A Guide To Verifying Users in Financial Services

Learn How Banks and Fintech Companies Can Securely Onboard Customers at Global Scale with Phone Verification

The world of financial services has radically changed. Alongside traditional institutions, there are now fintechs and challenger banks offering disruptive services and apps across payments, lending, money transfers, investing, crowdfunding, and cryptocurrency. It's a competitive space and on the global battlefield to win and onboard new customers, providing a convenient and seamless experience is what puts you in front.

Trust is also a company's most precious commodity in financial services. Trust is earned through your ability to protect your customers' identities while creating an outstanding experience. Which is why whenever you hear news of fraud or another **data breach**, it keeps you up at night. And recently, there has been a rise of both.

In 2018 there were **14.4 million** victims of fraud. While overall rates fell **15%**, fraudsters have turned their attention towards higher-impact fraud such as new account fraud, account takeovers, and digital payment fraud.

More than 1 in 9 of all new accounts opened in 2017 were reportedly fraudulent

New account fraud losses increased from $3 billion in 2017 to $3.4 billion in 2018

Online payment fraud is predicted to reach $22 billion in 2019 and $48 billion by 2023

The frequency of account takeover attacks has increased by 170%, with an account takeover now taking place once every ten seconds on average

In a world where users can open accounts, apply for loans, send money globally, and trade cryptocurrency with only a few taps of a device, financial services companies are prime targets.

It's now more crucial than ever to verify your users are who they say they are. Otherwise, it becomes more than just an inconvenience for you and your customers. Reputational damage, loss of trust, and enormous financial and legal costs are at stake that could destroy your brand before you've finished building it.

The average cost of cybercrime for financial services companies globally increased from nearly $13m million per firm in 2014 to over $18m million in 2017

Phishing and social engineering were among the most expensive type of attack, costing over $196,000 per incident

But as a fast growing financial services company onboarding hundreds of thousands of customers around the world, how can you securely verify users at global scale without sacrificing a seamless experience?

In this guide, you will learn how to protect your customers and your business with the most frictionless solution for global user verification: phone verification with two-factor authentication using SMS and voice.

User Verification: A Balancing Act in Financial Services

In the race to acquire users, onboarding is a make or break moment in the customer experience. Ask your users to jump through too many hoops and you risk frustrating them. But without a strong user verification system in place at registration (and beyond), you could be exposing your customers—and your business—to identity abuse and fraudsters.

Verifying new and existing users with two-factor authentication (2FA) has become the standard in financial services to combat the threat of fraud.

2FA can range from the extremely secure and expensive, to the relatively frictionless and cost-effective. When selecting and implementing 2FA for a growing global user base, you need to ask yourself several questions to strike the right balance between security and a seamless experience:

1. **One solution**
   Is it a single standard that works across different global infrastructures?
2. **Meets Global User Experience Standards**
   Will it be considered an acceptable experience by users in different regions?
3. **Fallback**
   Does it automatically failover to another channel if the first attempt doesn't get through?
4. **Letting Good Users In**
   Does it unintentionally block out good users?

What is 2FA?

2FA works by combining something a user knows (a password) and something that a user has (a phone or hardware token), to verify their identity. While it has become relatively easy for fraudsters to steal passwords it is much more difficult to steal a password ***and*** hack a second factor.

Phone Verification: The Most Effective Defense for Going Global

A frictionless experience for global growth using SMS and voice two-factor authentication

When balancing a great experience with effectively validating the identity of an individual, the ideal way to accomplish this on a global scale is through phone number verification. Unlike other 2FA methods that may require special hardware or an authenticator app, phone verification solution works with any phone number.

Phone numbers have emerged as the ultimate user identifier in financial services not only because almost everyone on earth can be reached by phone, but also because people retain their numbers for very long periods of time—ten years and more.

The Ultimate User Identifier

5.1 billion people across the globe can be reached via phone

90% of people read a text message within the first 3 minutes

While there are more secure (and cumbersome) options for 2FA, it's about striking the right balance between convenience and effective security. Phone verification provides that balance. It's the global standard today for a smooth onboarding.

Why Phone Verification?

- Works in virtually every country
- SMS has higher read rates than email
- Simple experience independent of infrastructure and culture
- There is extra data behind a phone number to identify fraud
- Customizable user experience

Phone verification helps you quickly, easily, and cost-effectively verify user identity and reduce the risk of fraud. Verifying users at sign up is the first key step to stopping fraud before it happens, but when else should you use phone verification in the customer journey?

How Phone Verification Works

A user is sent a PIN—also known as a one-time-password (OTP)—in a message sent over a phone-based channel such as **SMS**, **Voice**, **WhatsApp**, or **Viber**. Only the owner of that phone number gets access to the PIN. They enter it into the application to verify their identity and can then successfully register, log in, or confirm a payment. You can choose to have each PIN expire within a few minutes for added security, preventing fraudsters from using old codes to create fraudulent accounts.

1. Sign Up

Online

App

Enter phone number during account creation

2. Verify

SMS

Voice

Receive PIN by SMS or voice

Confirm PIN within application

3. Customer Onboarded

"Thanks for signing up!"

Account securely created

When Should You Use Phone Verification?

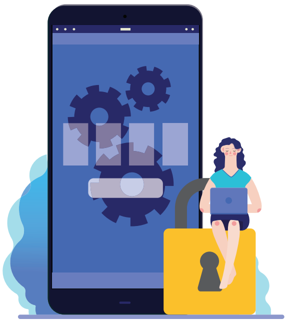
Verify users at sign up through to account changes and payment confirmation

New Account Creation

Seamlessly Sign Up a New User and Stop Fraud Before It Happens

Onboarding new users needs to be quick and easy, but also secure to protect your customers and your business against fake account creation. When a new user registers for your application, phone verification can help authenticate identity, ensuring your new user is who they claim to be.

For example, a new user who downloads an app and registers for a new account, will receive a PIN code via a messaging channel or via voice. They enter the PIN to complete the user registration process, which links the user and their device.

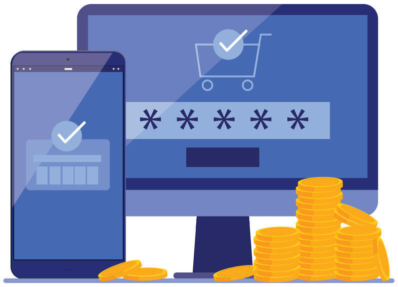


Account Changes

Protect Your Users and Your Platform Throughout the Journey

It's good practice to not only verify users at the point of sign up, but also when a change to the account is being made such as a password reset or profile update.

When a user logs in to a web or mobile app from an unknown or alternative device (i.e. with a different IP address from the one registered in their profile) and requests a password reset, sending a code to verify the user's identity can help reduce fraud and identity theft. Changes in user profile information should always be confirmed with a simple verification message to the mobile device linked to an account.



Authenticate Transactions

Reduce Payment Fraud and Address Compliance Requirements

Verifying transactions significantly reduces fraud. Confirming users at this critical moment via phone verification is so effective at reducing suspicious activity that many payment services now require authentication of transactions with a one-time PIN sent via SMS.

Driven by increasing payment fraud, as of September 2019, any business—including financial services companies—that process transactions in Europe will face a new layer of friction by requiring strong customer authentication. Set out in the **PSD2 regulations**, it will soon be mandatory to verify transactions over 30 Euros using two-factor authentication, even if only one party is in EU. Phone verification using a one-time PIN sent by a messaging channel or voice can help you address your strong customer authentication requirements with the least amount of friction on a global scale.

Alternative to the Password

A Stronger and User-Friendly Alternative to Traditional Passwords

By establishing a passwordless authentication process you can improve the user experience by enabling users to log in to applications without having to recall cumbersome passwords. Users can simply click or tap on the web or mobile application, receive a one-time PIN via message or voice, enter that code, and get immediate access upon confirmation.

Getting Global Phone Verification Right

8 key considerations when validating phone numbers in financial services

In theory, validating a phone number sounds easy. But in reality, as a growing financial services business onboarding users in dozens of countries, there are several challenges you need to be aware of to make it a success.

1. Delivering SMS Pin Codes Quickly and Reliably at Global Scale

The longer it takes for a user to receive a PIN, the less likely they are to sign up to your service, access their account, or confirm a payment. To avoid your verification messages hopping from carrier to carrier, you may need to work with several SMS vendors to manage routing logic in different regions.

2. Pin Code Management and Auto-Failover to Increase Conversion

To optimize conversions, you will need to implement an automated resend of the PIN if the user hasn't entered it within a certain time. Failing over to a voice call to present the PIN audibly is another option if the initial SMS doesn't convert.

3. Keeping Track of Global Compliance Requirements

When verifying international numbers via SMS or voice, you need to be aware of the complex myriad of regulations which vary around the world. If your messages do not comply with local regulations, they will be filtered and fail to reach your users.

4. Distinguishing Mobile Numbers, Fixed Lines, and Virtual Numbers

Some countries clearly distinguish landlines and mobile phones, while in others there is an overlap. You need to identify the difference to deliver messages to the right channel. Identifying and blocking virtual numbers is also critical for spam and fraud prevention.

5. Providing a Localized User Experience

When you are verifying phones across the globe, you cannot rely on using the same message templates or languages everywhere. Messages need to be targeted to optimize conversion rates including country-specific language, message format, and tone.

6. Ensuring Security

When generating a verification PIN, you need to follow industry standards for time-based one-time PINs. Balancing security with experience is critical at this step. You don't want a PIN to expire before your user can enter it, but you also need it to automatically expire if the user has not entered it within a reasonable time period.

7. Controlling Operational and Management Costs

The more verified users you onboard, the more fixed costs you will incur. Successful global verification needs dedicated teams to manage message routing, analytics, and navigate the many different global standards and compliance requirements.

8. Improving Insight to Optimize Conversion

Less than optimal conversion rates may be the result of something unrelated to the SMS infrastructure itself. Success requires the proper insight and analytics to understand where problems may lie and what, if anything, you can do to mitigate those problems.

How Financial Services Companies Verify Users with Nexmo

With over 20 billion phone verifications to date in over 230 countries, Nexmo helps global financial services companies overcome the challenges of phone verification to seamlessly verify users around the world.

Auka Adds a Layer of Protection with Nexmo-Powered SMS User Authentication

Payments

Driven by the increasing popularity of seamless payments and the sharing economy, leading Norwegian fintech provider **Auka** built a platform that empowers financial institutions and retail banks with seamless mobile payment technology.

The Auka cloud-based platform allows retail banks to offer mobile payment capabilities to its corporate and merchant customers with minimal cost, risk, and complexity.

To add a layer of protection to the platform and its users, Auka selected Nexmo to enable secure user authentication. Equipped with Nexmo's reliable, international SMS capabilities, Auka effectively scaled its user verification processes across the 17 banks running on the Auka platform.

"Having an agile platform is the key to staying ahead of our competitor's product innovations. Using Nexmo allows Auka to provide bank-grade systems and services that financial institutions trust and rely on for their business."

- Daniel Doderlein | Founder & CEO | Auka

Remitly Reduces Fraud with Nexmo SMS Two-Factor Authentication

Remittance

Remitly is the largest independent digital remittance company headquartered in the U.S. The 400+ person, Seattle-based company transfers over $2 billion annually from their customers in the U.S., United Kingdom, and Canada, to recipients in India, Mexico, Latin America, and the Philippines.

To ensure a trusted experience, it is imperative that remittances are sent through legitimate, highly-secure channels that use the most innovative technology to safeguard against fraud and suspicious activity. Global authentication was therefore on Remitly's list of "must-haves".

In addition to building trust, a significant way Remitly reduces costs is to make sure that fraudulent transactions are kept to an absolute minimum. It achieves this using SMS two-factor authentication powered by Nexmo.

Not only does phone verification make a significant impact in reducing Remitly's fraudulent transactions, but it also makes a big difference in terms of the money saved because of the losses that were prevented. Moisef estimates that somewhere in the neighborhood of $250K – $300K have been saved since implementing Nexmo phone verification.

"With Nexmo, we can verify a customer's identity, or the ownership of an account, in various ways. We have actually seen a discernible decrease in fraud rates by using these different methods that allow us to authenticate customer accounts."

- Nick Moisef | Director of Products | Remitly

How Financial Services Companies Verify Users with Nexmo

BitQuick Reduces Fraudulent Transactions with the Nexmo Verify API

Crytocurrency Marketplace

BitQuick is a leading cash-for-bitcoin marketplace that powers highly secure and convenient online peer-to-peer transactions via cash deposit in a matter of hours. To purchase bitcoins on **BitQuick.co**, a buyer deposits cash into the seller's account, and the bitcoins are sent shortly after uploading an image of the deposit receipt.

A major challenge for BitQuick is that of fraudulent and illegitimate transactions when users place bitcoin orders without any intention of paying for their purchases. This results in bitcoins "locking up" in escrow, disabling them for purchase by other buyers.

To solve this critical business issue, BitQuick required a solution that would allow them to verify purchases by authenticating the buyer for each transaction. The company needed a cloud communications partner that could deliver high conversion rates on an international scale, to support future global expansion. So, BitQuick opted for the Nexmo Verify API.

"BitQuick customers are looking for a quick buying or selling process. Knowing that phone numbers would conveniently provide identity information to verify our users, we needed a partner that we could not only integrate quickly but would provide high verification success rates."

- Jad Mubaslat | Founder and Former CEO | BitQuick

Using Nexmo Verify API, BitQuick successfully sends SMS-based verification codes to users to confirm that they intend to make the payment, effectively reducing the number of holds on unpaid orders and increasing the amount of bitcoin available for legitimate purchasers.

Nexmo Verify API helps BitQuick:

- Verify transactions using SMS-based two-factor authentication
- Ensure that only legitimate buyers with verified phone numbers can place transactions
- Reject virtual or VoIP numbers, which are often fraudulent
- Determine fraud risk by comparing IP-based locations with phone numbers

The results:

- BitQuick increased its order success rate from 35% to 55%, while also doubling the overall transaction volume during the initial 60 days
- Increased the volume of bitcoins, resulting in an increase in successful transactions
- Only charged for successful verifications, enabling accurate and predictable cost forecasting as volume increased
- Boosted the ARPU for each of their users by legitimizing online purchases

About Nexmo Verify API

Add seamless phone verification to your customer journey

To maintain the growth of your app or service, you need to protect your users and your business. Phone verification helps you filter out fraudsters while providing genuine customers a frictionless experience, on a global scale.

With the **Nexmo Verify API** you can verify any phone, anywhere. Quickly and seamlessly authenticate new or existing users with our global network to deliver verification codes that increase conversions across multiple channels.

Let us do the heavy lifting, or customize the experience for your users. The Nexmo Verify API is an all-in-one solution that lets you:

- Generate your own PIN or allow the Verify API to manage it for your application
- Choose which channels to use when verifying users, and in which order
- Only pay for what you use with pay-per-attempt or per-conversion pricing

+1 415.941.5878 | sales@nexmo.com

Beyond Verification

First impressions count. Using the Nexmo Verify API to verify users' identities adds a layer of protection and builds trust, from day one. Now is the ideal time to ask yourself how else you can strengthen the relationship by engaging your genuine customers throughout their journey?

Make every customer interaction count by adding voice, video, and messaging to your app or service with Nexmo APIs:

Voice API - Delight and inspire by adding custom voice interactions into your app

Video API - Engage your customers with interactive live video experiences

Messaging API - Drive deeper customer engagement with messaging

Global companies such as Alibaba, Expedia, and Viber rely on Nexmo to power millions of interactions per month with our easy-to-use APIs.

Speak to an Expert About How You Can Get Started with Verify.

GET STARTED