesses worried about a potential drop in revenue. The concern is that authentication slows down the process, making otherwise convenient electronic transactions more drawn out. For this reason, authentication needs to be quick and reliable, no matter the channel.

This is achieved by first validating the customer's phone number. Infobip can help you do this by performing a **Number Lookup**, to check the status of the customer's number against operator databases in real-time. This helps to optimize costs by choosing the appropriate channel.

An example is if a customer is travelling abroad without mobile data allowance, in which case 2FA over SMS may be the fastest and most efficient way of reaching that customer.



If a customer is unavailable over a particular channel, like in the example above, **Infobip provides failover channels to ensure delivery of OTPs for 2FA**. These channels can be set according to custom rules, so that if a customer fails to authenticate within a set amount of time, an OTP can be delivered over one or several subsequent channels.



For an added layer of security, authentication can be boosted using Mobile Identity, which seamlessly authenticates customers in the back-end. To find out more about Mobile Identity, a service that authenticates customer identity in the background, please read: infobip.com/products/mobile-identity

Client success story



1,000,000+
customers

Many of our clients have used 2FA to solve common industry challenges.

[Nickel](#) is a French-based fintech providing bank accounts and bank cards in 5 minutes through convenient stores throughout France and overseas departments. They needed a 2FA solution to optimize costs and streamline user onboarding.

The tailor-made sales approach Infobip offers provided them a global 2FA solution over SMS, using Voice as a failover channel. Nickel was able to quickly and securely authenticate new users using only their mobile phones.

The quick and efficient onboarding process helped Nickel to cross the 1 million new customer mark in 2018, reporting around 30,000 new monthly accounts - leading to an acquisition by BNP Paribas. For more information, read our Nickel case study: infobip.com/resources/case-studies/nickel

“ When we first started to work with Infobip, our main incentive was optimizing cost but in time we noticed that their 2FA greatly influenced our customer experience and they played a part in helping us to reach 1 million satisfied clients. We are very pleased by their skilled support teams and all the efforts they are providing to optimize their products for us.”

ADRIEN BONHOMME

Product and Organization Manager, Nickel

Use 2FA for:

- Device Authentication
- User Registration
- Transactions Confirmation
- Password Reset
- Money Transfer Validation

3. The Infobip Advantage

Our Two-Factor Authentication (2FA) uses 800+ direct connections to mobile operators, which ensures high delivery rates, fast delivery speed and unparalleled security.

This can help you to provide customers 2FA that is PSD2-compliant, and meets SCA and dynamic linking requirements.

Users can choose the 2FA channels they prefer

Infobip offers a wide selection of channels for 2FA. These are In-App Messaging (Push), Chat Apps, SMS and Voice.

Authentication needs to be fast and reliable, but also convenient for customers. This helps to maintain a positive customer experience. For this reason, Infobip gives you the ability to provide 2FA over the channels your users prefer for authentication.

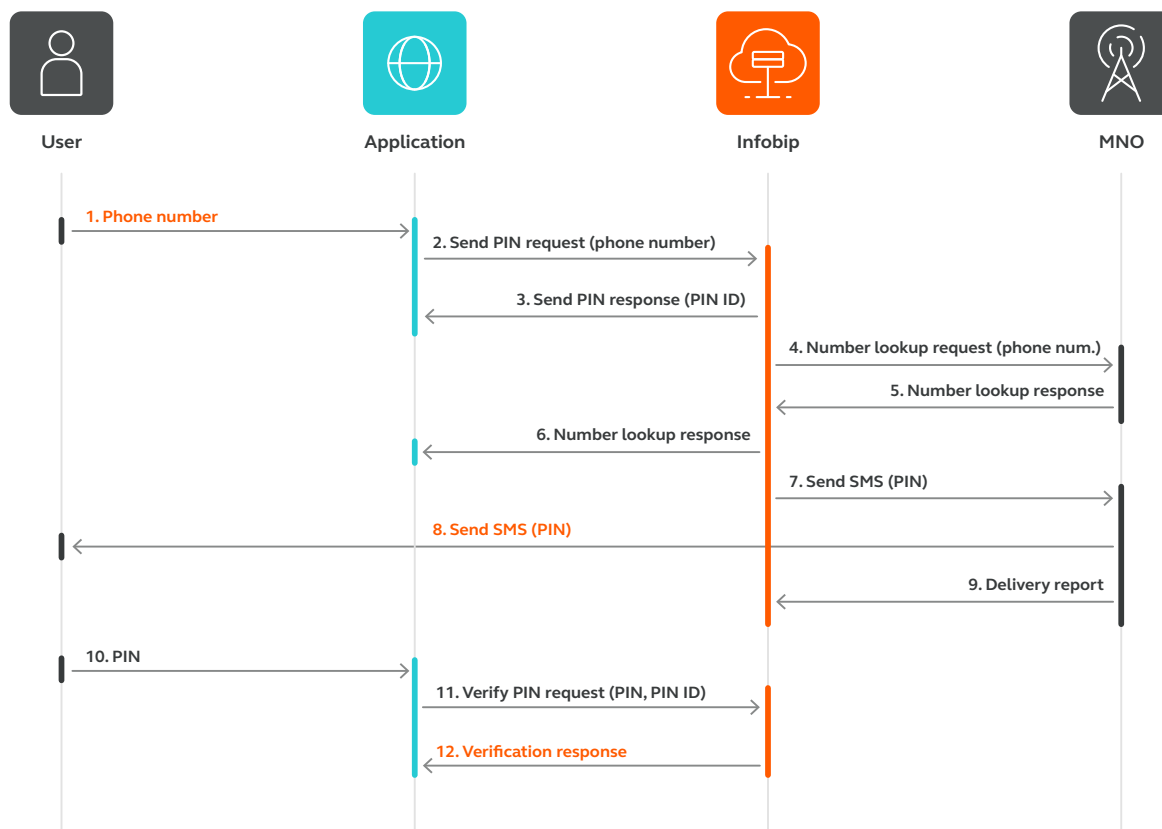
In addition to helping you create a positive customer experience, Infobip 2FA also uses **Number Lookup**. This gives you the option to check the validity of numbers in real-time against mobile operator databases, which helps optimize costs by sending to valid numbers, only. To learn more about this, see infobip.com/en/products/number-lookup

Generate your own OTPs and deliver with Infobip

For cases in which your organization requires you to generate OTPs using your own system, you can deliver these to your customers over Infobip channels (Push, Chat Apps, SMS, Voice...)

How our 2FA works

If you're using Infobip to generate and validate OTPs, before sending these to customers, Infobip's platform checks to see the fastest and most secure route over which to deliver an OTP. After confirming the validity of the mobile number, the process is as follows:



This all takes place in a matter of *seconds*.

“They are very easy to work with, extremely responsive and cooperative, and always there for us to overcome any obstacle. One of our greatest concerns was security and speed of delivery and that showed to be no problem at all with their solution.”

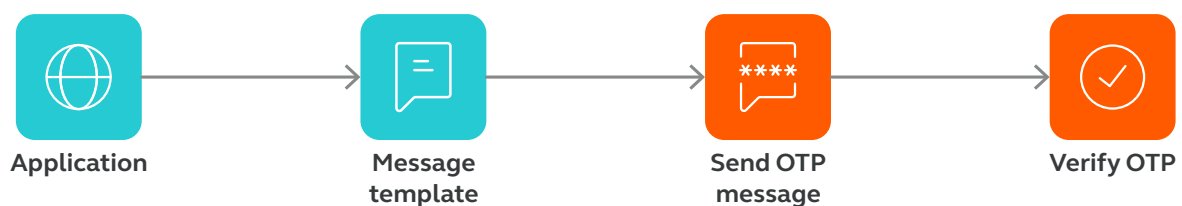
NATAŠA ZORIĆ

Head for Partnerships and Cards,
Partnership and Cards Department, Sberbank

4. How to Setup 2FA

2FA setup for PINs generated by Infobip

The setup of this solution consists of two parts, and requires only a small amount of coding – Application Setup and Message Template Setup. After setting up your template, you will reuse message templates to send out future OTPs.



Application Setup

The Application represents your service. It's recommended that you have separate applications for each individual service. You can also have separate applications for the same service and different use cases. For example, your login 2FA can be one application, and password change 2FA as another. Setting different use cases across applications gives you the ability to choose different options and behaviors for each use case (such as PIN attempts or PIN limits).

Find out how to start building a flow, here: dev.infobip.com/2fa#2fa-setup

Message Template Setup

Message template setup allows you to create custom message templates for sending OTPs to your users. You have the option to create several message templates for each application. This lets you use the same application for different use cases or even for different languages.

When creating your message template, you will be provided with a message template ID. This is used when sending OTPs. It works by referencing the message template ID, after which the Infobip platform generates an OTP. This is then inserted in the message template. After that, the message containing the OTP is sent to the user.

Find out how to set up message templates here: dev.infobip.com/2fa/message-template-setup

Send and verify OTPs

Once you've created the application and message templates, you are ready to send OTP messages. This process consists of two steps – Send OTP and Verify OTP.

Send OTP

OTPs are generated by our platform and sent out using the message templates you create. You can have one or several more message templates for each application, and reuse each template to send OTPs as many times as you like.

Verify OTP

Once the OTP is sent and received by the user to confirm their identity, you will need to verify whether the OTP is valid.

For details, please see: dev.infobip.com/2fa/send-and-verify-pin

Integrating Infobip 2FA

Our API supports three main authorization types – App, Basic and Single Session Login (IBSSO). The most flexible and secure of these options is App, which generates an API key.

API Keys allow you to generate authentication credentials that are independent from your username and password. These are not connected to each other and are easily disposable. It is suggested that you create unique API keys for each of your applications or servers, so that you can easily revoke them without disrupting other systems.

Type	Credentials Format	Notes
App	Infobip generated API key	Recommended authorization method
Basic	Base64 encoded username and password combination	Not recommended because the password is included in every request
IBSSO	Infobip generated single sign-on token	Useful for accessing API in a time limited session

Using API key is mandatory for sending and verifying OTPs. For more information about authorization, please see:

Security and authorization: dev.infobip.com/getting-started/security-and-authorization

Creating and managing API keys: dev.infobip.com/settings/create-and-manage-api-key

The advantages of using API keys:

- Ability to set permitted IP addresses for API origin, enabling you to define which IP addresses area permitted to access the API endpoint
- API permissions per API key, which enables you to set different API endpoint permissions for every individual key
- Validity periods for API keys, which can be set in accordance with your company's password policy
- No relation between usernames and passwords, meaning these login details are used only for API key creation and administration
- Easy API key deactivation – in case of breaches, a single API key can be deactivated without impacting other systems using different API keys

Offering customers 2FA is about more than being PSD2 compliant – 2FA keeps your customers and business safe from online fraud. Infobip provides turnkey solutions over secure channels that are quick and easy to integrate.

For more information, visit www.infobip.com. For a free consultation, [contact us](#).



infobip