OpenMarket
An infobip company

The complete guide to secure mobile messaging

How to enjoy all the benefits of business messaging, while protecting your organization and customers

Introduction

Business-to-consumer mobile messaging enjoys a reputation for delivering a spam-light and safe communications experience to consumers. It's one of the reasons the channel has enjoyed such a boom in recent years. But popularity inevitably puts a channel in the crosshairs of fraudsters and spammers.

So what measures should you put in place to protect your brand and customers? This guide is here to help.

It describes the mobile messaging risks out there and the people and processes you need in place to combat them. It can also be used to inform your mobile messaging procurement process, setting out all the security measures prospective solutions providers should be on top of. Let's work together.

Finally, this guide is a call to arms. Businesses like yours have a huge role to play in keeping business messaging safe. It starts with ensuring the provider you choose adheres to practices that protect your customers and the wider ecosystem.

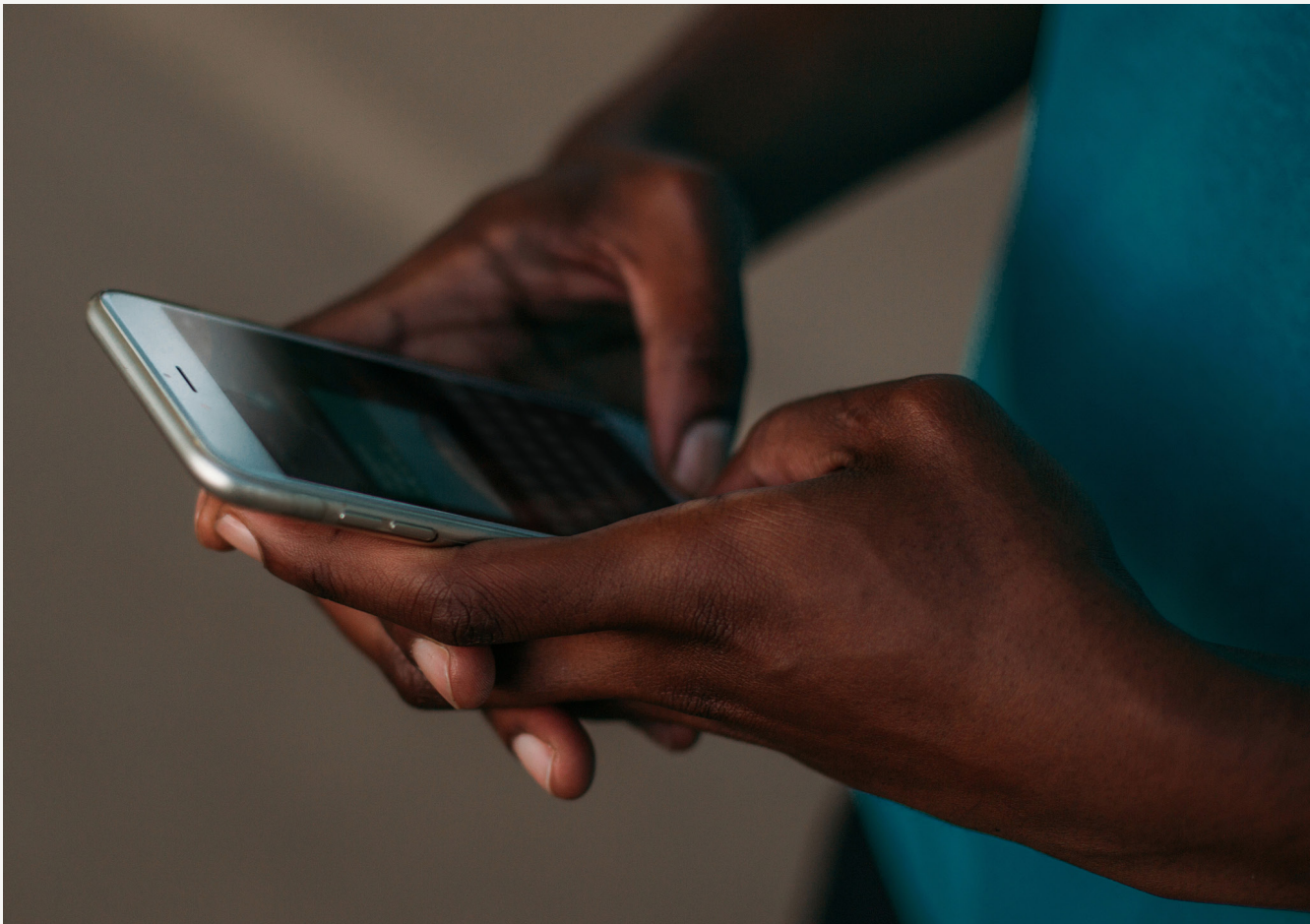
Mobile messaging is transforming the way organizations communicate with customers on a global scale. It allows you to be there for your customers at all times – no matter where they are in the world.

This is a channel we all need to protect. Let's keep it safe together.

Who is this guide for?

This is for everyone involved in buying, setting up and rolling out a mobile messaging service to consumers and employees. It should be especially relevant for these departments:

- **Procurement**
- **Marketing, Communications & Sales**
- **Product**
- **Logistics**
- **Legal & Compliance**
- **Technical**



Part one

The mobile messaging security landscape

Part one

Today's threats

The mobile industry started with voice calls. Then SMS came along. Then web functionality. Now the mobile devices we own are hubs for an overlapping, intertwining variety of communication services. Without the right security in place, these services are all potential areas of vulnerability.

Just a decade ago, businesses tended to protect themselves from online threats by purchasing the right antivirus and firewall solutions. Those simple days are behind us. No one solution or stakeholder in the mobile messaging ecosystem can combat fraud and channel misuse on its own. We need a concerted effort from all the players involved in sending and receiving business-to-consumer mobile messages. Let's look at who those five players are:

1. **The mobile operators**
   Otherwise known as carriers. Think Verizon, AT&T, T-Mobile, Vodafone and similar others.

2. **Messaging solution providers or aggregators**
   Traditionally, aggregators and messaging solution providers have been classified in terms of their connections to leading mobile operators. A Tier-1 SMS aggregator has both direct technical connections and commercial relationships with the mobile operators. This allows them to provide an assurance on quality and security matched only by the mobile operators themselves (more on that later in this guide).

3. **Brands**
   That's you.

4. **Consumers**
   Think of consumers as existing or potential customers of your brand – but also as customers of a carrier. You have to send messages through this carrier to reach your customer. The carrier wants the customer experience on its network to be safe, smooth and spam-free.

5

Support services

Various mobile industry players provide services – such as data security, antivirus software and firewalls – to mobile operators and messaging solution providers.

OpenMarket is a Tier-1 messaging solutions provider with direct connections to all the major mobile operators in the US and UK, and access to three billion mobile users in more than 250 countries.

The importance of providers

Every party has a role to play, but to ensure your messaging is secure, your single most important action is to choose the right messaging solutions provider. A provider should be a leading voice on security in the industry, and enjoy influence over mobile operators' security policies and practices. Just as importantly, it should protect its own systems from malicious attacks, prioritizing the security of customer data.

The center of a chain

Mobile messaging exposes users' personal data – namely their mobile number, personally identifiable data, and their messaging content – to a variety of companies involved in the processing of the messages.

A provider will be in the middle of a chain of players involved in transporting messages across the world. The more players there are, the more exposure there is to risks. The messaging solutions provider you work with should be careful about who it works with, checking that they work hard to protect its customers' data too.

Overall, look for transparency in your provider. It should let you know what happens after a message leaves you on its way to the consumer, and what happens when messages are sent back from a consumer to you.

Understand messaging risk factors

Messaging security risks to be wary of are much the same as those we're familiar with online – phishing (the SMS version is known as smishing), spamming, spoofing, identity theft, data theft and virus distribution are a few examples.

SIM-swap fraud has received a lot of media attention in recent years in relation to two-factor authorization (2FA).

A few years ago, just as SMS 2FA was taking off as a means to confirm identities, attackers worked out a way to call a carrier claiming to be a customer. They'd then persuade the operator on the other end of the phone to port that customer's number onto a new SIM card. This meant the attacker could receive all of that customer's SMS messages on their new SIM.

Happily, this process lapse has been tightened up in recent years. Now all major mobile operators insist customers prove their identity before making a configuration.

Securing the SS7 System
But then there's the rare incidence of attacks on the SS7 system to consider. SS7 (Signaling System 7) is a set of protocols that allows phone networks to exchange information with each other. Sophisticated attackers can potentially access the SS7 system. If they also have a target's username and password for a particular account – let's say a subscription to software – they can then reroute text messages
for that person's number, and access that account.

Fortunately, these types of attacks are rare and difficult to pull off. Attackers have to find a way to enter the SMS network AND get hold of usernames and passwords. Unless the target is extremely high value, they're highly unlikely to go to this trouble.

54%

What's more, operators across the world have awakened to the SS7 threat and have been installing firewalls to protect the network. Illicit messages and suspect patterns can be blocked immediately.

Industry analyst Mobilesquared predicts that 54% of mobile operators will have invested in SS7 firewalls by 2022. However, we believe that a roll out of SS7 firewalls will take place even more quickly. It's in the industry's interest to ensure SMS keeps its reputation as one of the most secure forms of business-to consumer communication.

Ease and simplicity

Let's be clear: no form of online security is absolutely secure. Using two authentication techniques (for example, a password and a passcode sent to your phone) is far more secure than one-factor authentication (a single password).

So don't be tempted to discount SMS authentication systems based on reports of weaknesses. The reality is that people everywhere – including a reported 90% of Gmail users – are still leaving themselves vulnerable to fraud by securing important online accounts with a single password only.

They're failing to take up the option of 2FA for reasons including the hassle involved, the unfamiliarity of the technology, or because they underestimate the threat to their accounts and applications.

To ensure as many of the reluctant masses as possible protect themselves, a simple and accessible 2FA method is needed. That's where SMS comes into its own.

Never use a phone number for one-factor authentication

One-factor authentication is no longer an effective security measure. That's why a phone number shouldn't be relied on by companies as a single source of identification in security processes.

Many companies still let users reset their passwords with nothing more than a one-time code texted to a phone number on the account. In this type of attack, the attacker doesn't need to know the victim's password to hijack the account. That's why phone numbers should be used as part of a two-factor or a multi-factor process.

In general, most types of messaging fraud can be defended against by the adoption of common sense, good security practices by the parties involved, and security technology at the network level.

An international challenge
The international nature of mobile messaging inevitably presents some big challenges. Some aggregators look to exploit the cross-border agreements that allow mobile operators to send messages across the world. This creates one of the biggest security challenges for the messaging industry – grey routes.

Grey routes

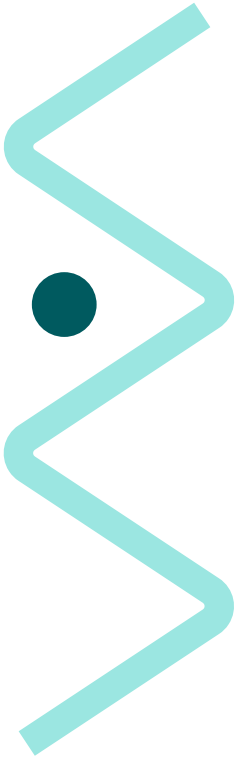
It's worth knowing a little about the history of grey routes to fully understand what they are and why they exist.

How grey routes began

Mobile operators have long had an agreement in place to ensure everyone can use their mobile phones when traveling. This agreement allows overseas operators to pass messages onto domestic carrier networks for a negligible cost.

However, this has created a 'grey route' loophole that can be exploited by unscrupulous SMS aggregators. It works like this: normally, if a business sends a message from the UK to a UK handset, the message goes straight to the UK mobile network. But by routing a business message from the UK to, say, Kenya, then back to the UK, an aggregator can ensure it never has to pay market-price routing fees to mobile operators. This reduces the cost of messaging to almost nothing.

The bad news for consumers? This practice comes at a big cost to messaging security and reliability.



Beware of low prices

That's why the cheapest mobile messaging provider is never the right one. Providers with prices that seem too good to be true send their traffic along grey routes. This would leave both your messaging content and your customers' contact details exposed, liable to interception, and at risk of being doctored.

What's more, messages sent through grey routes can endure long delays in transit. And as networks find new ways to shut grey routes down (more on that later), the risk of messages not being delivered at all rises.

White routes rule

Your messages should only be sent through direct, secure, fast routes set up solely for businesses. These are known as white routes. On white routes, both the messaging 'source' and messaging 'destination' have entered into a termination agreement covering both price and traffic.

The 'source' and 'destination' can be two mobile operators, or a mobile operator and a messaging solutions provider. Typically this will be a Tier-1 provider acting as a hub to other messaging aggregators or providers. (OpenMarket fulfills this role for most of the industry.)

The plague of SIM farms

Like grey routes, SIM farms have plagued the messaging industry in recent years. SIM farms are used by shady operators to pump out messages for minimal cost. They exploit the unlimited SMS deals offered on some prepaid SIM cards.

Hundreds or thousands of these cards are linked to a computer system and server connected to a mobile network. They then pump out messages at virtually no cost. Not surprisingly, SIM farms have become associated with illicit activity, not just spam, but non-compliant activity such as malware and virus distribution.

The message for brands is clear: when business messaging prices seem too good to be true, they probably are.

Good news on grey routes and SIM farms
The good news is, grey route traffic is gradually being eliminated from the business messaging ecosystem as key players invest in SMS firewalls.

Mobile analyst Mobilesquared found that the value of the grey route market accounted for just over half of business-to-consumer SMS traffic in 2017. But it predicts that white route traffic will account for 97% of total business-to-consumer SMS messaging revenues by 2022. SIM farms are also being squeezed out by improving firewall technology.

A more secure RCS future
The introduction of RCS (Rich Communication Services) has led to even more secure messaging.

As well as delivering a richer, more immersive experience, and deep data analytics, it provides a far more secure, traceable ecosystem. Grey route traffic is not possible on the RCS channel. That's great news for security-conscious brands and consumers.

Learn more about how RCS works **here**.

OpenMarket has a machine-learning-powered, anti-spam and fraud platform protecting its routes.

The system helps us unpack the semantics of a message in real time, so we can classify messages as safe, suspect or malicious. If an aggregator that sends messages through us is attempting to use a grey route, we're able to spot this.

The A2P (application-to-person) mobile messaging industry needs to leave no stone unturned in its fight to rid the network of unwanted traffic. As a new era of rich mobile messaging emerges, we need to push the technological boundaries to protect our business customers, and to improve the experience of their users.

Part two

How to choose a secure provider

Security first

Just like any communication ecosystem, the mobile industry will always have risks to tackle. Your most important move is to work with a messaging solutions provider that prioritizes the protection of your brand and customers.

There's a long list of competencies and practices you should look for when choosing a messaging provider. We set these out in this section, but on a high level, look for a provider with a global team of information security, privacy and regulatory experts, led by an experienced Chief Information Security Officer (CISO).

The provider should be able to go beyond just describing the security infrastructure, processes, and policies they have in place. They should be able to show independent confirmation from a trusted third-party that they have the right protections in place.

And remember, a cross-ecosystem approach to messaging is vital, so look for a provider that works closely with mobile operators, regulators and every messaging stakeholder to maintain the safety of the ecosystem.

Those are some top-top-level requirements. But here's a more granular list to refer to:

1. **Security history**
   Find out whether a prospective provider has ever had a security breach. If they have, find out why it occurred. A breach in itself shouldn't necessarily rule a potential partner out, but the circumstances of the breach could prove illuminating.

2. **Security frameworks**
   Look for certification under ISO/ IEC 27001 (2013). This is a globally recognized standard that certifies the robustness of the security controls concerning the people, processes, and technologies that make up a messaging platform.

3 **Availability, integrity, and resilience**

Components of a provider's platform should be highly available so customers are protected from data loss. Look for data centers that are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. If hardware, software, or a network does fail, services should be automatically shifted from one facility to another so operations continue without interruption.

4 **Regularly test disaster recovery plans**

Disaster recovery plans should be regularly tested. Look for comprehensive disaster recovery and business-continuity programs based on accepted standards. Infrastructure and application teams should test their disaster recovery systems. They should also test communication plans, failover scenarios, operational transition and other responses to emergencies.

5 **Access controls**

Employees' access rights and privileges to networks and data should be role-based and tightly monitored. Look out for the concepts of 'least privilege' and 'need-to-know' access. Requests for additional access should follow a formal process that involves a request and an approval from a data or system owner or someone higher up the chain.

Networks should be segmented into security zones that enforce these principles. The trust level of zones should be well-understood and enforced.

6 **Data protection**

The European Union's General Data Protection Regulation (GDPR) demands that both data processors and controllers implement technical and organizational measures that ensure their services are adequately protected from data leaks and breaches. Look for an infrastructure and processes designed to provide security through the entire information processing lifecycle.

7

Secure development lifecycle
Look for providers that build security into their development lifecycle and practices. This should include:

- Secure coding standards
- Secure coding training for developers
- Continuous code analysis and application security scans
- Secure deployment and operations
- Regular penetration testing
- Regular rehearsal of procedures to address security incidents, including the identification of security flaws in production.

Security practices should also extend beyond the traditional DevOps lifecycle to include factors such as the thorough vetting of personnel and procedures to maintain high availability and business continuity.

8

Vulnerability management
Providers should scan their systems for vulnerabilities, remediate the greatest threats, and stay current with the latest security patches.

9

Security through the entire information processing lifecycle
Infrastructure on which SMS, MMS and RCS are run should be built to provide secure deployment of services, secure storage of data, and secure and private communication with customers, complete with end user privacy safeguards.

Security infrastructure should be built in layers that support one another. The physical security of data centers supports the security protections of hardware and software, which support the processes that control operational security.

10

Safeguards for protection of personal or sensitive information

Look for an effective information security management system (ISMS), represented by leadership and key stakeholders. They should provide direction on measures such as:

- Identity and access management
- Awareness and training
- Audit and accountability
- Configuration management
- Information security governance
- Incident response
- Security operations
- Media protection
- Personnel security
- Physical and environmental protection
- Risk management
- Security development and acquisition
- Network security
- System and information integrity

11

Protection of systems against newly discovered vulnerabilities and threats

Continued cycles of risk assessment to identify new risks are important. Threat models should be used for determining vulnerabilities and threat vectors. Information security countermeasures – for example, firewalls – should be deployed inside and outside network perimeters to detect and prevent external and internal threats.

Any potential threats should also be monitored with vendor and industry security bulletins and alerts.

12 **Encrypt data in transit on external public network, including the internet**

Data should be encrypted in transit using common industry-accepted encryption ciphers and strengths. Customer content stored at rest should also be protected by one or more encryption mechanisms.

Connections to mobile operators should utilize encryption technologies appropriate to the sensitivity of the information being transmitted. This means either VPN tunnels or SSL (TLS 1.1 or greater) to encrypt data being sent over public networks or private networks.

13 **Data protection team**

Look for a dedicated team to handle data protection-related enquiries. It's also a good sign to work with a company that's provided contractual commitments around incident notification for many years, even before GDPR.

14 **Find out the stated approach to GDPR**

If you're a data controller that works with external partners to support your customers, you're required to use data processors that implement GDPR compliant technical and organizational measures. Mobile messaging providers are considered by GDPR legislation as data processors.

Ensure potential providers employ information security and privacy experts who implement security policies, maintain defense systems, develop security review processes, and build secure infrastructure. Information privacy and regulatory compliance experts are important parts of a provider team too.

15 **Data processing agreements**

Data processing agreements should clearly articulate a provider's commitment to customer privacy. You should be able to clearly assess your compliance status when using a provider's services.

16 **Data protection commitments**

Any data entered into a provider's systems should only be processed in accordance with a customer's instructions. Personal data should be retained for only as long as is necessary to fulfill the purpose identified in the notice or as required by law.

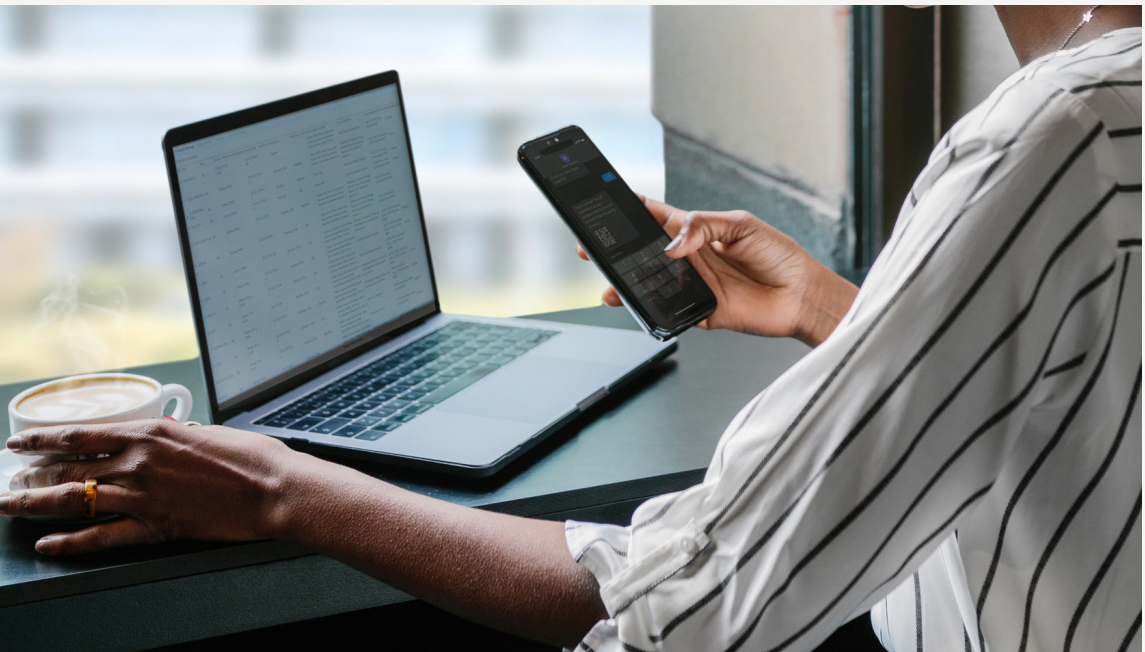
If your company has stricter data retention standards – or is subject to local regulations that require stricter data retention standards – check whether the provider adheres to them. Relevant employees should also complete confidentiality and privacy training.

17 **Relationships with data 'sub-processors'**

Sometimes providers have to route messages through one or more intermediaries before the message arrives at the carrier. Each of these mobile operators and intermediaries might be considered sub-processors under GDPR. Your provider should ensure these sub-processors protect customer data from leaks and breaches in compliance with GDPR and other internationally accepted security standards.

18 **Data storage**

A combination of storage technologies should ensure customer data is protected from hardware failures. Hosting should take place in data centers maintained by industry-leading service providers, with state-of-the-art protection for the infrastructure.



We're in this together

If you've read to the end of this guide, you no doubt already take the security of your business and customers seriously.

You'll know that threats and vulnerabilities change from week to week. And you'll know that maintaining security in a wireless environment is a constantly evolving dynamic.

Your task is to stay ahead of the curve, keeping your systems and processes up to date, working with leading, security-conscious tech providers.

It's hard to underestimate the importance of mobile messaging security as the channel becomes ever-more central to brands' communications infrastructure.

Work with the right provider, and you'll maximize your chances of enjoying a secure, open line to your customers, long into the future.

That's it!

Your complete guide to secure mobile messaging.
We hope it has answered all your questions and proved useful. If you have any more questions or you'd like some specific advice about security issues, we'd love to chat.

Get in touch

We are OpenMarket
As an Infobip company, we help the biggest brands in the world use mobile messaging to connect with people in the moments that count. When they need to be helpful and responsive in real time. When customer experience isn't just a buzzword, it's an obsession. We'd love to do the same for you.

OpenMarket
An infobip company