MEF

MOBILE MESSAGING FRAUD REPORT 2016

GLOBAL INSIGHTS INTO FRAUD IN CHAT APPS & SMS

CONSUMER & ENTERPRISE TRENDS

🇧🇷 🇨🇳 🇩🇪 🇫🇷 🇬🇧 🇮🇳 🇳🇬 🇿🇦 🇺🇸

A NINE-COUNTRY STUDY

MEF MOBILE ECOSYSTEM FORUM

IN ASSOCIATION WITH CLX

FOREWORD

This report forms the next instalment of the continued collaboration between Mblox, now CLX Communications and MEF on better understanding the use of mobile messaging globally. It provides a remarkable update on how the messaging ecosystem is evolving and how some newer mobile messaging channels are increasingly being polluted by unsolicited and fraudulent messages.

It's interesting to note that although the SMS channel receives the highest daily occurrence of unsolicited messages it remains the most trusted. This is likely because the percentage of spam messages is still a tiny fraction at less than one per cent overall. When compared to the nearly 50 per cent on email, SMS is still a clean and powerful channel. It's extremely surprising that over-the-top messaging apps only lag SMS by two per cent in daily occurrence, yet SMS is by far more ubiquitous and open.

In our experience we have always seen a high correlation between the cost to deliver a message and the amount of spam and fraud the channel attracts. It could be argued that the reason for low levels of spam in Germany and France is directly related to:

a) The cost to send a message through legitimate routes is relatively high in those countries
b) The effectiveness of local operators in those countries to block fraudulent routes into their networks and filter spam is very good.

By contrast India, Nigeria and South Africa have a cost for sending a message that is relatively low, and although things are improving rapidly these networks have historically been less protected. It is also true that in many of these mobile first countries consumers are less likely to have email addresses and SMS therefore acts as a substitute for email marketing.

Cost, (or lack of it) may be the reason why 72 per cent of users have received unsolicited messages on over-the-top (OTT) messaging apps such as Whatsapp etc. yet no official API exists for sending enterprise-to-consumer messages on many of these platforms yet. This is concerning as it indicates that fraudsters are using weaknesses in the person-to-person capabilities of these apps to send messages on behalf of enterprises.

These apps will need to tread carefully when they do decide to open their apps up to legitimate enterprise communications. They would not want to replicate the fate of push notifications, where overzealous marketers have caused this channel to be only trusted by 16 per cent of people according to the report.

It could be argued that the reason why most people in the UK report unsolicited SMS messages is because the mobile operators have done a good job at collaborating on creating a cross operator shortcode (7726) that can be used to report such messages. In addition, there is a perception that regulators in the UK and the USA will prosecute offenders, which is not always the case in other mobile first countries.

In our view there are a number of things that can be done in order to reduce fraud and spam across all channels:

1. Create a global shortcode, long number or email that can be used to report unsolicited messages. The easier we make it, the more people will do it. Ensure these reports are shared across the eco-system in an automated way so they can be acted on by key players.

2. Operators must continue to install SMS and SS7 firewalls into their networks to prevent grey and fraudulent routes from being exploited and used for sending spam and phishing messages.

3. OTT messaging apps must close holes in their systems that allow individual user accounts to send large amounts of unsolicited marketing messages undetected.

4. When OTT messaging apps finally allow for sanctioned enterprise-to-consumer messages to be sent legitimately via an API, they must seriously consider charging something meaningful to deliver the message so as to ensure that both fraudsters and overzealous marketers do not abuse the channel.

5. Cloud communication providers like us must innovate and implement better ways validate the identity of companies to ensure that phishing attempts are thwarted early and often.

All of the above recommendations will be presented and discussed at the MEF Future of Messaging Programme with the intention of getting adoption across the ecosystem and driving real change to protect and improve the consumer experience of mobile messaging.

ROBERT GERSTMANN
MANAGING DIRECTOR

CLX COMMUNICATIONS

EXECUTIVE SUMMARY

Mobile messaging in all its forms is brilliantly effective. There's no technical barrier: no one needs a lesson to understand how SMS works. And it's highly personal too, meaning people open texts and app messages faster than other media, and responded to them more frequently. Consumers and enterprises know this. It's why they have embraced messaging so enthusiastically.

Regrettably, fraudsters know this too.

There's probably no greater indicator of the success of a communications channel than when the fraudsters arrive. Think about all those spam emails. Criminals wouldn't bother if email wasn't so popular.

Like email, mobile messaging between companies and people is very popular. MobileSquared says the market for 'application to person' (A2P) messaging is currently worth around $17 billion. Credence Research recently predicted enterprises would transmit two trillion messages a year by 2017.

These numbers make SMS an inevitable target for criminals. And now that millions are switching to messaging apps like WhatsApp, the fraudsters are inevitably active there too.

MEF estimates that fraud is costing the ecosystem at least $2 billion a year. Its industry working group identified 11 distinct fraud types and set up the Future of Messaging Programme to raise awareness and take action against all fraud types including the use of grey routes and SIM farms.

This study shows why industry action is so pressing. It reveals that 28 per cent of SMS users receive an unsolicited text message every day. 58 per cent receive at least one a week. Only 16 per cent have never received one. Within messaging apps, the fraud problem is currently less severe. But it's still serious: 26 per cent of chat app users receive an unsolicited text message every day, while 49 per cent receive at least one a week.

Of course, the malpractice varies in its severity. Many unsolicited text messages are merely a nuisance - alerting users to an unwanted offer or service. But others are criminal in intent. Fraud types include attacks such as 'phishing' messages, which aim to trick the recipient into disclosing personal data. The research reveals that 33 per cent of mobile users have received a text message of this type.

The problem is at its worst in emerging markets such as Brazil, China, South Africa and Nigeria. Indeed, while 31 per cent of Germans have never received a phishing text, in Nigeria it's just six per cent.

Malpractice erodes overall trust in mobile messaging and its effectiveness as a relationship building channel for enterprises. It also adds to a growing sense of suspicion among the public towards tech services. Consider the impact of the Snowdon relations and the game-changing introduction of ad-blocking.

The rise of Russia's Telegram app is another expression of this distrust. By focusing on privacy and security (encrypting its messages), the app has filled a market demand for privacy in chat. Telegram says it has attracted 100 million users with 'zero marketing budget'. It may even have inspired WhatsApp's decision to adopt end-to-end encryption this year.

This report lays bare the rising problem of mobile messaging fraud. It's not 'terminal' yet. In fact, the study found that people still trust text messaging more than chat apps even though fraud is higher on SMS. Clearly, the industry must be vigilant and ensure that this kernel of trust remains.

CONSUMER INSIGHTS

MORE THAN A QUARTER OF MOBILE USERS ARE SPAMMED EVERY DAY

PROBLEM IS WORSE ON SMS, BUT GROWING ON MESSAGING APPS

SMS is simple to use, well-understood by virtually all people, ubiquitous and affordable. That's why it's growing so fast as a business to consumer medium. Regrettably, the channel's many benefits have also attracted criminals, chancers and fraudsters.

The problem of text spam and phishing is widespread. The study reveals that 28% of SMS users receive an unsolicited text message every day. 58% receive at least one a week. Only 16% have never received one.

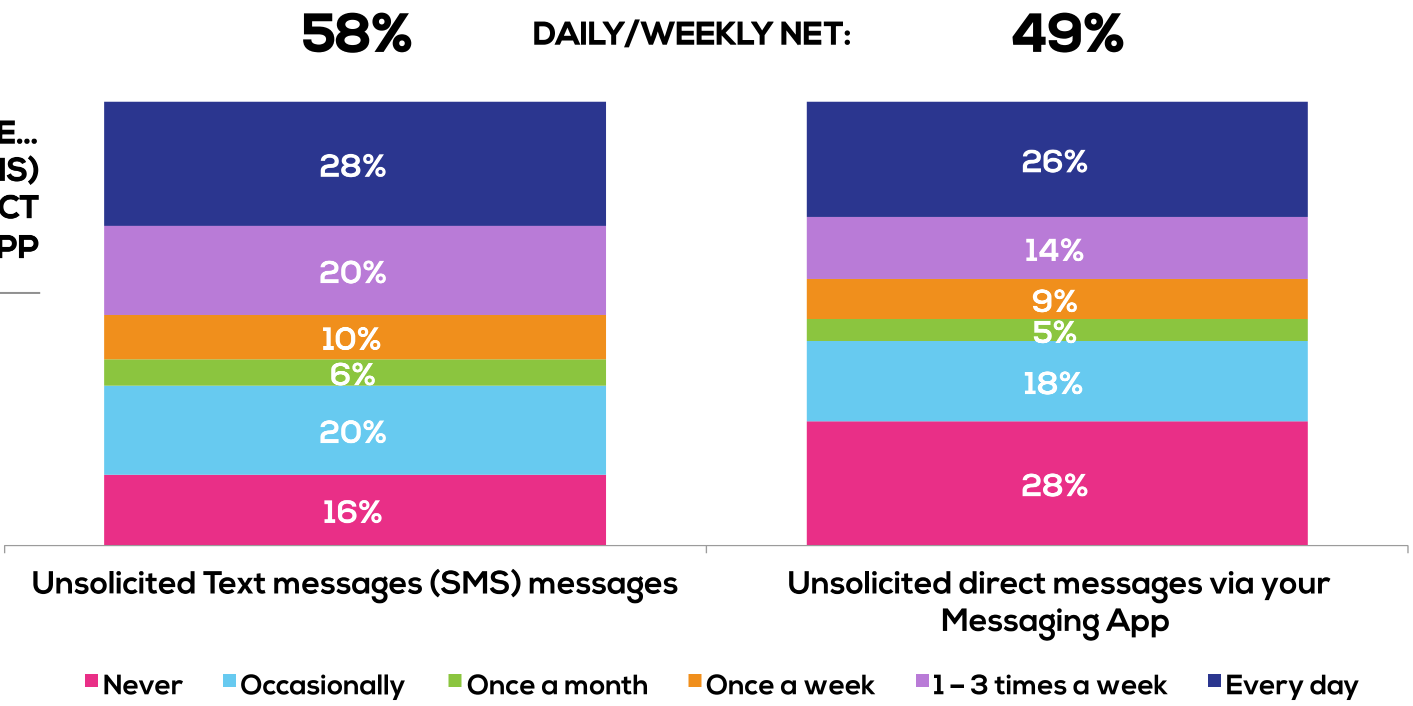
Within messaging apps, the problem is less severe - though not by much. This may be merely be a reflection of the fact that OTT apps are generally used less by enterprises to keep in touch with customers. Here, 26% of chat app users receive an unsolicited text message every day, while 49% receive at least one a week. 28% have never received one.

It's fair to conclude that the messaging app is already a polluted channel.

To repeat an earlier observation, the problem of unsolicited texts is worst in mobile-first economies. 73% of South Africans receive these texts at least once a week, and in Nigeria it's 76%. Those are the two highest rates in the world. And while 31% of Germans have never received a text of this type, in Nigeria it's just six%.

As part of its Mobile Messaging Programme: The Future of Messaging, MEF members defined 11 distinct fraud types and estimates that fraud is costing the ecosystem at least $2billion a year.

HOW OFTEN DO YOU RECEIVE... UNSOLICITED TEXT MESSAGES (SMS) MESSAGES/UNSOLICITED DIRECT MESSAGES VIA YOUR MESSAGING APP



A THIRD OF CONSUMERS HAVE RECEIVED A 'PHISHING' MESSAGE

AND TWO IN TEN ARE NOT SURE

While some unsolicited text messages are a nuisance, alerting users to an unwanted offer or service, others are more pernicious. These are 'phishing' messages, which purport to be from an official organisation in an attempt to dupe the user into revealing private information.

The research reveals that 33% of mobile users have received a text message from someone pretending to be someone they are not, and asking for personal account information or money. These messages can, of course, be very convincing which is why 21% reveal they are not sure if they have received one or not.

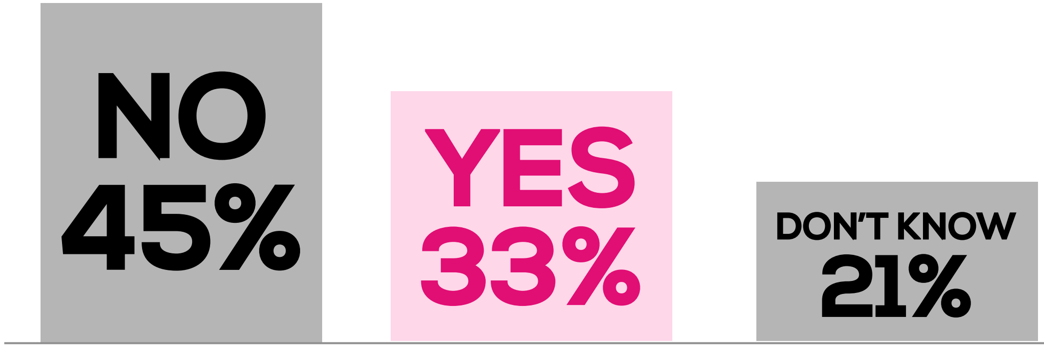
Phishing is an unfortunate result of the popularity and ubiquity of SMS - and also, perhaps, the 'taming' of the phenomenon on email. A report by Whitepages in 2015 revealed that email spam is at an all time low. It's still a big problem – 49.7% emails sent are junk. But that's the lowest percentage in over a decade.

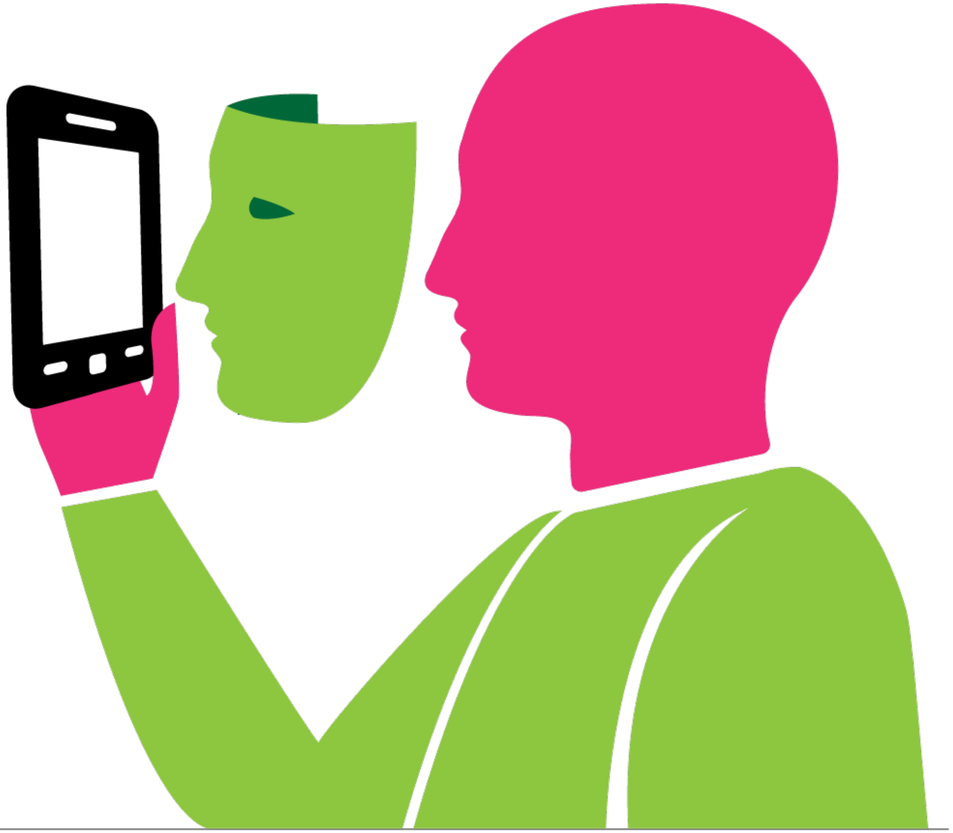
Spam filters and consumer awareness are helping to reduce email fraud, but this has caused fraudsters to turn their attention to SMS.

As elsewhere, the problem is at its most severe in Brazil, China, South Africa and Nigeria. Respectively, the number that have received a phishing text is 39%, 47%, 48% and 60%.

Users do not receive as many phishing messages on OTT apps. To repeat, this is probably because of the relative 'newness' of these media. That said 23% of people have received such a message to their app inboxes.

HAVE YOU EVER RECEIVED A TEXT MESSAGE (SMS) FROM SOMEONE PRETENDING TO BE SOMEONE THEY ARE NOT, E.G., YOUR BANK OR A COMPANY THAT YOU HAVE AN ONLINE ACCOUNT WITH, ASKING FOR PERSONAL ACCOUNT INFORMATION OR FOR MONEY?





SMS IS THE MOST TRUSTED MESSAGING PLATFORM

MORE THAN A THIRD TRUST IT - TWICE AS MUCH AS FACEBOOK, YAHOO AND SKYPE

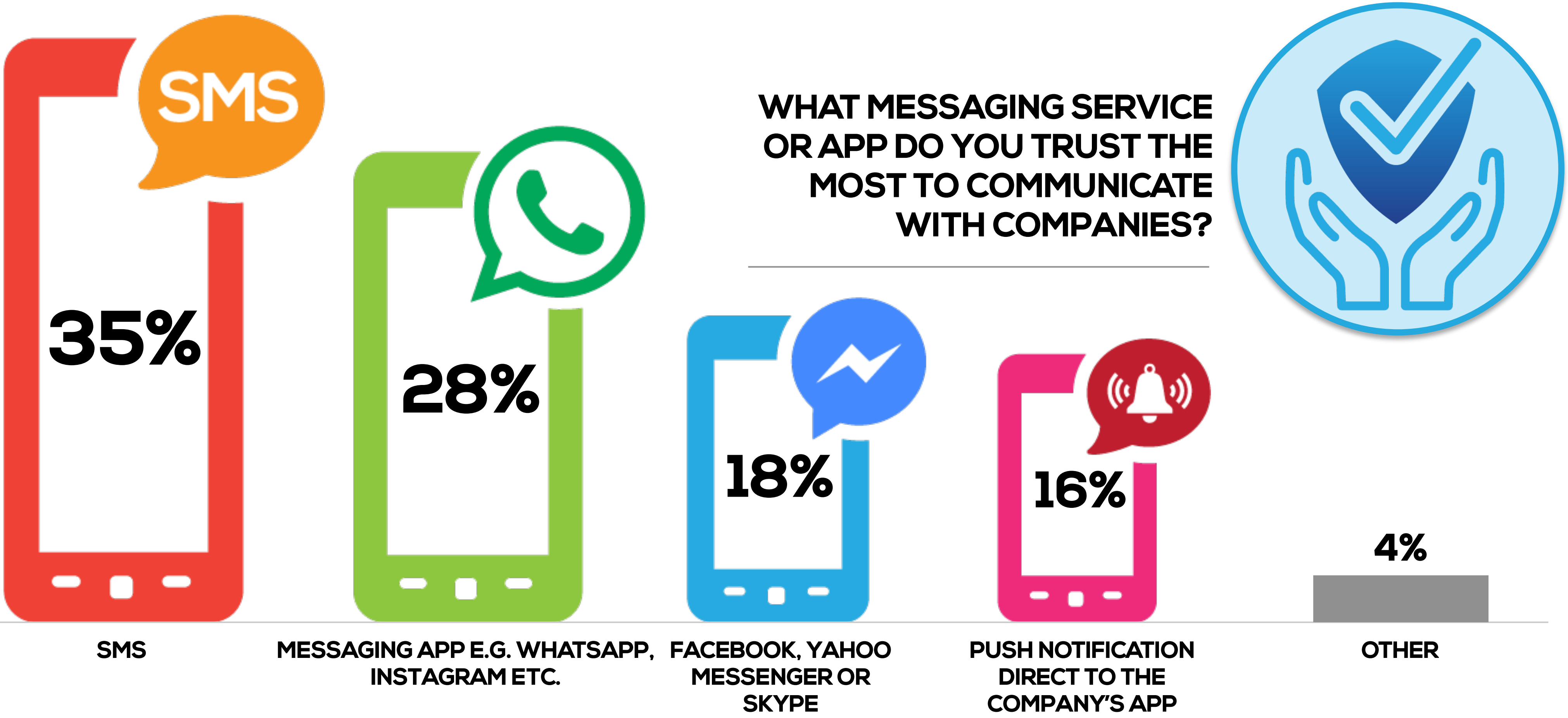
Despite the higher level of unsolicited message traffic on SMS, the research shows that people trust it more than other options. 35% said it was their most trusted channel.

28% trust messaging apps the most and 18% chose Facebook, Yahoo and Skype. It's difficult to guess why. It's possible that people view dedicated messaging apps like WhatsApp and Instagram in a favourable way to 'general' tech companies like Facebook, Yahoo and Skype. Maybe they believe the latter to have covert agendas.

This is supposition. And the irony, of course, is that Facebook owns both WhatsApp and Instagram.

The only countries to depart from a trust preference for SMS were Brazil and China, where messaging apps were more trusted (50% and 38% respectively). This is slightly odd given that these two regions are among the most affected by messaging app spam. But it's possible the immense overall popularity if WhatsApp (Brazil) and WeChat (China) in these countries leads to a favourable impression.

WHAT MESSAGING SERVICE OR APP DO YOU TRUST THE MOST TO COMMUNICATE WITH COMPANIES?



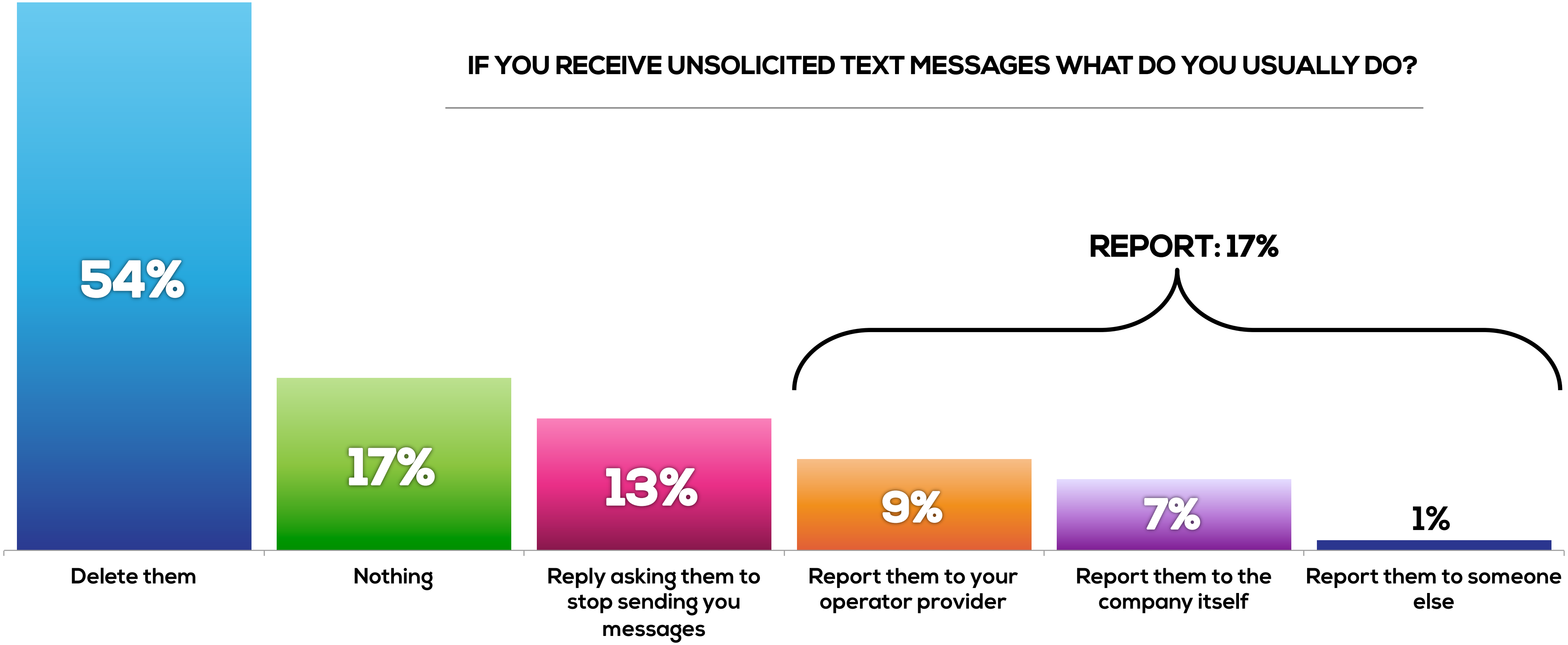
SEVEN IN TEN TAKE NO ACTION AGAINST UNWANTED TEXTS

THEY EITHER DELETE OR IGNORE THEM

It seems as if most people treat messaging spam as an unfortunate fact of life. The study shows that 54% delete unwanted messages and 17% ignore them. 13% reply with a ‘stop’ command while 17% report them.

The British (23%) and Germans (22%) are the most active in reporting unsolicited SMS. It’s difficult to pinpoint why - though one can assume that there is more consumer education and more regulatory activity in these markets than elsewhere.

Clearly, there is a lesson here for other countries if they are to reduce spam and encourage the idea that it is not inevitable.



ONE IN 30 PEOPLE USES TELEGRAM'S PRIVACY-CENTRIC APP

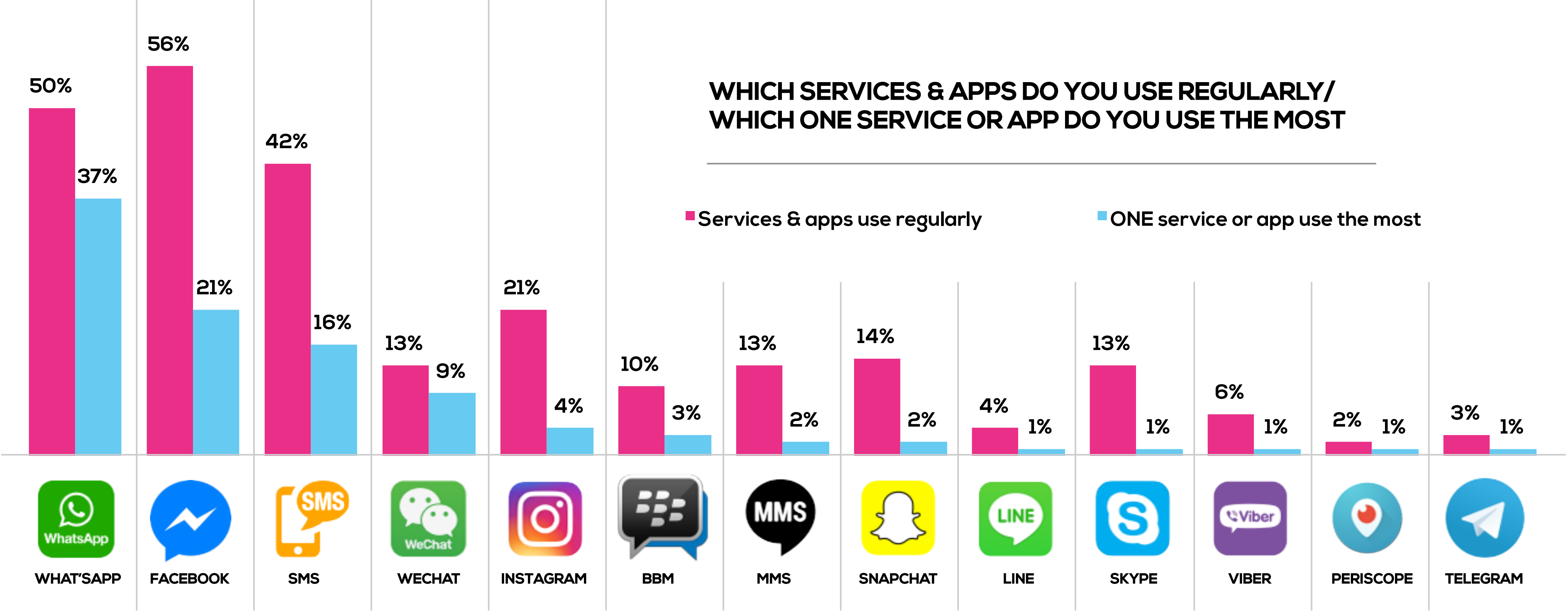
SECURITY-FIRST OPTION FINDS A WILLING USER BASE

Russia's Telegram app has established itself as one of the small number of genuinely global message apps. It's done so in just over two and a half years by focusing on a USP of privacy and security. According to our survey, three% of respondents use it regularly and one% use it most of all the apps.

Telegram confirmed at Mobile World Congress in February that it has 100 million monthly active users - an increase of 38 million new users since May 2015. It has users in 200 countries sending 15 billion messages daily.

To repeat, what's most interesting about these users is that they clearly choose Telegram solely for its focus on encryption. The app has a secret chat feature that makes it easy to delete messages or schedule a time for them to self-destruct. Telegram has clearly filled a market demand for privacy in apps. It says it achieved 100 million users with 'zero marketing budget'.

Since its announcement, it no longer has such a stranglehold on the encryption idea. In an update on March 31, WhatsApp enabled end-to-end encryption by default to its chat and call functionality. And in May, reports emerged suggesting Facebook is preparing to release an optional encrypted mode for its Messenger app.



THREE QUARTERS OF NIGERIANS RECEIVE UNSOLICITED TEXTS EVERY WEEK

ONLY 6% HAVE NEVER RECEIVED ONE

The problem of spam, phishing and other unwanted messages is growing – and it's worst of all in Nigeria. The research revealed that 47% of Nigerians receive an unwanted text every day, and 76 get one every week.

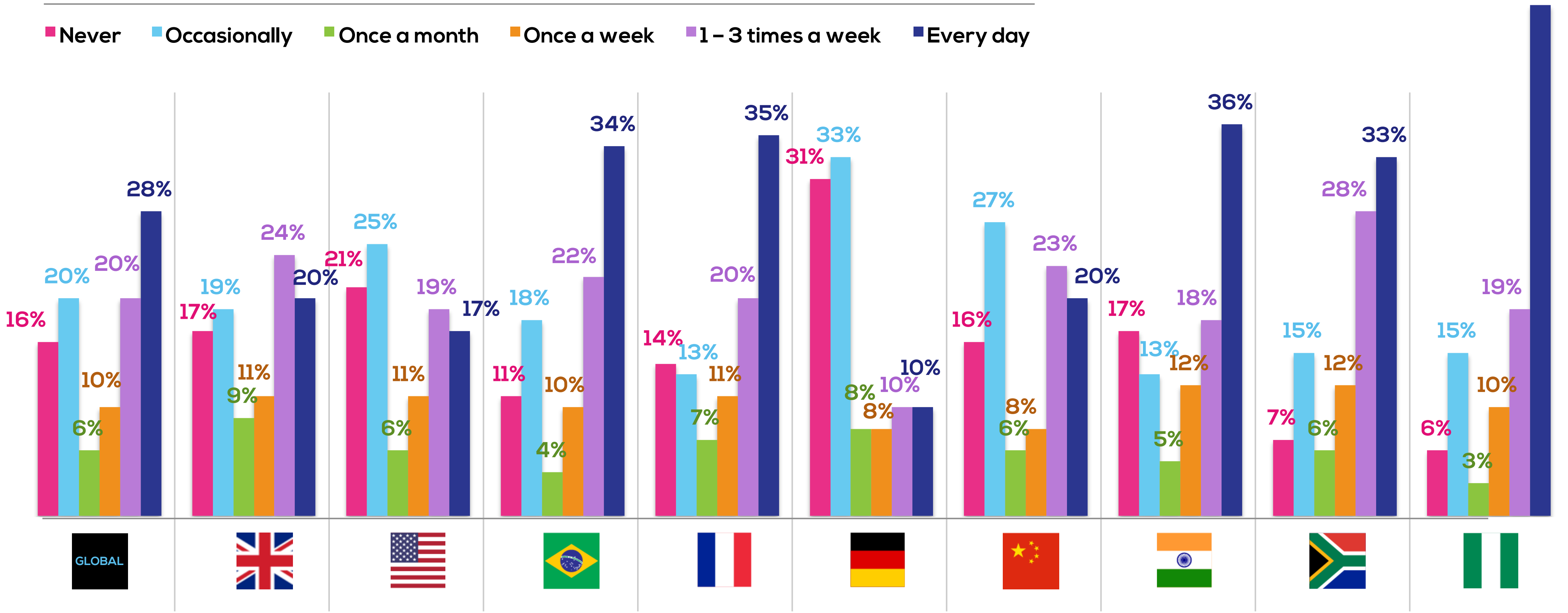
And it's the same story with messaging apps. Here, 63% of Nigerians receive unsolicited comms every week.

Regrettably, Nigeria also tops the poll when it comes to the most phishing. 60% of Nigerians say they have received a text from someone pretending to be someone else. Again, that's the highest figure in the survey.

One can assume that the high quantity of unwanted texts is a by-product of the generally high level of enterprise

Messaging in Nigeria. For example, 35% of Nigerians have used text to set up an account against the 17% global average.

HOW OFTEN DO YOU RECEIVE...UNSOLICITED TEXT MESSAGES (SMS) MESSAGES



BACK TO CONTENTS

MORE THAN HALF OF BRITISH MOBILE USERS REPORT UNWANTED TEXTS

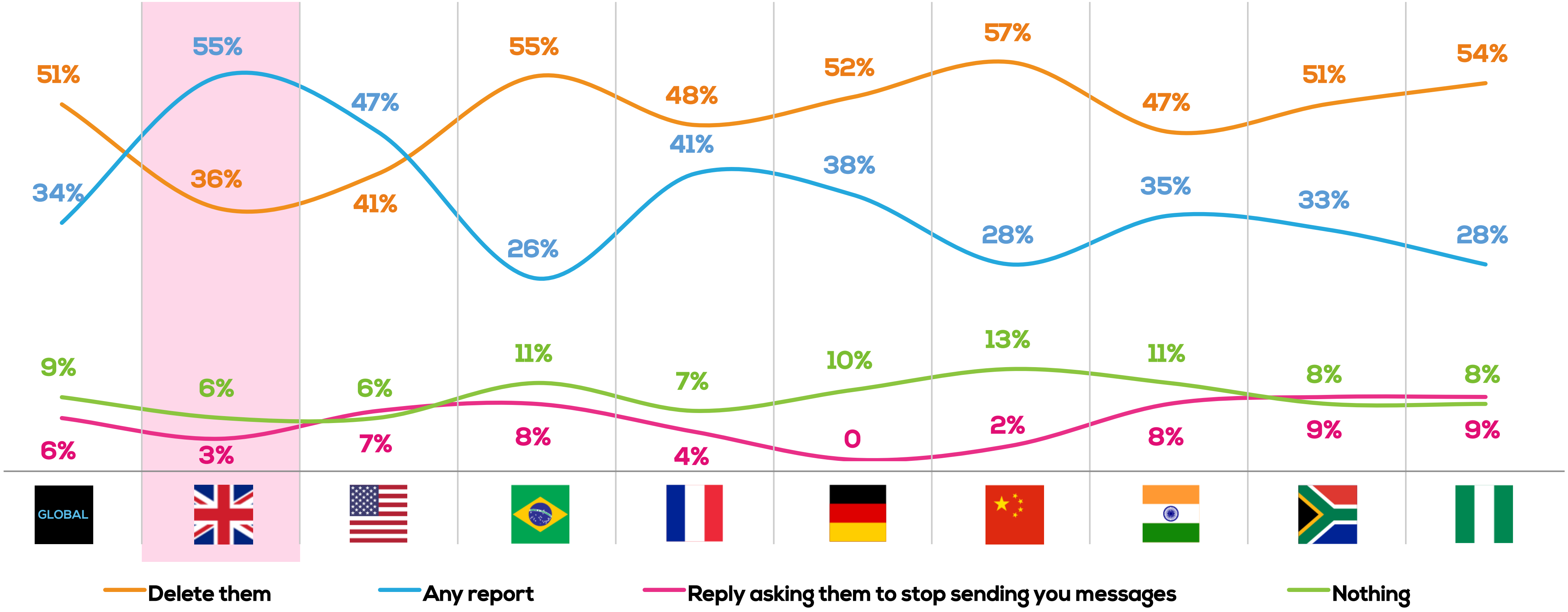
UK DOES MOST TO HIT BACK AT FRAUDSTERS

There are a handful of options available to anyone receive unwanted messages: delete, report, stop or unsubscribe, do nothing. Of all the countries in the study, only the UK does more reporting than deleting.

55% of Brits say they most often respond to fraudulent SMS messages by reporting them. 36% delete them. Meanwhile 36% delete them. Everywhere else, the preference is to delete.

The UK has a mature regulatory sector, which may explain this.

WHAT DO YOU USUALLY DO ABOUT THESE TEXT MESSAGES (SMS)?



ABOUT THE REPORT

ABOUT THE SURVEY

MEF’s Mobile Messaging Survey 2016 was commissioned by global trade body Mobile Ecosystem Forum.

The field study was carried out by On Device Research in Q2 2016. It questioned nearly 6000 mobile media users in 9 countries, namely: Brazil, China, France, Germany, India, Nigeria, South Africa, UK and US.

The study digs deep into consumer trends and attitudes, providing insight and analysis on their wider industry impact. The report delivers insight that can help all stakeholders in the mobile ecosystem exploit the rich opportunities that mobile messaging provides.

QUESTIONNAIRE

- Which services & apps do you use regularly to send or receive direct messages on your mobile device (excluding email). Please tick all that apply
- Which ONE service or app do you use the most (select one) to send & receive direct messages on your mobile device (excluding email)
- In the last 12 months, have you received a text message (SMS) from the following companies or institutions? Please tick all that apply
- In the last 12 months, have you sent or received a message via one of your messaging apps to talk to the following companies or institutions? Please tick all that apply
- In the last 12 months have you sent a text message (SMS) to do the following? Please tick all that apply
- And in the last 12 months have you sent a message from one of your messaging apps to do the following? Please tick all that apply
- How do you most like to communicate with your….: Bank
- How do you most like to communicate with your….: Doctors / dentist / hospital or other healthcare provider
- How do you most like to communicate with your….: Retailer
- What messaging service or app do you trust the most to communicate with companies? (Select one)
- How often do you receive… Unsolicited Text messages (SMS) messages
- How often do you receive… Unsolicited direct messages via your Messaging App (e.g. WhatsApp)
- If you receive unsolicited text messages what do you usually do? Please tick one option that you do most often
- If you receive unsolicited direct messages from a Messaging App (e.g. WhatsApp) what do you usually do? Please tick one option that you do most often
- Have you ever acted on a message received from a company with an offer based on your physical location? E.g. get a free cake when you buy a coffee from a shop you are close to.
- Have you ever received a text message (SMS) from someone pretending to be someone they are not, e.g., your bank or a company that you have an online account with, asking for personal account information or for money?
- What do you usually do about these text messages (SMS)? Please tick one option that you do most often
- Have you ever received a direct message from your messaging app (e.g. WhatsApp) from someone pretending to be someone they are not, e.g., your bank or a company that you have an online account with, asking for personal account information or for money?
- What do you usually do about these messages that where sent to your messaging app (e.g. WhatsApp)? Please tick one option that you do most often

THANKS TO OUR PARTNERS

About CLX Communications

CLX Communications connects enterprises to people and things. We combine programmable API's and cloud computing with our unparalleled Tier 1 Super Network to make it easy for businesses to embed global communications, including voice, SMS and mobile data into their apps, business processes and IoT devices.

Our leading communications Platform-as-a-Service (CPaaS) delivers one of the highest service levels in the industry whilst processing more than 1 billion API calls per month across 6 continents. We provide services to 4 of the top 5 CPaaS companies, and 3 of the top 5 global internet brands with Tier 1 connectivity on which many of their services rely.

CLX Communications (publ) is listed on the Nasdaq in Stockholm.

About On Device Research

On Device Research is a research company that gathers responses on mobile devices - so far we've sent over 2.3 million surveys across 53 countries.

By conducting research on mobile phones and tablet computers we can reach consumers wherever they are, at any time and in any location.

Mobile research also brings fresh, instant responses that accurately capture consumers' feelings, thoughts and opinions.

For more information visit www.ondeviceresearch.com

MEF
MOBILE ECOSYSTEM FORUM

ABOUT MEF

The Mobile Ecosystem Forum is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. We provide our members with a global and cross-sector platform for networking, collaboration and advancing industry solutions. The goal is to accelerate the growth of a sustainable mobile ecosystem that drives inclusion for all and delivers trusted services that enrich the lives of consumers worldwide. Established in 2000 and headquartered in the UK, MEF has Regional Chapters across Africa, Asia, Europe, Middle East, North and Latin America.

The editorial and analysis in MEF’s Mobile Messaging Report 2016 contains references to third party products, services and metrics. This data is sourced by the author from official press material distributed by the companies concerned. Its inclusion does not represent a recommendation by the MEF or the authors of this report in anyway. All other trademarks are the property of their respective owners.