Call for Input response: Reducing mobile messaging scams. Evidence and options for addressing consumer harm

7th October 2024

Introduction

Twilio is a global Communications Platform as a Service (CPaaS) provider. Our CPaaS products allow customers to communicate with their customers over voice, messaging including SMS and RCS, and email with features that companies have added into applications across a range of industries, from financial services and retail to healthcare and non-profits.

Twilio Ireland Limited provides these services, including SMS and its recently launched RCS offering, within the UK as well as in other jurisdictions. In the UK, Twilio will typically procure capacity and services from mobile network operators (MNOs), resellers and other third-party providers, which we then package and integrate to provide to our customers to meet their business requirements (e.g. integration via Application Programming Interface (API) tools for messaging). Twilio is pleased to help our UK business customers including Marks & Spencer, Oxfam, and Deliveroo better connect with their customers.

Twilio recognises the importance of addressing the risks and harms caused by scam and fraud messaging for UK consumers and other stakeholders alike. It is an issue which we deal with and combat on a regular basis, and we have implemented solutions to do so. We are keen to work collaboratively and to assist Ofcom in fulfilling its statutory duties, including identifying and implementing solutions which aim to address the harms caused by mobile messaging scams.

The RCS and SMS Messaging Market — SMS Remains the Default

Twilio operates both RCS and SMS services in the UK, with each offering distinct value for our customers. The RCS product has only recently been launched in the UK. Worldwide, RCS is currently mostly driven by Google, and adoption remains limited but is expected to grow rapidly. The popularity of RCS is increasing, and with RCS messages able to be sent to Apple devices adoption will be even further increased. As older devices are phased out and replaced through regular upgrade cycles, RCS penetration will naturally grow. Unlike third-party messaging apps that require downloads, RCS is natively integrated into the

device's messaging app, making it more accessible and likely to become the default messaging protocol over time.

Twilio sees that our RCS messaging provision can increase value to UK businesses by offering branded and verified messages that instil trust with end-users. RCS enhances traditional messaging by introducing branded sender identification in end-users' default messaging app, ensuring that end-users can immediately recognize and trust the source of their incoming messages. Twilio's RCS features include the incorporation of business logos, tagline, business name, trusted sender verification by Google, and read receipts to ensure that customers know who they are communicating with. We have not observed any scam or spam in RCS A2P messaging in the UK; however, the ecosystem is fairly nascent and the channel was only recently made available in the UK within our products.

However, it is important to note that RCS will not replace SMS. SMS is a trusted channel for businesses and consumers alike, providing solutions for different use cases in the marketplace. While SMS remains a vital tool for many use cases, RCS A2P provides a standardised, feature-rich platform that bridges the gap between traditional messaging and the interactive experiences offered by over-the-top (OTT) channels like WhatsApp.

RCS

Twilio believes that Ofcom has listed the main methods used by scammers using mobile messaging services. We would however put a slightly different emphasis on the gravity of the issue given the different technologies. While RCS offers certain security options, SMS is still often the go-to technology in the absence of widespread availability of RCS and it is important not to lose sight hereof. RCS P2P channels are particularly vulnerable to scammers as messages are not branded and are instead represented by a phone number. RCS is also only effective as long as there are strong and sensible Know Your Customer (KYC) processes in place and measures to prevent account takeovers.

Ofcom should be aware of the potential for scammers to use features not available to SMS users to inform and enhance their number targeting activities, more easily allowing those operating bulk scam messaging schemes to differentiate between active and inactive

numbers. Use of monitoring tools, which can be effective in filtering out SMS scam messages, will be limited due to RCS encryption.

RCS A2P Channels Can Help Build Consumer Trust

RCS for P2P and A2P are effectively two different channels. P2P is phone number-based and tied to a SIM card, while A2P is not represented by a phone number nor does it have a SIM card prerequisite. Businesses using RCS are represented by an AgentID, and agents must go through a KYC process. At this time, that KYC process is typically controlled and defined on an individualised basis by carriers. A2P messages using RCS have a statement that says they are vetted by the respective carrier — we believe this is done at the appropriate level/actor in the value chain.

Sensible KYC measures are effective in mitigating fraud on A2P channels. Twilio has raised concerns in other fora about disparate KYC formats and requirements across countries and regulatory regimes, as well as disparate documentation requirements for operators. KYC requirements should be digitally-based instead of relying on biometric documentation that cannot be easily provided or verified for a legal entity. Operators should be given the flexibility to use in-house or external products or services, including commercially available solutions, that provide KYC cross-checks within statistically acceptable boundaries of accuracy. Twilio encourages all participants in the RCS ecosystem to engage in constructive dialogue to develop harmonised standards and approaches for KYC vetting.

However, despite checks from multiple actors in the ecosystem (e.g. MNOs, aggregators), fraudsters can still misrepresent their brand or affiliation. This is why a whole-ecosystem approach to combating fraud is necessary that includes global engagement from law enforcement to target scammers at the source.

RCS P2P Channels Remain the Largest Risk

RCS P2P channels remain at a substantial risk for fraud because of the lack of KYC checks and lack of recognized branding commonly associated with A2P RCS channels. Ineffective or incomplete KYC checks by larger platform providers could also lead to increases in scam

messages. Given these factors, we expect that P2P will continue to be the channel that is more likely to attract fraud.

As RCS is still a nascent service, any assessment of the scale of scam messages sent over RCS, compared to SMS, should take into account the quantity of scam messages received by users relative to the total traffic across the two services. The potential for underreporting of scam messages on RCS can be further complicated by encryption. Account takeover for RCS also has a higher potential for impact because the fraudster's message is branded with a badge saying they were vetted by the relevant carrier which directly impacts consumer trust.

Moreover, consumers and businesses need to benefit from competition and multiple choices, and it will be crucial to maintain competition to ensure a healthy and innovative messaging ecosystem where both RCS and SMS can be used as trusted methods of communication. As we detail further in this response, there are effective tools available and in place to combat SMS scams. There is a vibrant and legitimate place for both types of messaging for consumers and businesses, and this should not be prejudiced by asymmetric regulation.

Industry-led SMS Solutions Should Continue

Twilio notes the range of measures set out by Ofcom as possibilities for tackling SMS scam messaging on P2P channels. Ongoing efforts to continue to secure SMS against scammers should be part of the agenda, and complement broader efforts to continue cross-industry action on scams.

Twilio has engaged with the Government to put forward industry-led solutions, including participating in the working group started by the previous government on an updated voluntary Telecommunications Fraud Charter, and Twilio is eager for that work to continue in the fight against fraud. As a B2B provider without direct consumer relationships, we welcome an increased focus on consumer education and reporting from the wider telecoms industry and Government where they are better placed to do so, including through the 'Stop! Think Fraud' campaign launched earlier this year.

Twilio recognizes that SMS Pumping Fraud (also known as Artificially Inflated Traffic), is a growing concern for our business customers. In this scheme, attackers exploit mobile numbers in apps and websites to redirect SMS codes or links, profiting from the revenue generated from the fraud. Businesses, regardless of size, suffer revenue loss, loss of trust and resource strain due to this complex issue.

In response, Twilio launched Verify Fraud Guard, which applies Machine Learning (ML) to block SMS OTPs from being sent to certain users. Between June 2022–July 2024, Fraud Guard successfully blocked 489 million fraudulent activities and saved customers $55.8 million in costs associated with SMS Pumping Fraud.

Twilio also offers a SMS Pumping Risk Score that allows our customers to get real-time risk assessment on a phone number's involvement in SMS Pumping Fraud. It uses a proprietary risk model that leverages data signals associated with this type of fraud including risky operators, anomalous SMS traffic patterns, and low conversion rates. To raise customer awareness, we also offer a fraud calculator to help businesses understand the cost to them of SMS Pumping Fraud.

Twilio has developed a limited release SIM swap security feature that we are evaluating for general availability. This tool is designed to help to stop fraud and account takeovers with timestamps and dates of any SIM changes, with a configurable risk tolerance that enables accurate modelling and metrics.

Measures to Foster SMS Trust

Below Twilio suggests measures for disrupting mobile messaging scams but, in general, Twilio would like Ofcom to consider how responsibilities are distributed across the value chain. As a general principle, the provider best placed to manage and most effectively implement the responsibility of the relevant solution and means of intervention to address the harm, should be considered in regard to their relationship with the potential victim of scams, their access to relevant data, and their ability to intervene and break links within the fraud chain.

Any interventions should avoid being: (i) disproportionate, relative to the level of harm and risk; (ii) overly burdensome, where more cost-effective solutions are available; and (iii) overly restrictive, where they may result in a greater increase in false positives, relative to the volume of scam messages identified and prevented.

SIM-based Measures

On SIM Farms, Twilio supports the Government's previous draft proposals to ban SIM Farms and would like to see this extended to SIM Blasters, as these technologies perpetuate scam traffic generation without legitimate business use cases.

Twilio agrees with Ofcom's finding that scammers who exploit P2P messaging often rely on SIM Farms, and Twilio has supported the banning of SIM Farms in response to the previous Government's Fraud Strategy. However, we had urged the government to avoid expanding the definition to virtual alternatives where the current technologies are still evolving, as it may inadvertently cause technologies with overwhelmingly legitimate business use to fall into scope.

In relation to Ofcom's consideration of volume limits on SIM card packages, Twilio acknowledges that the CFI already notes that all MNOs have volume limits in place for some contracts. Twilio's view is that relevant volume limits are a matter for MNOs and that the introduction of regulation in this area risks being too blunt a tool.

KYC/KYT Harmonisation

Twilio also implements robust Know Your Customer (KYC) and Know Your Traffic (KYT) measures to prevent scams and build consumer trust. Twilio institutes KYC checks in the UK through Regulatory Compliance (RC) bundles, requiring customers to provide compliance information directly to Twilio for verification. Twilio has integrated with industry recognized fraud and KYC vendors to verify customer identity as part of our KYC and KYT processes, including leveraging device fingerprints and payment information to prevent bad actors from creating accounts on our platform.

Sensible and workable harmonised rules and registry requirements for KYC/KYT are key to enabling a global solution. This will benefit businesses and consumers alike while allowing small and medium-sized providers to compete in the marketplace. It should not be left solely to larger players to set individualised requirements with little or no recourse for other actors in the value chain.

Harmonisation is important for requirements and reporting across the UK with both government and operators, and to align with sensible regimes proposed in the EU, such as Ireland's SenderID registry. A harmonisation of KYC rules for numbers and for SMS Sender IDs, or at least a list of the maximum number of requirements that can be asked for each, would allow for a more centralised regime of customer verification.

For KYC to be most effective, those closest to the customers are best positioned to carry out the most extensive checks. Twilio carries out KYC for long codes and we encourage others to do so.

Improved SenderID Registries

Twilio urges Ofcom to ensure that Tier 1 aggregators such as Twilio are given the tools they need as a key part of the A2P ecosystem in order to continue to address scams. One route that will continue to be important for the perpetration of mobile messaging scams is unreliable SenderID management.

On SenderID, aggregators need to be able to arrange and manage alphanumeric SenderIDs on behalf of customers, as well as make their own alphanumeric SenderID available to customers, on the same conditions as MNOs and mobile service providers. The best way to ensure this is for Ofcom to operate any future UK SenderID registry (rather than an industry body, and certainly as opposed to the system being controlled by just the MNOs), and act as a national regulatory authority for SMS SenderID. The process initiated by ComReg in Ireland may serve as a useful reference in this regard, and could be a sensible model for adoption in the UK and EU.

Twilio is concerned about the continued use of the MEF's SenderID registry, which has experienced limited adoption due to the cumbersome process of the registry that further limits its use by small and medium sized companies. Clarity is needed on how Sender IDs could be registered in a way which does not introduce burdensome and costly compliance hurdles for business, and how the current competing registration approaches — for instance those of MEF and carriers — would be reconciled.

A harmonised industry and regulatory approach to SenderID has the potential to create benefits for both businesses and consumers. In order to ensure continued competition in the marketplace, registry requirements should be standardised across both industry (the operators) but also regulatory regimes. Twilio also cautions against relying on tools such as whitelisting, due to their limited scope and compliance burdens for smaller operators, without significant benefit to the consumer.

We continue to welcome Ofcom's recognition of voluntary industry measures and agreements where appropriate, and we believe the government should refrain from interfering in contractual obligations, particularly where existing contract measures have successfully reduced incidents of fraud. A national regulatory authority for SMS SenderID would be helpful.

Solutions to Detect Fraud

As part of Know Your Traffic (KYT), Twilio uses both in-house and third-party account and messaging traffic monitoring tools to detect suspicious behaviour and block malicious traffic destined to UK mobile subscribers as well as a global team staffed to monitor traffic on our platform.

Twilio's message filtering tools incorporate advanced machine learning (ML) systems and lists of prohibited terms to identify and block suspicious text messages. Twilio has also built an internal tool, the "ATOnator," which uses advanced ML to identify account takeovers and prevent compromised accounts from sending traffic over Twilio's network, forcing account sanitization before it can be re-enabled. This tool has been successful in detecting account takeovers at launch, with the latest version of the tool leading to a 300% increase in the

detection of compromised accounts on the network. The increased efficacy of this tool would not have been possible without leveraging the latest in ML/AI technology.

Twilio has built an in-house ML algorithm designed to quickly detect and shut down accounts that have been compromised and to force account sanitization before the account is re-enabled. Twilio is also integrated with third-party vetting services that leverage device fingerprints and payment information to prevent bad actors from creating accounts on our platform.

This ability to filter for scam and fraud content can be an effective solution in the toolbox to combat fraud. However, industry needs further assurances from regulators that any efforts to reduce fraud won't be penalised on privacy grounds. This is an area where further clarity may be helpful.

Improving Inter-Industry Cooperation

In addition to the above, as the Government has recognised in its recent work on fraud, there are opportunities for industry across all sectors to address fraud more effectively – including social media companies, telecommunications, and payment service providers – to work together.[1]

Twilio works to combat fraud as a member of i3Forum, an industry body working with national regulatory authorities to tackle unwanted communications. The group launched the Restore Trust Initiative in 2023, a project aimed at restoring trust in international communications and bridging the gap between regulators and industry, and has made strong progress thus far in building industry and regulatory discussions.

[1] As the Home Office notes, overall fraud has decreased by 13% since the launch of the Fraud Strategy in May 2023 (Home Office, 2024) in the context of rising levels of fraud due to non-messaging sources. For instance, UK Finance found that financial APP fraud predominantly starts online, with 76% of APP fraud originating online (compared to 16% starting through telecommunications networks) — up from 70% in 2020 (UK Finance, 2021/2024). The Financial Ombudsman Service also indicated that it had seen a significant rise in complaints where fraud has originated on social media (Financial Ombudsman Service, 2024).

Prioritising harmonisation and clarity on requirements would make it easier for all actors in the ecosystem to participate, such as creating the appropriate data sharing framework, as fraud increasingly originates online. Fostering shared knowledge between industries on the sources and content of scams has the potential to allow for more frequent anti-scam measures, such as URL blocking and social media content takedowns, tackling scammers at source and increasing law enforcement.