



Market Insight Report Reprint

Trusted Communications Emerge as a Critical Requirement for Digital Customer Experience

February 22 2023

by **Raul Castanon-Martinez**

The growing adoption of mobile communications and digital channels for customer engagement have led to an increase in abusive and fraudulent practices, including robocalls, spam SMS and artificially inflated traffic. We examine the implications these can have for enterprises, mobile network operators and the customer experience.

451 Research

S&P Global

Market Intelligence

This report, licensed to Infobip, developed and as provided by S&P Global Market Intelligence (S&P), was published as part of S&P's syndicated market insight subscription service. It shall be owned in its entirety by S&P. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from S&P.

Introduction

In December 2022, the U.S. Federal Communications Commission — which regulates interstate and international communications by radio, television, wire, satellite and cable in the U.S. — proposed a \$300 million fine over an alleged auto warranty robocall scam. The scheme, involving more than five billion unsolicited calls to more than 550 million wireless and residential phones between January and March 2021, is the largest robocall operation the FCC has ever investigated. The incident illustrates the growing problem of abusive and fraudulent practices such as robocalls and spam SMS, which according to the FCC are the commission's top consumer complaint.

The misuse of mobile communications and digital channels can have numerous implications that go beyond annoying messages and phone calls that consumers have to put up with. In addition to negatively impacting a brand's reputation, they can result in account takeover and identity theft. Here, we look at threats that have emerged with the growing use of mobile communications — namely robocalls, spam SMS and artificially inflated traffic — and the implications these threats can have.

THE TAKE

The use of mobile communications and digital channels for customer engagement has brought with it a growth in fraudulent activity leveraging these channels, with numerous implications for enterprise organizations, mobile network operators (MNOs) and the customer experience (CX). For consumers, this can range from annoying messages and phone calls to fraudulent transactions that seek to steal their money or identity. For organizations, this can result in consumers ignoring legitimate calls and messages containing alerts and other important notifications, leading to costly follow-up calls. For MNOs, this results in lost revenue due to reduced call completion rates; they also incur significant costs from investigating and resolving customer complaints. These factors highlight the relevance that trusted communications have as a critical requirement for enabling the digital customer experience, and the need for joint efforts across the entire ecosystem, including enterprise organizations, MNOs, communications PaaS providers and CX technology vendors.

The use of mobile A2P communications continues to grow

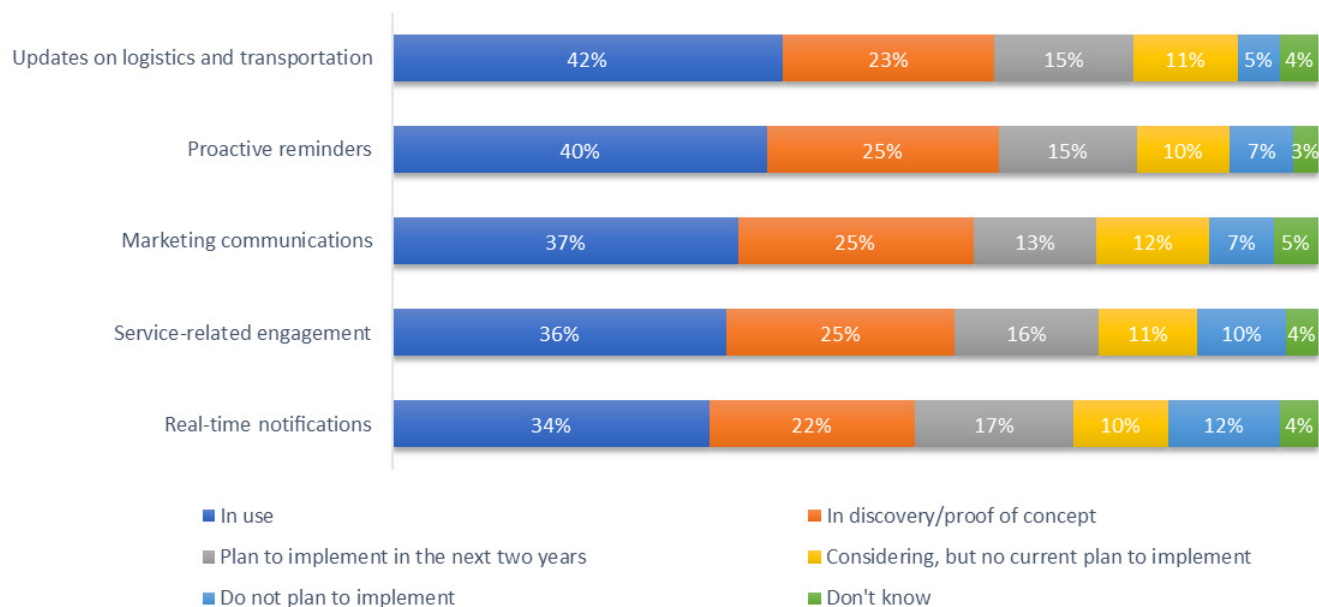
The use of mobile communications and digital channels enabling the digitization of the customer and employee experiences accelerated in the wake of COVID-19. According to 451 Research's Voice of the Enterprise: Workforce Productivity & Collaboration, Technology Ecosystems 2022 survey, organizations are increasingly relying on mobile application-to-person (A2P) communications for numerous use cases.

Typical customer-engagement use cases leveraging real-time, mobile communications include:

- Real-time notifications (e.g., order status, appointment reminders, bank alerts).
- Multifactor authentication via SMS or phone call.
- Banking use cases (e.g., transaction confirmations, alerts, transaction status).
- Ability to change appointments, re-route package delivery or service-related engagement via mobile phone.
- Marketing communications for customer engagement (e.g., loyalty programs and promotional offers).
- Proactive reminders (e.g., repair service alerts, health reminders or home alarm notifications) via connected devices.
- Updates on logistics and transportation (e.g., driver/rider communication for ride-hailing applications, delivery updates for food/grocery).

Our research shows that use of mobile A2P communications will likely continue to grow. For instance, 65% of survey respondents say their organization has deployed mobile A2P communications either in production (42%) or in proof of concept (23%) to provide logistics and transportation updates to their customers (Figure 1), with other use cases following a similar pattern.

Figure 1: Use Cases for Real-Time Mobile Communications for Customer Engagement



Q. What is the state of current enterprise investment in each of the following tools used to communicate to your customers?

Base: All respondents (n = 480).






Source: 451 Research's Voice of the Enterprise: Workforce Productivity & Collaboration, Technology Ecosystems 2022.

Key issues that enterprises should be aware of

Consumers are mostly familiar with spam, robocalls and phishing messages, which have significantly increased over the past two years. In general terms, spam refers to unsolicited messages sent over various channels. This includes bulk unsolicited campaigns, which are generic and not specifically targeted at an individual, with the aim of initiating communication — typically impacting subscribers more than enterprises. A second type includes campaigns targeting specific customers to collect sensitive information, incur costs or spread malware. Known as phishing, it can be considered a subset of spam, as well as a separate fraud category, and can impact subscribers and an organization's reputation.

Other emerging threats include smishing and artificially inflated traffic, which can have numerous implications for consumers, enterprise organizations, MNOs, and CPaaS and CX technology vendors (Figure 2).

Figure 2: Fraud Use Cases for Real-Time, Mobile Communications

	Terminology	Affected parties	Description
	Phishing	Consumers, enterprises	Socially engineered email attacks exposing users to dangerous websites, malware, or data collection
	Spear phishing	Enterprises	Socially engineered email attacks targeting selected individuals within an organization.
	SMS Traffic Pumping Fraud	MNOs, enterprises	Driving revenue for SMS service providers and MNOs through the generation of fake traffic.
	Smishing	Consumers, MNOs	Socially engineered attack that uses SMS as the main communication vector.
	Vishing	Consumers, enterprises, MNOs	Socially engineered attack that uses phone calls or voice messages to lure targets.
	Whaling	Enterprises	Attacks targeting high-value individuals within an organization, such as top executives.

Source: 451 Research

Smishing

While robocalls and spam SMS can be considered an annoyance for mobile users, smishing — a portmanteau of SMS and phishing — can have significant financial implications for consumers and enterprises. The term refers to a social engineering attack that relies on fake text messages to trick people into downloading malware, sharing sensitive information or sending money to cybercriminals. Fraudsters will try to impersonate brands and copy their websites and processes, making it easy for mobile users to confuse the fraudulent communications with those sent by an authentic brand. Typical examples include delivery scams, where fraudsters mimic a logistics company's processes, tricking consumers into clicking through websites that seem valid to collect their personal information.

SMS attacks include high-profile incidents such as FluBot, an SMS banking Trojan designed to steal private data from Android smartphones. The malware masqueraded as an innocuous message — such as a missed call or delivery — asking the receiver to click on a link. First spotted in December 2020, it gained traction in 2021, compromising a significant number of devices worldwide. In May 2022, FluBot infrastructure was taken down in an operation involving 11 countries; it is not expected to resurge.

Artificially inflated traffic

Also known as SMS traffic pumping fraud, the term refers to the generation of fake traffic from legitimate websites and applications with the intent of driving revenue for SMS providers and MNOs. It happens when fraudsters take advantage of a phone number input field to receive a one-time passcode, an app download link or anything else via SMS.

Fraudsters will then use a bot to repeat the process, generating SMS messages to thousands of numbers. This is fake traffic that businesses are compelled to pay for, but is not converted into real business. Unfortunately, by the time an organization detects the fraud — typically by noticing an increase in signups from new countries, a sudden decrease in conversion rate, or a high number of signups from the same IP address or within a limited range of mobile numbers — it is already too late.

Implications for MNOs

Robocalls, spam SMS, smishing and artificially inflated traffic can have significant financial implications for MNOs. If MNOs are not securing the ecosystem or are involving providers that do not have high security standards (whether intentionally or unintentionally), they could be jeopardizing the security of their end users. The same holds true for enterprises, who might place their customers at risk and open the possibility for different frauds or privacy issues if they choose to use less expensive options for A2P and P2P communications in order to reduce costs.

Gray route providers typically do not have the infrastructure to handle sensitive content as they are not operating legitimately, so there is no incentive for them to invest in the security aspects of their platforms. With platforms that are not securely handling A2P traffic, there is a whole spectrum of opportunities for fraudsters to intercept A2P traffic or perform different fraudulent attacks on the end customers.

CONTACTS

The Americas

+1 877 863 1306

market.intelligence@spglobal.com

Europe, Middle East & Africa

+44 20 7176 1234

market.intelligence@spglobal.com

Asia-Pacific

+852 2533 3565

market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

Copyright © 2023 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON “AS IS” BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT’S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence’s opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global’s public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.