telestax»

Smart 2FA Guidebook
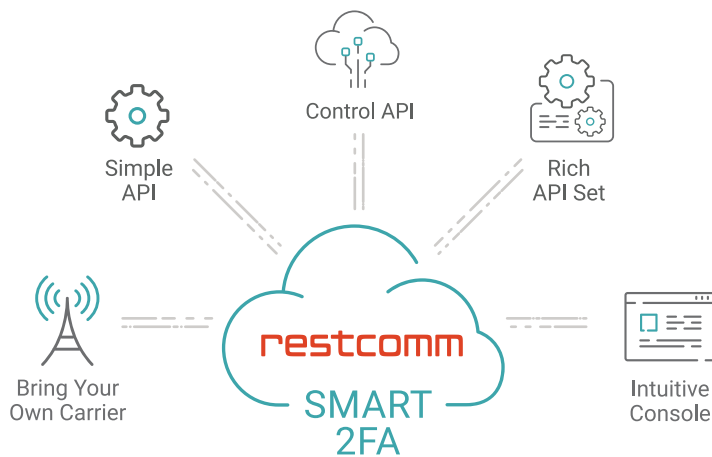
restcomm
SMART
2FA

Explore the security benefits of two-factor authentication (2FA) for financial, healthcare, travel, and more.

Today, nearly every popular application relies on two-factor authentication (2FA) as the best method to verify user identity when signing up or logging into online applications.

2FA Value

According to a recent report, receiving a secondary SMS code blocked 100 percent of automated attacks, 96 percent of bulk phishing attacks, and most direct, targeted attacks.* But like many technologies, it can be difficult to deploy. That's why Telestax developed Restcomm Smart 2FA.

Simple API

Control API

Rich API Set

Bring Your Own Carrier

restcomm

SMART 2FA

Intuitive Console

2FA FACTS

Adding a recovery phone number to an individual account can block up to

100%

of automated bots,

99%

of bulk phishing attacks, and

66%

of targeted attacks.*

With Smart 2FA, communications service providers (CSPs) can help enterprises and small-to-medium size businesses quickly deliver 2FA with a one-time password (OTP) to their customers, providing this critical safeguard for account security.

*Google Security Blog

Bring Your Own Carrier (BYOC)
Reduce costs and enable better delivery rates. Control routing from existing core Softswitch / SMSC to quickly address delivery or routing issues.

Simple API
Send OTP via various channels including SMS, voice, or email.

Control API
Cancel an existing OTP (while it is still active) to resend a new one, or keep an OTP active while a new one is sent.

Rich API Set
Select any language for voice calls via text-to-speech (TTS) with support for engines like VoiceRSS, Acapella, Amazon Poly, and Google Text-to-Speech.

Intuitive Console
Easy to use and view usage reports by day, month, year and search using filter criteria like country code, channel, delivery status, and more.

What Types of Businesses Can Benefit from Smart 2FA?

In this guidebook, you will discover the ways in which CSPs can help a variety of different businesses with Smart 2FA including:

- **Financial**
- **Healthcare**
- **Travel & Hospitality**
- **Retail & Online Marketplaces**
- **Government**

Each vertical market has its own distinct challenges. Fortunately, Smart 2FA offers CSPs a superior method of delivering services across these verticals.

Financial institutions enable 2FA to ensure secure access to banking portals, mobile devices, financial records, and more.

Securing Transactions

As 2FA is language-agnostic and completely programmable, it can be integrated within any mobile or web application. A bank may choose to require 2FA on specific events like sending an international wire when the amount exceeds a specified value or the destination is to a specified country. For example, business customers might be prevented from automatically sending over $5,000 USD or from sending money to countries with known active phishing scams without a confirmation. Another important use case is when the consumer adds a new beneficiary account the system will trigger a 2FA authentication before the user is able to send money to the new beneficiary.

Online Payments

Payment gateways are on the rise. Companies like Stripe or PayPal empower millions of businesses to accept online payments through their service. Payment gateways use 2FA to enhance their business users' security, ensuring that payouts are going to the verified bank account. The flexibility of a self-service portal allows users to update payout banking details securely when needed.

Additionally, most countries have regional startups, which are basically a localized version of PayPal and Stripe. For example, in Jordan Hyperpay is a payment gateway startup with a mission to be an alternative for businesses to Paypal and Stripe. A CPaaS-enabled CSP can provide 2FA to these types of payment gateways to enhance user security and user experience with a couple lines of code.

Digital Wallets

A digital wallet is a payment system that protects users' banking information and passwords and allows consumers to make safe transactions without using cash. Digital wallets require maximum security and end-user verification. 2FA is mandatory for digital wallet applications around the globe. With that in mind, a CSP can offer a dedicated 2FA solution targeting digital wallet providers.

2FA FACTS

With more than

9 in 10
MILLENNIALS

now owning smartphones and nearly

20%

of those users accessing the internet exclusively with smartphones, SMS becomes a critical way to do business.*

*Pew Research, Mobile Fact Sheet

THERE ARE MANY DIGITAL WALLET SERVICES AVAILABLE GLOBALLY INCLUDING:

Etisalat
UAE telecom carrier launched its digital wallet recently.

Bharti Airtel
Indian telecom carrier with nearly $12B in revenues per year launched a digital wallet solution in India.

UAE Exchange
A large financial institution based in UAE partners with EZ-cash to offer real-time mobile wallets across the globe.

Google Pay
Digital wallet platform and online payment system developed by Google to power in-app and tap-to-pay purchases on mobile devices, enabling users to make payments with Android phones, tablets, or watches.

Chirpify
Lets you use social media apps like Twitter and Instagram to buy, sell, send, and receive money.

Apple Pay
A mobile payment and digital wallet service by Apple Inc. that allows users to make payments in person, in iOS apps, and on the web. It is supported on the iPhone, Apple Watch, iPad, and Mac.

Samsung Pay
A mobile payment and digital wallet service by Samsung Electronics that lets users make payments using compatible phones and other Samsung-produced devices.

A CPaaS-enabled CSP can help digital wallet providers or financial technology companies around the globe to offer an intuitive, easy-to-integrate 2FA solution with Telestax Smart 2FA.

Healthcare facilities enable 2FA to allow for secure access to patient records and online appointment scheduling. Also, patient identity and privacy are protected in consultative calls when the doctor is in a different location.

Appointment Scheduling

CPaaS adds value in scheduling doctor's appointments and follow-up appointments, physical therapy appointments, recurring appointments, and more. It also facilitates the confirmation of appointments, improves the ability for patients to show up on time, reduces no-shows, and helps avoid cancellations. 2FA protects the identity of patients utilizing these appointment scheduling features by adding another layer of identity protection for users.

SaaS Provider Integration

When it comes to healthcare, there is noticeable growth in digitizing healthcare applications, which makes communication between patients and doctors more direct and convenient 24/7. Every healthcare organization using software as a service (SaaS) is interested in securing their patients' records from history to appointments, and more. Smart 2FA comes as a plug-and-play solution for every doctor, hospital, or pharmacy that utilizes software to manage their business. A CPaaS-enabled CSP can offer the 2FA integration directly with SaaS providers including **Practo**, for example. Once the integration is done with the SaaS provider, every healthcare provider is able to immediately enhance patient security using this new feature.

Patient Identification for Remote Care

CSPs can provide online remote care or "doctor-on-demand" applications with a method to trigger 2FA every time a patient is trying to connect with a doctor or other healthcare provider. This way, the provider can effectively verify the identity of the patient. For example:

1. The user is trying to initiate a video call to a doctor at $10.00/minute.

2. Smart 2FA sends a verification code - before the call - to the user via various channels (SMS, voice, or email) to confirm the identity of the user before they initiate the call.

3. 2FA helps reduce potential headaches or incorrect billing ahead of time with identity verification.

2FA Plus IVR

Another use case combines 2FA with interactive voice response (IVR). Most traditional doctors have a PBX on premises or in the cloud that handles patient calls for inquiries or setting up appointments. Since CPaaS is a multichannel technology, patients are able to access their visit history, records, and appointment calendar through self-service IVR. However, since the customer phone number can be spoofed, CSPs can offer 2FA as a second security layer for IVR menus to send a dynamic OTP every time the patient calls into the self-service toll-free or domestic number to access their records.

This is a compelling reason for doctors and healthcare enterprises to upgrade their communication infrastructure to a multichannel PBX flow built on CPaaS.

"

Missed appointments cost the healthcare industry over $150 billion per year. CPaaS solutions like appointment scheduling verified with 2FA can help organizations to be more effective.*

Healthcare Innovation, SCI Solutions, APRIL 26, 2017

Travel and hospitality businesses use booking portals to share deals, confirm itineraries, provide information, and more.

2FA implementation can allow customers access to their account history securely and privately, save credit or debit card information for a faster checkout experience, and gain the status of a verified account that can book now and pay later.

Account Registration and Security

Travel and hospitality businesses can introduce Smart 2FA into the sign-up process to simplify new registrations or the log-in process of returning users. By simply entering a phone number, the user receives a PIN via email, SMS, or voice call. Once they enter it, they are able to access the travel or hospitality service and quickly search, book, and pay for their upcoming experience.

Live Chat

Travel and hospitality businesses often introduce a live chat functionality on their website as a customer service channel. Agents are able to verify the identity of a customer by sending an OTP to the phone number on file or by asking the user to enter it in the chat box before they make any changes to the ticket, reservation, or itinerary.

Fast, Secure Protection for Frequent Flyers

Frequent flyers are often seeking a fast, easy, and secure booking experience. Financial details and government-issued identification need to be on file for these high-value travelers to quickly book tickets on any channel, whether online, by phone or using SMS chatbots. To combine convenience with security, Smart 2FA offers frequent flyers an automatic recognition of their account details on file as well as dynamic security via OTP delivered using SMS, email, or voice channels.

Unlike other 2FA solutions, Smart 2FA offers additional protection from caller-id "spoofing." The Restcomm Smart 2FA application programming interface (API) will recognize the frequent flyer customer phone number, or "from" number and pass it to the travel agency API to see if it matches any of the customers on file. If it does, then the customer will receive an OTP on another channel (SMS or email). Once the user enters the OTP, they are authenticated and able to search, book, and pay for their upcoming flight in seconds. Sending the OTP on a different channel like SMS or email on file is the best way to ensure maximum security for the caller.

A retail chain or online marketplace may enable 2FA so that customers can log in securely to order goods and services or save and update their payment information with confidence.

By verifying the identity of their buyers and sellers, they can ensure that the other party has been securely authenticated in advance to speed sales.

Retail and Online Marketplace 2FA Benefits:

- Verify buyer and seller identity during log-in and sign-up processes

- Secure financial transactions when a buyer is initiating a large payment or when the seller is requesting a payout

- Secure password recovery with 2FA in case email is compromised

- Make important changes with online customer service agents like changing the 2FA phone number on file, completing an address change, or uploading important documents

Loyalty Programs

Both retail and online marketplaces can win more business by providing the consumer with a loyalty program. A phone number or email is a user-friendly and cost-effective method to register consumers in a loyalty program and customers can sign up during checkout. Smart 2FA helps to verify the user phone number allowing the user to redeem points or gain access to their point balance in real time.

Electronic Receipts

Consumers around the world visit grocery stores to buy needed goods, completing their transactions with a paper receipt. Now, grocers can collect phone numbers from customers to provide electronic receipts and also use that phone number to deliver discounts or coupons and promote store events.

Once the consumer pays the bill, the following action is triggered:

1. SMS messages are sent to the consumer containing a "thank you" message and a URL

2. User clicks on the URL to view the receipt with all purchase details in PDF format

3. User can review all past purchase receipts by entering their phone number and PIN code received using 2FA

Expense Tracking

This approach unlocks a new feature for consumers and merchants where both can track the spending by customer phone number and then use this data for savings recommendations. For privacy reasons, this data should only be accessible by the customer with strong security measures. Smart 2FA can be triggered to ensure that accessing digital receipts is only possible when the customers want to do so.

Smart 2FA can provide retail stores with a single intuitive and multichannel OTP that can verify existing users or easily sign up new users and secure important future events like reward points redemption or acces to digital receipts history.

Governments may enable 2FA so that citizens can access e-government service securely 24/7.

Services can be additionally secured by 2FA to verify the identity in the case of important changes such as the ability to:

- Automate sign-up identity verification process for citizens
- Access or pay for automotive renewals
- Request passport renewal services online
- Access and pay taxes online securely
- Provide the government with a verified tip on a national emergency threat
- Secure e-filing services for trademarks or patents
- Apply, renew, or cancel residency services secured with 2FA
- Change the address on file
- Schedule, change, or cancel a government-related interview

Remove the Obstacles to 2FA Implementation

Smart 2FA allows CSPs to deliver a reliable and scalable 2FA solution over SMS, voice, and email channels to their enterprise customers and developers. With Smart 2FA, CSPs can go to market in hours using their own carrier network to provide better network quality, pricing, and network configuration for business customers.

Smart 2FA can provide e-governments with a single intuitive and multichannel API to trigger 2FA for any important event.

Let's talk about how Smart 2FA can deliver security and value to CSPs and their business customers.

Contact us at info@telestax.com.

telestax

CPaaS Enablement and Cloud Apps for Global Communications

www.telestax.com