CONSUMERS INTERNATIONAL

COMING TOGETHER
FOR CHANGE

SOCIAL MEDIA SCAMS:

UNDERSTANDING THE CONSUMER EXPERIENCE TO CREATE A SAFER DIGITAL WORLD

MAY 2019

ABOUT US

Consumers International is the membership organisation for consumer groups around the world.

We believe in a world where everyone has access to safe and sustainable goods and services. We bring together over 200 member organisations in more than 100 countries to empower and champion the rights of consumers everywhere.

We are their voice in international policy-making forums and the global marketplace to ensure they are treated safely, fairly and honestly. We are resolutely independent, unconstrained by businesses or political parties.

We work in partnership and exercise our influence with integrity, tenacity and passion to deliver tangible results.

With thanks to the Public Authority of Consumer Protection in Oman, for supporting the delivery of this international research led by Consumers International.

Consumers International is a charity (No.1122155) and a not-for-profit company limited by guarantee (No. 04337865) registered in England and Wales.

CONTENTS

EXECUTIVE SUMMARY

Social media is a modern phenomenon, revolutionising the way that consumers seek information, communicate with one another and interact with businesses. There are three billion active users of social media[1], such as Facebook, Twitter, WhatsApp and Instagram, with numbers increasing at an estimated one million each day.

The widespread use of social media provides plentiful opportunities for criminals to connect with consumers and commit fraud, using a range of tactics. Scammers are constantly devising new and innovative ways to trick people out of money or harvest personal data, which can be used for financial gain. Social media scams have the potential to cause significant harm to consumers in terms of financial loss, emotional wellbeing and degradation of trust. Urgent action is needed to protect consumers and minimise detriment.

In the absence of consistent and comparable data at a global level, Consumers International undertook this pioneering study to better understand the consumer experience, identify good practice in tackling the issues and recommend solutions. We monitored public online conversations about social media scams in nine countries for two years, supplementing this with interviews of consumer protection and enforcement agencies about national trends. See 'Our Research' in Chapter 1 for more details.

Our findings suggest that the volume and impact of social media scams is increasing rapidly. Impostor scams - where criminals pose as authentic brands, authorities or friends to deceive victims - are most common, followed by e-commerce scams - where scammers fail to provide goods that consumers have bought, or send goods which are counterfeit or substandard quality.

It is clear that social media scams present complex challenges for consumers and those charged with protecting them. This report highlights the global nature of scams and suggests ways that all stakeholders in this diverse space - from consumer protection organisations to government agencies, industry and social media platforms - can work together to enhance safety and minimise harm.

> It is clear that social media scams present complex challenges for consumers and those charged with protecting them.

The key recommendations of this report are to: develop consistent rules for consumer protection; drive increased liability of social media platforms; define good practice for business; explore the potential of digital tools to detect fraud; facilitate consistent and effective reporting of social media scams; improve stakeholder cooperation; and raise consumer awareness.

[1] The Next Web, Number of social media users passes 3 billion with no signs of slowing, 7 Aug 2017

1. INTRODUCTION

Billions of consumers worldwide are active on social media. These platforms open up a wealth of opportunities for scammers to connect with consumers, and the potential for harm is immeasurable.

To effectively protect consumers against increasing threats from social media scams, it is essential that all stakeholders understand the issues and how to address them. But although evidence suggests that social media scams are on the rise, it is difficult to get accurate data about the scale of the problem, due to a number of factors. Evidence suggests that scams are severely underreported, which may be caused by consumers not realising that they have been the victim of a scam, feeling too embarrassed to report the crime, or simply not knowing who to contact. On a global level, data collection is carried out by a range of different organisations, using a variety of methods. This has resulted in fragmented and inconsistent data, which is impossible to compare.

To fill this critical information gap, Consumers International commissioned this qualitative research study, the first of its kind, to better understand the consumer experience of social media scams, identify trends, assess potential risks and recommend solutions to tackle problems at a global level.

This report summarises the findings of our research. Chapter 2 explains common social media scams, how they work and why social media platforms are rapidly becoming the number one choice for online fraudsters. Chapter 3 investigates the prevalence of social media scams and where they are taking place.

Chapter 4 explores how consumers get information about social media scams and highlights good practice systems for detection, reporting and enforcement. Chapter 5 puts forward recommendations for effectively tackling social media scams at both a national and international level.

CONSUMERS INTERNATIONAL WOULD LIKE TO THANK ALL OF THE INDIVIDUALS AND ORGANISATIONS WHO CONTRIBUTED TO THIS STUDY.

OUR RESEARCH

To gain insight into the consumer experience of social media scams, Consumers International commissioned global research agency, We Are Social, to monitor public online conversations about social media scams in nine countries located in three different language markets

These were:
- English speaking - UK, US, Nigeria, India
- Spanish speaking - Spain, Chile, Argentina
- Arabic speaking - Egypt and Saudi Arabia

Countries chosen had a comparatively high level of social media activity within their region, plus one or more Consumers International member organisations. Between August 2016 and August 2018, the agency analysed more than 4,500 posts from consumers and influencers across Facebook, Instagram, Twitter, blogs and public forums, based on 'keyword' searches.

To supplement this research, Consumers International conducted in-depth interviews, between August and November 2018, with representatives from 20 global consumer groups, consumer protection authorities, civil society organisations and enforcement agencies. In December 2018 we invited all of these experts, plus senior representatives from banking, telecoms, e-commerce, national police, government, and major tech companies to a stakeholder workshop to share ideas about how to make the online environment safer for consumers.

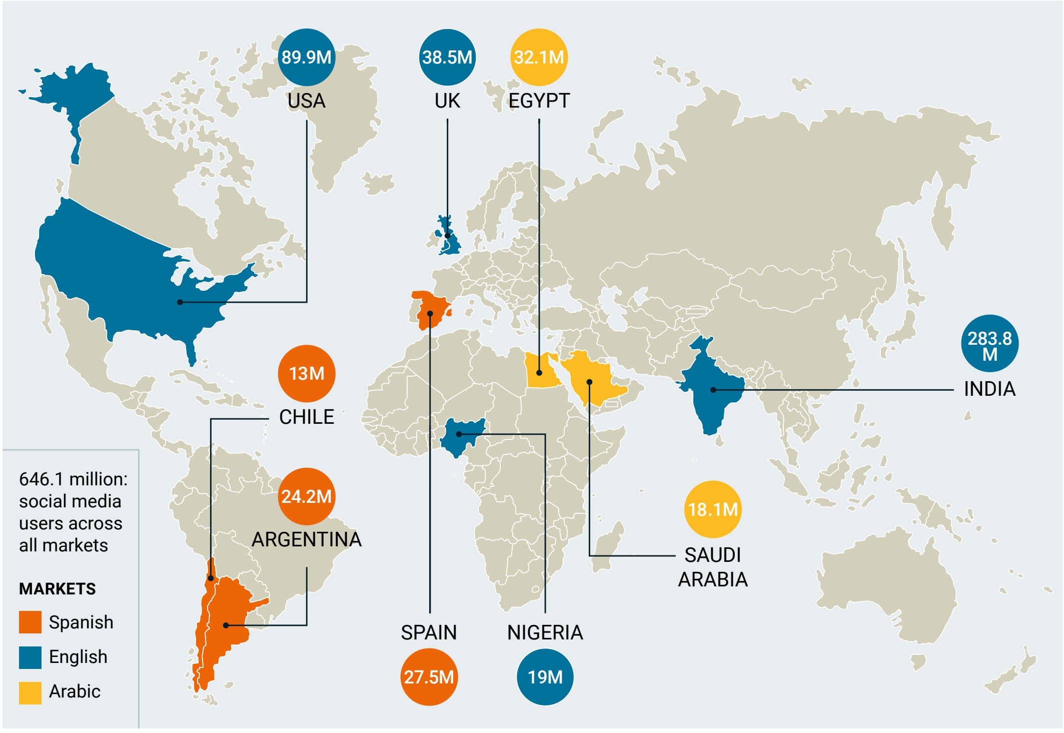


Figure 1: Number of social media users, by markets analysed

2. SOCIAL MEDIA SCAMS EXPLAINED

2.1 WHAT IS A SCAM?

Scams are fraud: a criminal activity designed to trick someone out of money or personal details. Methods constantly evolve as scammers look for new ways to commit fraud and avoid detection. Consumers might be contacted by telephone, post, email or even on their doorsteps. In the long history of scams, the internet is a relatively new way for fraudsters to target potential victims and they have been quick to reinvent old tricks for new digital platforms.

2.2 WHY SOCIAL MEDIA?

Social media is a dream come true for fraudsters. Three billion people - 40% of the global population - are active users of social media, such as Facebook, Twitter, WhatsApp and Instagram, with a million new users estimated each day[2]. This popularity, combined with the open nature of social media platforms, makes it easy for criminals to reach incredibly large numbers of people.

Social media enables 'social engineering' of scams, giving criminals access to vast amounts of personal data, which can then be used to target specific demographic groups and personalise scams to make them more convincing. For example, using a person's real name, or making reference to their hometown, recent holiday, hobbies and friends.

Social media gives fraudsters the ability to hide their true identities and motives behind the anonymity of fake profiles and accounts, which they use to mislead consumers[3], impersonate trusted sources and make offers that are too good to be true[4]. These scams can be difficult to spot as they appear to come from trusted sources such as family, 'friends', 'followers', online community members or known brands.

Scams can spread with alarming speed across social media, as likes, shares and retweets propagate content to a wide range of audiences. In effect, the social media model allows scammers to sit back and let consumers, albeit involuntarily, do much of the hard work.

[2] We Are Social, Global Digital Snapshot

[3] Guardian 'It's not just the Fyre festival – this is the golden age of the social media con', 17/01/18

[4] European Commission, Too good to be true: the real price of fake products, 2017

2.3 COMMON SOCIAL MEDIA SCAMS

The aim of a scam is to trick people into parting with money or revealing sensitive personal data - such as email addresses, passwords and birth dates - to facilitate ID theft (known as 'phishing'), which can then be used for financial gain. However, approaches can vary.

Most scams fall into three broad categories:

- E-commerce scam - fraudsters claim to be genuine online sellers, on sites such as Facebook Marketplace. Consumers pay for goods, which then turn out to be counterfeit (e.g. fake clothing or gift vouchers) or poor quality (e.g. faulty or substandard). In some cases, goods simply never arrive.

- Investment scam - fraudsters advertise a 'too good to be true' investment opportunity, sometimes using news stories and advertisements that appear to be from genuine sources. Consumers who are tempted to invest lose some or all of their money.

- Impostor scam - fraudsters pose as authentic brands, genuine friends or family, to gain a consumer's trust asking them to purchase goods, send money or click on links which download malware to their computer.

Within these three categories, lots of different tactics are used. Figure 2 explains some current social media scams.

2.4 WHO IS AT RISK?

Scammers use increasingly sophisticated techniques to target consumers and anyone can become a victim. The experts we interviewed, reported no significant differences in the number of victims in terms of age or gender. However, fraudsters are likely to target certain scams at specific demographic groups if they think it will increase success. For example, Trading Standards in the UK reports that young men are the most likely to be targeted by online scams involving steroids, while middle-aged women are most likely to be targeted by scams involving diet pills. The Public Interest Advocacy Centre in Canada told us that younger people seem the most likely to be targeted by cryptocurrency scams.

Consumers in vulnerable situations might find it more difficult to make informed choices or say no to high pressure selling, which can make them more susceptible to fraud[5]. For example, Citizens Advice in the UK found that older people can be particularly vulnerable to online scams, including those on social media[6]. Research by the Swedish Consumer Agency found that consumers with physical or cognitive impairments, low incomes, low levels of education and poor language skills were more likely to become victims of subscription traps[7].

2.5 IMPACT AND HARM

Scams have the potential to cause great harm to consumers and financial losses can be potentially life changing. Consumers International member Which? recently reported on bank impersonation scams that lost 19 victims almost £350,000 between May 2018 and January 2019[8]. Evidence from other Consumers International members suggests that the amount of money being lost per scam is increasing. For example, data from the Australian Competition and Consumer Commission shows that, despite reported social media scams remaining fairly static over the last few years, the amount of money lost quadrupled between 2015 and 2018, from $3.8 to $13.1 million AUS dollars[9].

The Canadian Anti-Fraud Centre reports similar trends, with complaints of fraud decreasing, while total losses increase[10].

In addition to financial losses, victims of scams can be affected mentally and emotionally. They may feel ashamed and suffer from social isolation, which can affect their interactions with others. It can also degrade consumer trust in digital marketplaces, social media platforms and genuine brands, affecting future online behaviour and interactions[11].

It is important to note that social media scams can have a negative impact on brands as well as consumers. Impostor scams, where criminals pose as authentic brands, reviewers and well-known figures to trick consumers out of money can cause reputational damage to the individual or organisation being impersonated.

[5] Lee, J. and Soberon-Ferrer, H. Consumer Vulnerability to Fraud: Influencing Factors, Journal of Consumer Affairs, 31, 1997
[6] Pardoe, A. and Couture, X. 'Changing the story on Scams,' Citizens Advice
[7] 'Consumer Reports 2017,' Swedish Consumer Agency, p. 21.
[8] Which? Bank Transfer Scam Victims to get Refunds from May, 2019
[9] Australian Competition and Consumer Commission 'Scams Statistics'
[10] Canadian Anti-Fraud Centre 'Statistical Reports'
[11] National Trading Standards Scams Team, UK

CATFISH: fraudsters create fake profiles to make contact with individuals and lure them into an online relationship. They take time to build trust, then ask consumers to send money or share personal details.

CRYPTOCURRENCY: fake advertisements, news articles or messages tempt consumers into investing in cryptocurrency, such as bitcoin. Consumers lose their investment, have their personal details stolen, or both.

CLICKBAIT SCAM: social media posts with 'exciting celebrity news' encourage consumers to click on links or hidden URLs. These lead to an external site which downloads malware to the victim's computer.

CASH GRABS: a fraudster hacks into someone's social media account, then sends messages to their friends claiming to be in desperate need of help and asking them to send them money. For example, in the 'stranded traveller' scam a 'friend' on holiday has had their wallet stolen and needs money to get home.

FAKE COMPETITIONS OR GIVEAWAYS: fraudsters pose as a legitimate business, usually on Facebook, asking users to 'like and share' posts or click on links to win non-existent prizes. 'Like-farming' allows scammers to build followers, who they can target with spam or scams. Clicking links could download malware.

MEMBERSHIP SCAMS: a consumer is invited to join a fake group or fan page and is required to share personal details, send premium text messages or pay for membership.

QUIZ SCAMS: a consumer sees an innocent looking 'fun quiz' on a friend's feed. They are asked to enter details such as their mother's maiden name, birthday month and first pet's name - often used in account security questions - to create their own 'Superhero' or 'Rockstar' name. This is an attempt to 'phish' for personal data.

SUBSCRIPTION TRAPS: a consumer is directed to sign up for a product or service which they never receive, Ongoing debits are made from their account, or they are targeted with demands for payment.

Figure 2: Types of social media scam

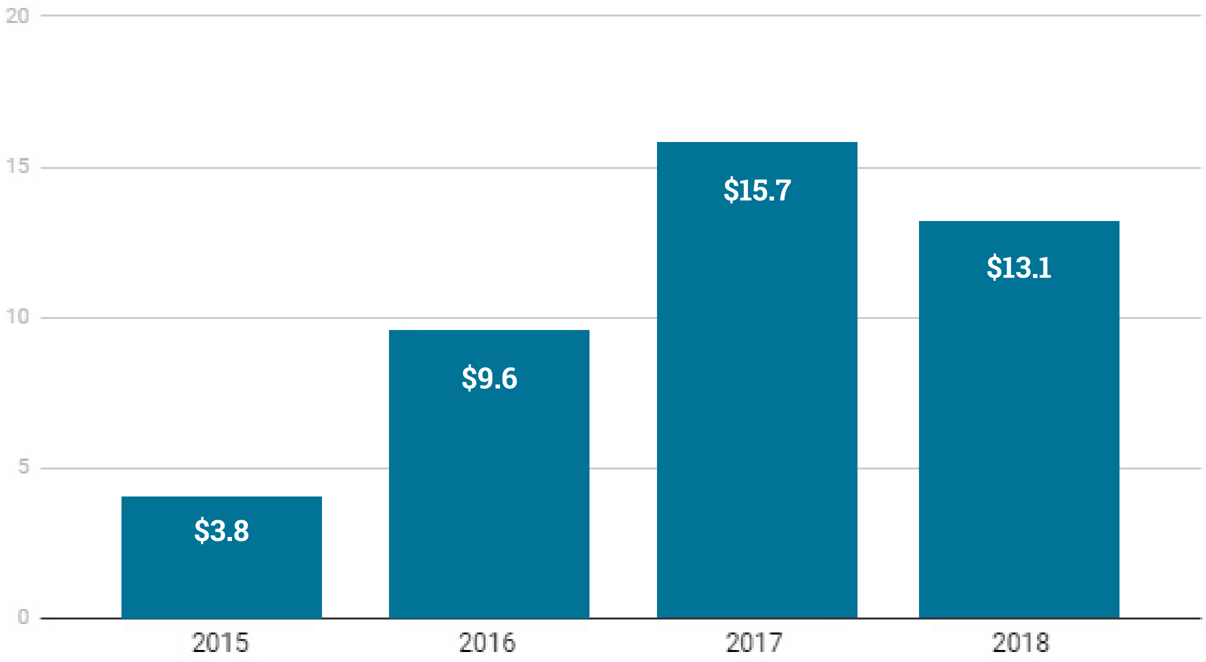


Figure 3: Money lost to social media scams by year, in millions of Australian dollars

Source: January 2015 to October 2018 Australian Competition and Consumer Commission

3. SCAM CONVERSATIONS AND TRENDS

3.1 SCALE OF THE PROBLEM

Online scams have grown exponentially as internet usage has flourished and cybercrime is the biggest source of concern for 81% of internet users around the world, according to a 2018 survey[12]. Social media is an increasingly popular way for scammers to target consumers online, according to our expert interviews, and platforms such as Facebook and Instagram have rapidly become the primary channel for online scams.

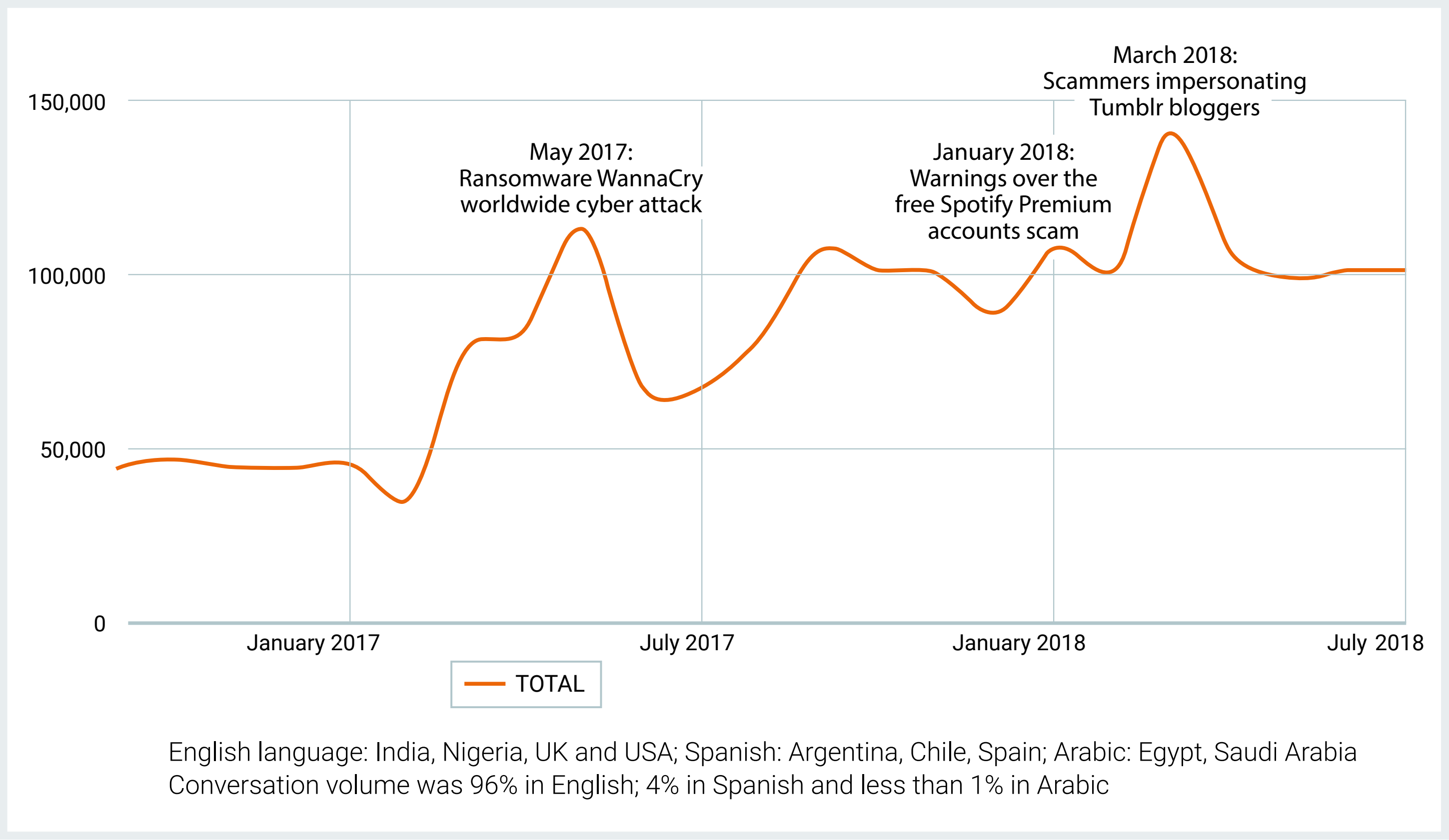
To date, understanding the true scale of the problem, and the real impact on consumers, has been difficult due to a lack of comparable data at a global level.

However, our research reveals a significant increase in online conversations about scams in all the countries analysed, with volume more than doubling between August 2016 and August 2018 (see Figure 2).

During this period, there were significant spikes in conversation volumes during specific scam attacks, such as WannaCry in May 2017 and Tumblr scam in March 2018, when users were sharing information, warnings and advice.

Our analysis shows that media coverage of such incidents promotes wider awareness as consumers seek information outside social media, for example by conducting Google searches.

[12] Centre for International Governance Innovation, The Internet Survey, 2018



English language: India, Nigeria, UK and USA; Spanish: Argentina, Chile, Spain; Arabic: Egypt, Saudi Arabia
Conversation volume was 96% in English; 4% in Spanish and less than 1% in Arabic

Figure 4: Conversation volume of social media scams

Note: We monitored online conversations about scams in India, Nigeria, UK, USA, Argentina, Chile, Spain, Saudi Arabia and Egypt from August 2016 to August 2018

3.2 SCAM CONVERSATION TRENDS

By country

Scams are a hot topic of discussion worldwide, but conversation volumes vary by country. Unsurprisingly, there is a strong correlation between conversation volumes and the number of social media users. For example, the majority (96%) of online discussions about social media scams take place in the English speaking markets, which have the highest numbers of social media users. The US, with the largest number of social media users out of the countries surveyed, dominates in terms of absolute volume – with 1.3 million 'mentions' of scams between August 2016 and August 2018.

However, the proportion of scam mentions per social media user (see Annex), tells a different story. Nigeria had the highest number of scam 'mentions' per social media user, mainly driven by the popularity of the Nairaland forum[13], where 71% of scam-related conversations took place. While India had a disproportionately low volume of scam conversations per social media user.

Online scams are often 'borderless' - committed by criminals who operate internationally - or at least have international elements.

We found that social media scams often originate from another country where the same language is spoken. For example, scams affecting consumers in the UK might originate in Canada or the US, and the National Consumer Complaints Centre Malaysia (FOMCA) receives complaints from consumers who have been targeted by social media scams originating from China.

By platform

Across all nine countries, where it was possible to identify the origin of scams, WhatsApp and Facebook were the platforms through which scams propagate the most, followed by Instagram and Twitter. Consumers do not necessarily reference the platform when sharing information about a social media scam, therefore in all countries we analysed, there are large numbers of scam 'mentions' where the platform of origin was unclear.

[13] Nairaland was established in 2014 and reportedly has over 55 million Internet users, corresponding to 32.9% of the entire population of Nigeria.

3.3 TYPES OF SCAM

Local cultural and market factors influence the types of scams consumers experience – a finding shared by the organisations we interviewed, and reinforced by our social media analysis across English, Arabic and Spanish speaking markets. (See Figure 5).

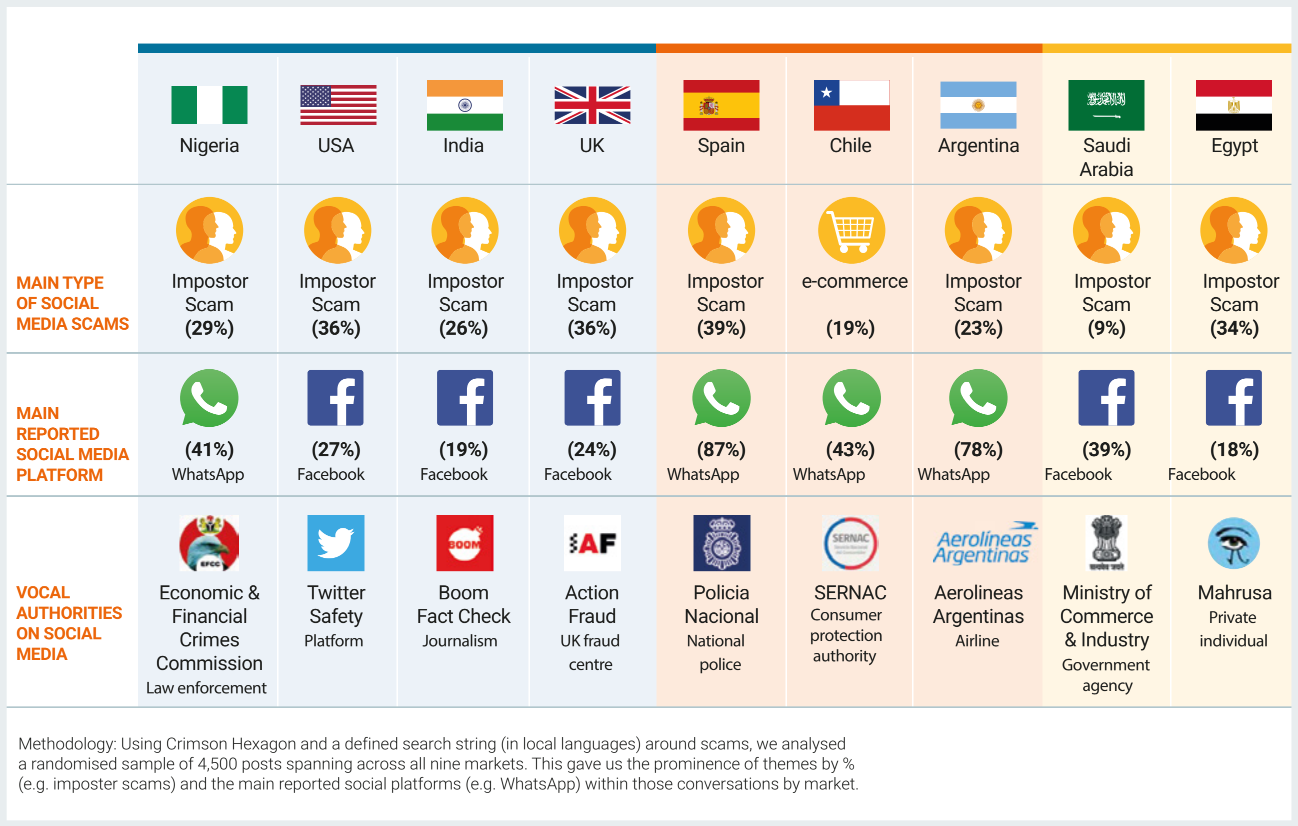
Three types of social media scam dominated discussions:

Impostor scams

Impostor scams, where scammers pose as brands, authorities or even friends to deceive victims, are the most commonly discussed type of scam in most countries. These were most frequently discussed by consumers in Spain (51%) and closely followed by Argentina (49%).

The most popular form of impostor scam, particularly in the Spanish and Arabic markets, consists of scammers impersonating the WhatsApp brand to promise downloadable add-ons, such as the ability to customise colours. Scams are often spread using compromised accounts, where a fraudster hacks into a genuine account then sends out links to harmful downloads.

According to the experts we interviewed, consumers have high levels of trust communicating with contacts via WhatsApp and are likely to open messages they believe are from genuine contacts. In the UK and US, the most talked about impostor scams are catfish and dating scams.



	Nigeria	USA	India	UK	Spain	Chile	Argentina	Saudi Arabia	Egypt
MAIN TYPE OF SOCIAL MEDIA SCAMS	Impostor Scam (29%)	Impostor Scam (36%)	Impostor Scam (26%)	Impostor Scam (36%)	Impostor Scam (39%)	e-commerce (19%)	Impostor Scam (23%)	Impostor Scam (9%)	Impostor Scam (34%)
MAIN REPORTED SOCIAL MEDIA PLATFORM	(41%) WhatsApp	(27%) Facebook	(19%) Facebook	(24%) Facebook	(87%) WhatsApp	(43%) WhatsApp	(78%) WhatsApp	(39%) Facebook	(18%) Facebook
VOCAL AUTHORITIES ON SOCIAL MEDIA	Economic & Financial Crimes Commission Law enforcement	Twitter Safety Platform	Boom Fact Check Journalism	Action Fraud UK fraud centre	Policia Nacional National police	SERNAC Consumer protection authority	Aerolineas Argentinas Airline	Ministry of Commerce & Industry Government agency	Mahrusa Private individual

Methodology: Using Crimson Hexagon and a defined search string (in local languages) around scams, we analysed a randomised sample of 4,500 posts spanning across all nine markets. This gave us the prominence of themes by % (e.g. imposter scams) and the main reported social platforms (e.g. WhatsApp) within those conversations by market.

Figure 5: Scam trends by country

Note: The main type of social media scam refers to the most commonly cited type of social media scam in public online conversations.
Note: The main reported social media platform refers to the most commonly cited social media platform in public online conversations about social media scams.

E-commerce scams

E-commerce on social media platforms is growing. And Facebook Marketplace, Instagram ads, and 'buy buttons' embedded in social media posts aim to create a seamless marketplace experience for consumers.

Unfortunately, this creates further opportunities for scammers to exploit consumers, with our research showing that e-commerce[14] scams are particularly prevalent on Facebook Marketplace and WhatsApp.

E-commerce scams are particularly widespread in the emerging markets of Nigeria and India where fake vendors spread scams via social media forums and online marketplaces. These typically involve the purchase of clothing items, with consumers receiving far-lower quality items than advertised or, in some cases, not receiving any item at all. Consumers mention these scams taking place on Facebook Marketplace and WhatsApp.

In higher income economies like the US and UK, e-commerce scams typically involve tech goods like mobile phones, or high cost items such as cameras or event tickets. Interviews with consumer protection organisations indicate that the most common type of e-commerce scam is sending items of much lower quality than described.

Finance and crypto currency scams

Finance and currency scams are the third most prevalent scam in the markets we analysed. This type of scam is most common in Nigeria, where they make up 21% of conversation volumes about scams and least common in Egypt and Saudi Arabia where they represent less than 1% of the social media scams analysed. Finance scams in Nigeria most often take place via WhatsApp and one-to-one chats – where scammers make direct contact with consumers to gain their trust and persuade them to make investments.

Theme	Argentina	Chile	Egypt	India	Nigeria	Saudi Arabia	Spain	UK	USA
WhatsApp	21%	10%	7%	0%	41%	13%	29%	6%	5%
Facebook	6%	6%	8%	19%	22%	39%	5%	24%	27%
Instagram	4%	2%	0%	4%	4%		2%	8%	7%
LinkedIn							0%		
Twitter	3%		11%	11%	8%	12%	1%	16%	17%
Platform unclear*	67%	82%	73%	67%	24%	36%	63%	46%	49%
Grand Total	100%	100%	100%	100%	100%	100%	100%	100%	100%

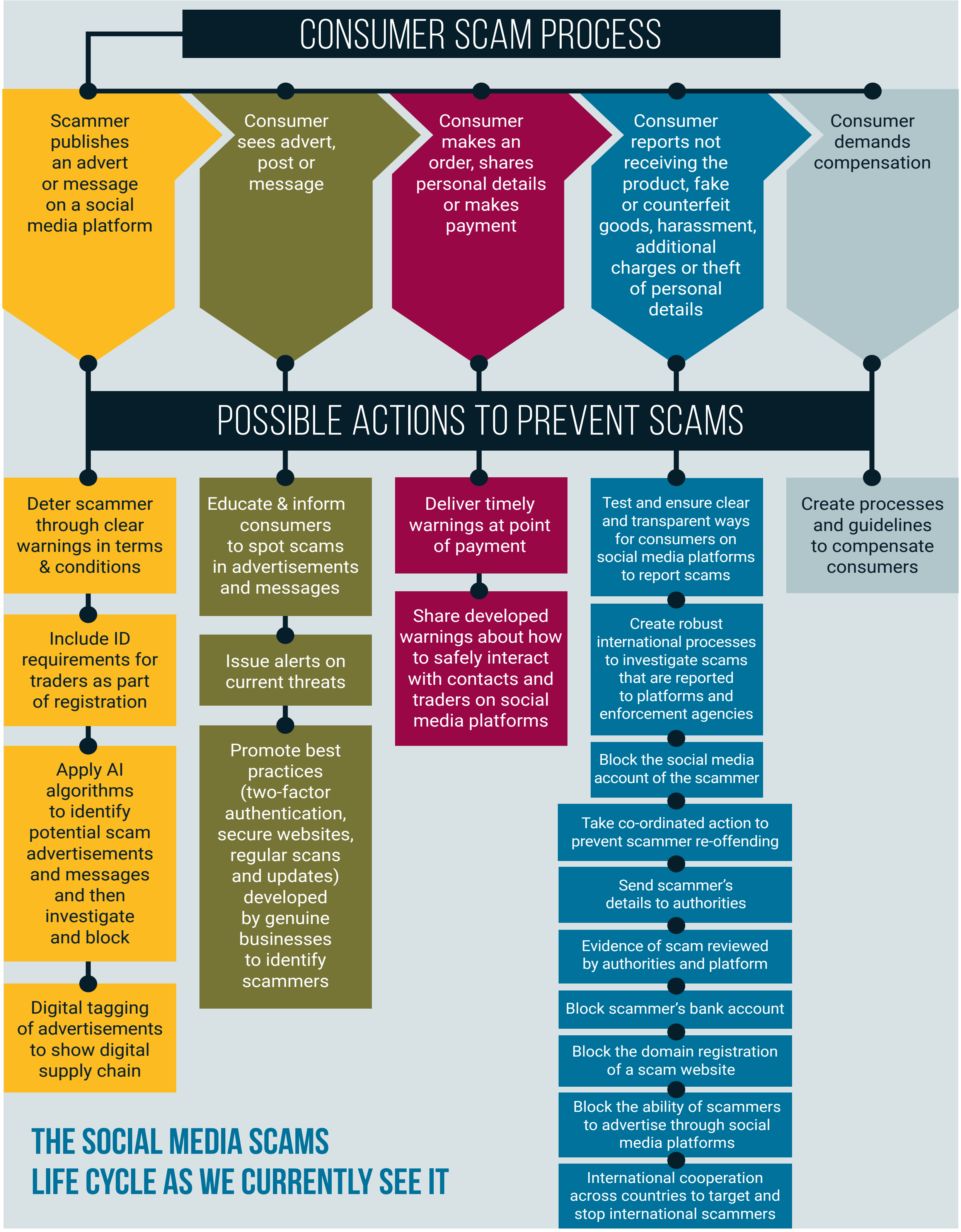
*Consumers mentioned social media scams in posts but it is unclear which platform is being referred to either because there are no links, or the social media platform has not been mentioned

Figure 6: Origin of scams, by social media platform

[14] European Commission, Euro-stat

4. TAKING ACTION AGAINST SCAMS

Swift and effective action against scams is essential to minimising consumer detriment (see Figure 6). Our research discovered a wide range of actions being employed by consumers, consumer protection authorities and organisations to tackle the complex challenges we are facing. This chapter summarises the current situation and highlights some of the good practice that we found.



CONSUMER SCAM PROCESS

Scammer publishes an advert or message on a social media platform

Consumer sees advert, post or message

Consumer makes an order, shares personal details or makes payment

Consumer reports not receiving the product, fake or counterfeit goods, harassment, additional charges or theft of personal details

Consumer demands compensation

POSSIBLE ACTIONS TO PREVENT SCAMS

Deter scammer through clear warnings in terms & conditions

Include ID requirements for traders as part of registration

Apply AI algorithms to identify potential scam advertisements and messages and then investigate and block

Digital tagging of advertisements to show digital supply chain

Educate & inform consumers to spot scams in advertisements and messages

Issue alerts on current threats

Promote best practices (two-factor authentication, secure websites, regular scans and updates) developed by genuine businesses to identify scammers

Deliver timely warnings at point of payment

Share developed warnings about how to safely interact with contacts and traders on social media platforms

Test and ensure clear and transparent ways for consumers on social media platforms to report scams

Create robust international processes to investigate scams that are reported to platforms and enforcement agencies

Block the social media account of the scammer

Take co-ordinated action to prevent scammer re-offending

Send scammer's details to authorities

Evidence of scam reviewed by authorities and platform

Block scammer's bank account

Block the domain registration of a scam website

Block the ability of scammers to advertise through social media platforms

International cooperation across countries to target and stop international scammers

Create processes and guidelines to compensate consumers

THE SOCIAL MEDIA SCAMS LIFE CYCLE AS WE CURRENTLY SEE IT

Figure 7: Tackling social media scams

4.1 SHARING WARNINGS AND ADVICE

Consumers turn to each other

Our research shows that consumers are most likely to turn to other social media users, rather than official sources, to seek information about suspected scams, or share warnings. Evidence gathered across markets indicates that consumers tend to be confused about social media scams and where to turn for a trusted mediator, leading to online discussions instead.

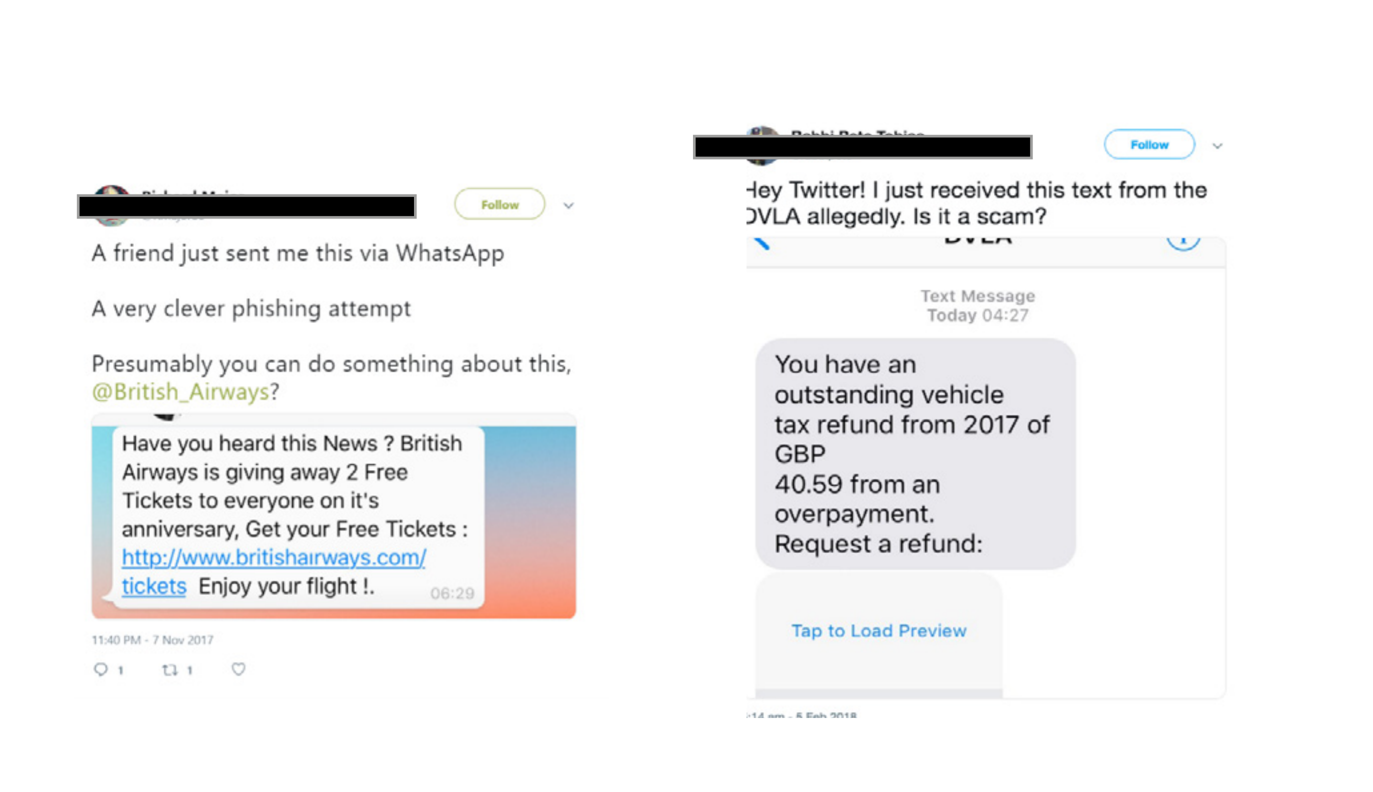
In Spanish speaking markets, consumers tend to share suspected scam threats posted by the Spanish police or mainstream news accounts. In Arabic speaking markets, consumers actively warn others of scam risks and frequently offer advice – such as how to report fraudulent activity, how to protect yourself from scammers (e.g. antivirus software) and what to do if a consumer's account has been compromised. In English speaking markets, consumers share views about the increasing sophistication of phishing attempts, and how difficult they are to spot.

For example, in the US, social media users often complain about the number of 'bots'[15] that exist on platforms.

Where social media users suspect they have been approached by a scam, they appeal to a range of organisations and individuals to verify the situation – such as the brand impersonated by the scam, the platform it occurred on and the wider social media community.

However, scammers have been known to take advantage of consumer trust in online communities. For example, many scam victims in Nigeria turn to Nairaland[16] for advice, but there is evidence to show that scammers often respond to these calls for help with more scam attempts.

While social media users appear willing to share information about unsuccessful scam attempts, or stories about other scam victims, they rarely speak about their own experiences once they have fallen victim to a scam. This is particularly true in Spanish speaking and Arabic speaking markets. Stigma around falling for scams, and the assumption that the victim may have been reckless or naïve, can make victims reluctant to share information.



[redacted]

A friend just sent me this via WhatsApp

A very clever phishing attempt

Presumably you can do something about this, @British_Airways?

Have you heard this News ? British Airways is giving away 2 Free Tickets to everyone on it's anniversary, Get your Free Tickets : http://www.britishairways.com/tickets Enjoy your flight !. 06:29

11:40 PM - 7 Nov 2017

[redacted]

Hey Twitter! I just received this text from the DVLA allegedly. Is it a scam?

Text Message
Today 04:27

You have an outstanding vehicle tax refund from 2017 of GBP
40.59 from an overpayment.
Request a refund:

14 am - 5 Feb 2018

Figure 8: Examples of consumers seeking advice about social media scams

Note: The most commonly cited platform for social media scams in each country is highlighted.

[15] Algorithms that impersonate individuals or organisations

[16] Nairaland is an online community that was established in 2014 and reportedly has over 55 million Internet users, corresponding to 32.9% of the entire population of Nigeria.

Official warnings need to evolve at a fast pace to keep up with current risks. Our conversation analysis reveals which authorities are most vocal about social media scams, in each of our nine countries (see Figure 5).

For example, Action Fraud is most active in the UK, the National Consumer Service in Chile and the national police in Spain (see Case study). Although many countries have authorities responsible for fighting fraud, there are different approaches in how they deal with warning consumers about scams, possibly due to resources and legislative powers[17].

Our research shows that some agencies engage very little with social media to communicate with consumers, while others proactively use their official social media accounts to warn consumers about emerging scams. For example, the Competition Bureau of Canada told us that it regularly issues scam alerts through Facebook, Twitter and LinkedIn, which have had a positive impact on a wide audience.

CASE STUDY: CONSUMER ENGAGEMENT ON TWITTER

In Spain, the Policia Nacional have established themselves as a trusted point of contact for consumers seeking advice on how to avoid scams or wishing to report incidents. They successfully engage consumers on Twitter by posting humorous and light-hearted warnings to raise awareness and encourage social media users to interact with them directly. This is a model that could be taken up by authorities in other countries as a way of building trust between consumers and enforcement in online spaces, as well as helping to reduce the social stigma associated with falling victim to a scam.

The role of consumer organisations

Both Consumers International members and consumer protection authorities we interviewed stressed the need for more consumer education about scams, and often play a vital role in raising awareness. For example, the Danish Consumer Council has demonstrated that apps can be an effective way of reaching consumers to provide real time advice.

CASE STUDY: DIGITAL SELF-DEFENSE APP

In 2017 the Danish Consumer Council (Forbrugerrådet Tænk) developed an app called 'My Digital Self-Defense' in response to a survey that showed more than one in seven Danish citizens had been scammed online. The app shares daily updates, guidance and advice to boost consumer safety online. Several companies, authorities and institutions have joined the initiative and contribute content including warnings about impostor web pages, scam competitions and dangerous links in texts and e-mails[18]. As a result of these efforts the My Digital Self-Defense app published 7,300 user-generated tips and 236 scam notifications and warnings in 2018.

Figure 9: Digital self-defence app

[17] Not all national consumer authorities have an obligation or the legal powers to investigate or resolve consumer complaints. And some national consumer authorities focus on law enforcement actions to protect the public interest but do not intervene in individual cases. International Consumer Protection and Enforcement Network www.icpen.org/resolve-dispute

[18] 'New app helps Danish consumers protect themselves from online fraud', BEUC

The role of industry

The private sector also has a key role to play in educating consumers. Financial service providers are in a good position to disseminate timely and relevant information. Our analysis found that some banks already provide regular alerts to customers about the risk of scams, through online banking websites, apps and social media posts. However, some interventions from banks go beyond simple warnings and include interactive content to engage consumers. For example, Barclays bank in the UK runs 'Digitally Safe Quizzes' and NatWest conducts Twitter polls asking followers if certain messages are safe or are scams.

4.2 OFFICIAL REPORTING

Experts estimate that reported scams are only the tip of the iceberg, with UK Trading Standards and the Canadian Anti-Fraud Centre estimating that only 5% of scams are reported in their countries. Our research shows that those who have fallen victim to a scam are extremely unlikely to report it to official sources due to a range of factors, including embarrassment, apathy and uncertainty about who to contact. In many countries there are multiple agencies collecting data about fraud in different sectors, leading to consumer confusion about where to report scams or seek redress. Some consumer organisations we interviewed, particularly in the Middle East, told us that consumers are unlikely to report as they are accustomed to accepting unsolicited scams as part of using digital communications and tools.

Consumer protection authorities record and classify fraud incidents in different ways, making it difficult to compare data. On a positive note, in our interviews, some organisations explained that they are starting to code online fraud incidents with reference to where they originate from on social media platforms. However, this good practice is not consistently applied at a global level.

4.3 DETECTING HARMFUL CONTENT

Swift identification of fraudulent, offensive or harmful content is key to protecting social media users, yet the experts we interviewed highlighted the challenges given the sheer volume of online content coming from multiple sources. However, they also raised some ideas for good practice.

In some countries, authorities carry out checks to verify the legitimacy of the businesses which may then create an account, advertise or post on social media. For example, the NCCC/FOMCA in Malaysia requires traders to register with the authorities. However, many small traders fail to do so.

Other projects, such as ScamAdviser and the Trustworthy Accountability Group (TAG) (see case studies) aim to authenticate businesses or advertisers using digital tools such as Artificial Intelligence (AI). Although AI-enabled solutions are already being successfully deployed to identify suspicious websites, the enforcement agencies we spoke with felt that AI could struggle to identify scam advertisements, as they often use the same language as legitimate ones.

Social media platforms themselves could be more proactive in using digital tools to detect fraudulent ads. However, advertising provides key revenue[19], which can create a potential conflict of interest when it comes to effective self-policing. Independent regulators can wield more power.

For example, in the UK, the Advertising Standards Authority (ASA) can require the amendment or withdrawal of ads that break rules[20] and local Trading Standards can issue fines for repeated breaches[21].

CASE STUDY:
SCAMADVISER TOOL

ScamAdviser.com, developed by the Ecommerce Foundation, is a free tool for consumers to check the legitimacy of a website. When a consumer enters a web address into the site, algorithms check 40 factors such as the IP address, site reviews, security and spam reputation to generate an overall 'trust score'. ScamAdviser.com has more than 55 million websites on its database and 2.5 million unique users per month.

[19] 'Social Advertising Worldwide', Statista
[20] 'ASA Sanctions', ASA
[21] 'Unfair trading, trade descriptions and pricing FAQs', Law Donut

CASE STUDY: TACKLING AD FRAUD

The Trustworthy Accountability Group (TAG) is a cross-industry self-regulatory programme to tackle criminal activity in digital advertising. It has developed a set of standards to tackle ad fraud that brands, their agencies and advertising technology partners can sign up to[22].

Platforms can check TAG to make sure companies have been authenticated, then host content secure in the knowledge that it is not fraudulent. The number of companies voluntarily signing up to this service is growing, which increases the viability of the system as a solution. Further development could be instrumental in providing a counterbalance to the difficulty of identifying intentionally misleading advertising using moderators and AI solutions.

Some tech companies we spoke to demonstrated how they are using innovative digital tools, such as algorithms, to tackle fraud before it reaches the consumer:

- eBay has developed a new algorithm to identify and flag activities that fall outside the norm in e-commerce transactions. In initial tests, which analysed almost 300,000 transactions, the algorithm detected 40% of 492 fraudulent cases, incorrectly flagging only 29 legitimate transactions (around 0.001% of the sample)[23].
- Google is harnessing technology to improve its ability to analyse and block scam emails headed for a Gmail inbox. Security measures include the ability to predict email messages that contain malware, warnings when a user is replying to someone not in their contact list or when a user clicks on a phishing link[24].
- Airbnb uses machine learning and predictive analytics to evaluate hundreds of risk signals to offer real-time detection of fake listings on its platform, which it flags to prevent scams before they can harm consumers. Airbnb also publishes prominent warnings on its accommodation listing pages on how to avoid scams.

4.4 ENFORCEMENT

Responsibility for monitoring social media scams and enforcement of consumer protection measures may be shared between the police, consumer protection and enforcement agencies and social media platforms themselves. However, the nature of social media scams can make it difficult to track down those responsible and bring them to justice.

Difficulties of operating cross border

Our expert interviews show that, at a global level, the biggest obstacle to enforcement is the absence of a cohesive and consistent framework of consumer protection legislation. Online fraud is frequently committed across national borders, while many consumer protection and enforcement agencies are restricted by national or regional boundaries. As one consumer protection authority highlighted, different consumer law can apply in different countries with different powers to prosecute crimes so this can complicate the pursuit of fraudsters. For example, US regulators can levy substantial fines, whereas UK regulators can prosecute.

Some countries and regions, such as Malaysia and Japan, have bilateral agreements where they agree to prosecute scammers who target consumers across country borders. However, without bilateral agreements in place, national consumer protection authorities are limited in the action they can pursue in the country that the scam originated. Even where jurisdiction does exist, national consumer protection authorities often lack resources, which can limit their ability to investigate cross-border scams where proving liability can be difficult, expensive and time consuming.

Our research suggests that a high level of consumer detriment is caused by a proportionally low number of criminals, who use social media to propagate scams to a large global audience. So, on a positive note, when scammers get caught it can have far reaching benefits for consumers. One takedown of a botnet operation[25] in Canada resulted in a significant reduction in the number of scams being reported.

[22] 'About the TAG Certified Against Fraud Program', Trustworthy Accountability Group
[23] 'eBay's AI identified techniques to avoid credit card fraud' The Paypers
[24] 'Google Says Gmail Now Blocks 99.9% of Spam and Phishing Emails', Bleeping Computer
[25] Bots are automated software that can carry out tasks on a large scale, in this case for the purposes of fraud.

Platform liability

There is fierce international debate around who is liable for social media content and what actions should be taken to tackle it. Social media platforms often claim that they are neutral intermediaries in an ecosystem created by their users, thereby denying responsibility for content. However, there is growing pressure on platforms to tackle fraudulent, illegal or harmful content - such as hate speech – as the potential implications become more apparent.

The cross-border nature of social media platforms complicates the matter. In most cases, platforms are bound by the law in the country that they are based, but national laws vary. Most global social media companies are based in the US, which means that they adhere to US legal and regulatory structures[26]. The US Constitution defends the right to free speech, which affects its legislative approach to this matter.

The fact that platforms' terms and conditions are seldom tailored to other regions in which companies operate, can have far-reaching implications for cross-border consumer protection. For example, in US law[27] most big platforms are protected by 'safe harbour' provision that gives online platforms legal immunity from most of the content posted by their users. This means that platforms are not liable for the actual content posted by third party users. European legislation or voluntary agreements set-up between enforcement agencies and platforms may place responsibility on social media platforms to remove harmful content once they have been notified through notice and action procedures[28]. The current approach does not guarantee the same level of protection to consumers regardless of their location, for example in the instance that a consumer is targeted with a social media scam that is originating in the US.

In the European Union (EU), consumer protection legislation is particularly well developed and laws relating to unfair commercial practices, transparency of information and distance selling rules could be applied in cases of social media scams. In recent years, efforts have been made to align platforms' terms of service with EU consumer protection rules after finding that platforms were operating unfairly under EU law[29]. For example, by excluding liability for negligence and reserving the right to change their terms and conditions without notice. In 2016, the EU's Consumer Protection Cooperation Network reached an agreement with social media platforms including Facebook, Google and Twitter to establish a 'notice and action procedure', which allows European consumer protection authorities to report and request the removal of illegal content, including scams. The Commission also developed legal guidance for social media platforms around how they should deal with detection, notification and removal of illegal content[30]. The effectiveness of these new procedures is still being assessed[31].

CASE STUDY: VOLUNTARY AGREEMENTS

The Anti-Fraud Centre of the Royal Mounted Police in Canada has a voluntary agreement in place with social media platforms. It notifies them of fraudulent activity, and the platform reviews ads and posts to decide if they are contrary to their terms of service. Content that breaches codes can be removed. Although the process works in a timely manner, it is understood that there is always the risk of scams being re-posted, so efforts are ongoing.

There is also work at a national level to compel platforms to take down offensive content, related to terrorist activity and content deemed harmful to children, within a short time[32]. For example, in Germany, the Network Enforcement Law of 2018 allows social media companies with over two million users to be fined up to €50 million if they do not delete posts contravening German hate speech law within 24 hours[33]. Legal action in the UK recently forced Facebook to improve the way it tackles scams, although changes will only benefit UK users at this time.

Participants in our stakeholder workshop also highlighted good practice that businesses can follow in tackling harmful online content. For example, Google's page-level enforcement helping to protect consumers from threats such as malware, advertising fraud and content scamming.

[26] Riefa, Christine, Consumer Protection on Social Media Platforms Briefing note for Consumers International 2017
[27] Section 230 of the Communications Decency Act of 1996 states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider", '7 ways Protections for online content are being eroded'
[28] European Commission Workshop on Digital Platforms and Fundamental Rights,12 June 2017, BU-25 00/S1
[29] Twitter Terms of Service, ; Instagram
[30] 'Illegal content on online platforms', European Commission
[31] 'Social media companies need to do more to fully comply with EU consumer rules' European Commission
[32] 'Platform Responsibility', London School of Economics; 'Social media companies should have a 'duty of care' towards kids',
[33] 'Impact of social media and screen-use on young people's health', Science and Technology Committee UK Parliament

CASE STUDY: MARTIN LEWIS VS FACEBOOK

In the UK, Martin Lewis, a well-known public figure whose name and image appeared in thousands of scam adverts on Facebook, settled out of court with the platform after submitting a campaigning defamation lawsuit (pledging any proceeds to charity).

Instead of going to court, Facebook and Martin Lewis agreed a two-step action plan to fight against this industry wide problem.

Facebook is creating a new scam ad reporting tool for UK Facebook users, and dedicated internal operations teams to handle these reports, investigate trends and enforce against violating ads. This reporting tool will help users easily and quickly flag ads they believe to be scams violating Facebook's Advertising Policies or other standards.

Facebook is also donating £3 million to UK charity Citizens Advice to deliver a new Scams Action project[34]. The project, when launched in 2019, aims to:

- Increase public education and awareness about digital scam ads
- Build on existing work with partner organisations
- Provide one-to-one tailored support though a phone helpline and webchat to help people recognise scams
- Work with victims of online scams who need help

CASE STUDY: GOOGLE ENFORCEMENT POLICIES

In 2017, Google took down 3.2 billion ads, which equates to 100 ads per second, 320,000 publishers, 90,000 websites and 700,000 mobile apps and has developed page-level enforcement which is enabling Google to remove more bad ads from more websites.

Page-level enforcement affects individual pages in violation of Google's AdSense Program Policies. This includes ads for counterfeit goods, malware and phishing. Google also has a list of AdSense Program Policies on prohibited content which includes the promotion of content, products or services using false, dishonest or deceptive claims (e.g. 'Get Rich Quick' schemes)[35].

4.5 CONSUMER REDRESS

At present, it is virtually impossible for consumers to get their money back after they've been scammed as they have essentially 'agreed' to hand over cash. With fraudsters difficult to track down, reimbursement often falls to financial service providers.

In some countries, advances are being made to tackle this issue. For example, in the UK, Which? is campaigning to make banks responsible for refunding authorised payments (e.g. where consumers have been tricked into authorising a payment) in addition to unauthorised payments.The Anti-Fraud Centre in Canada also works with financial service providers to request reimbursements in cases of fraud (see case study).

CASE STUDY: REFUNDS FOR COUNTERFEIT GOODS

The Canadian Anti-Fraud Centre deals with consumer complaints about websites selling counterfeit or fraudulent goods. When a consumer files a complaint, they must provide details of the goods, website address, date and amount of purchase. If the Anti-Fraud Centre confirms that the goods are not authentic it will relay the information to the credit card company and issuing bank to assess other suspicious charges on the retailer's merchant account, while the credit card company initiates a chargeback or reimbursement to the consumer. This typically results in the termination of the counterfeit retailer's merchant account by the bank, so that the fraudster can no longer process payments and the problem is dealt with at the source.

[34] www.moneysavingexpert.com/news/2019/01/martin-lewis-drops-lawsuit-as-facebook-agreed-to-donate-p3m-to-a/
[35] Google AdSense help

5. RECOMMENDATIONS

There are no easy solutions to fighting scams. However, our research has identified good practice by some government agencies, consumer protection authorities and businesses that, if applied systematically, could help to empower and protect consumers and enhance trust in social media platforms. Our key recommendations are detailed below:

5.1 DEVELOPING CONSISTENT RULES FOR CONSUMER PROTECTION

Solid foundations at national level

Those we interviewed agreed that consumer protection legislation can be an effective tool to aid enforcement against social media scams, enabling decisive action by regulators and enforcement agencies. However, our research shows that there are different levels of protection in different countries and regions. For example, the National Society for Consumer Protection in Jordan and Consumers Lebanon claim that the largest barrier to tackling social media scams in their countries is the lack of consumer protection legislation.

Consistent, legally-binding consumer protection rules could help to establish a baseline of good practice in dealing with social media scams, from liability through to enforcement.

International guidance and cooperation

Given the cross-border nature of social media scams, and online fraud in general, it is essential that national consumer protection legislation is complemented by international cross-border cooperation, including intelligence sharing and agreements to prosecute scammers that operate across national borders.

International guidelines can provide valuable guidance for consumer protection authorities. For example, the United Nations Conference on Trade and Development (UNCTAD) and the Organisation for Economic Co-operation and Development (OECD) are driving initiatives to improve the regulation of e-commerce, including developing guidelines. The International Consumer Protection Enforcement Network (ICPEN) also promotes co-operation between national enforcement agencies. Several countries have made proposals to start formal negotiations for an international e-commerce trade deal, which could include measures to promote better consumer protection needed to help address the gaps.

5.2 INCREASING RESPONSIBILITY FOR SOCIAL MEDIA PLATFORMS

Self-regulation

Social media platforms have a responsibility to protect consumers by taking swift and effective action against fraudulent users, accounts, posts and advertisements. The consumer protection authorities and consumer organisations we interviewed, agree that social media platforms should take more decisive action to tackle fraudulent, harmful or illegal content on their platforms. This should include:

- Setting rules – clear terms and conditions about what is and isn't allowed on the platform
- Reporting of scams - making it easy for users to flag harmful content
- Taking action against those that break the rules – e.g. removing content, blocking accounts and barring users
- Minimising future risks – mechanisms in place to prevent reappearance of same or similar content e.g. monitoring content or taking steps to authenticate traders, websites and adverts

The largest social media platforms are global in nature, but often operate differently in different countries, as demonstrated in the Facebook case study in Section 4.4, where planned improvements will only apply in the UK. As scams operate cross-border, platforms should standardise their systems, policies and procedures, where possible, across different countries so that all consumers benefit from the same measures.

Voluntary agreements

As described in Section 4.4, there is currently no clear legal liability over social media content, which can restrict progress. In the absence of statutory guidance, some consumer protection authorities (for example in Europe and Canada) have reached voluntary agreements with platforms - they notify the platform of harmful content and it commits to investigate and remove the content if necessary. It will be important to monitor these agreements to see if they are operating effectively and, if so, more voluntary agreements should be explored.

5.3 DEFINING GOOD PRACTICE FOR BUSINESS

Policies and procedures

Businesses such as financial service providers, online retailers and intermediary sites have a role to play in protecting their customers from scams, which will also help to enhance their reputation and boost consumer confidence in their brand. Where fraudsters impersonate brands in impostor scams, the genuine business should be quick to respond to alert consumers to the scam and provide reassurance and advice on what action to take.

Financial service providers, as the custodians of consumer cash, are in an ideal position to raise awareness of current scams and minimise the risk of fraudulent transactions. In the UK, consumer and industry experts have successfully developed a code of practice to help banks develop policies and procedures to minimise the risk of consumer harm as a result of fraud and financial abuse.

Steps are also being taken by financial institutions and consumer protection authorities to build a picture of fraudulent merchant activity. These initiatives provide increased protection for consumers who have been defrauded through social media, providing a way to get their money back and shut down counterfeit retailers' bank accounts.

International standards

Voluntary standards, developed by expert working groups, can help businesses by defining good practice in the delivery of online services, systems and goods. As social media scams operate across geographical boundaries, international standards and codes will have the greatest impact.

The International Standards Organization (ISO) publishes specifications and guidelines to ensure quality and safety for consumers. ISO standards already exist for e-commerce, mobile payments, online reviews and internet security – to protect consumers against phishing and malware. International experts are currently developing new standards in the area of 'Privacy by Design' and the sharing economy. To date, we are not aware of any standards that tackle social media platforms specifically, or the legitimacy of online advertisements.

A new global standard detailing good practice for social media platforms could help to secure online marketplaces and provide assurances to consumers.

5.4 EXPLORING THE POTENTIAL OF DIGITAL TOOLS TO DETECT FRAUD

Algorithms to identify online fraud

The ability to identify and block fraudulent content before it reaches consumers could be a huge step forward in the fight against scams. Digital solutions, such as algorithmically-driven artificial intelligence (AI) systems and machine learning, are already being used with some success to tackle online fraud in a broader context (see section 4.3).

Although not 100% effective, algorithms can certainly help to reduce the risk of social media scams spreading on platforms. Some of the experts we interviewed stressed that AI-enabled tools alone are not capable of identifying all scams and should be used in conjunction with human moderators to check, verify and block harmful scam content. Developing algorithms to monitor social media content and identify the perpetrators of fraud is an area that Consumers International is keen to explore further.

Authentication of 'legitimate' businesses and ads

Our research found that impostor and e-commerce scams are the most prevalent types of scam on social media. Therefore, the ability to identify authentic business accounts and advertisements is important for consumers and solutions should be explored. Systems for trader or website verification, such as that being developed by the Ecommerce Foundation (see case study in Section 4.3) could be one answer.

Criminals often use malicious or fraudulent ads to perpetrate social media scams but, at present, anyone can advertise on social media as long as they follow the terms and conditions set by platforms, and there are very few mechanisms in place to distinguish between fraudulent and legitimate traders.

Experts we interviewed agreed that businesses wishing to advertise on social media platforms should undergo a greater level of authentication to establish their legitimacy. Digital identification tools could help to do this, playing a crucial role in the multi-stakeholder response to fraudulent ads on social media.

Considerable efforts have been made by a range of advertisers, major brands and industry groups, such as TAG to develop such tools (see case study in Section 4.3).

Free ad-blocker software, such as Adblock Plus, can help consumers to filter and block domains and ads that may spread malware by selecting preferences from pre-defined criteria. Exploring ways to link ad-blocker filter lists to businesses and advertisers that have been 'authenticated' using digital identification systems, could give consumers the option to block social media ad content from unauthenticated sources in future.

5.5 FACILITATING CONSISTENT AND EFFECTIVE REPORTING

Detailed information about the scale and nature of online scams is crucial to inform strategies for preventative and remedial action. But our research shows that scam reporting at a global level is fragmented, inconsistent and unreliable. Improvements could be made in four key areas:

- There is a need to address the low levels of scam reporting. Consumer education to 'normalise' scams could help to overcome the stigma wrongly attached to it. Consumers need to understand that anyone can be a victim of a scam and that reporting it quickly could benefit others. To facilitate this, victims need clear, timely information about where to report scams and submit complaints. Social media platforms must make it easy for consumers to flag scams, and other harmful content. For example, Facebook's UK operations are developing a new 'scam ads' reporting tool as part of a legal settlement (see case study in Section 4.4).

- Comprehensive data collection systems need to be in place to record and analyse all online scam incidents, including their channels of origin. Although a single point of data collection for fraud in each country would be ideal, it is recognised that multiple organisations might deal with scam reports. To facilitate sharing of insight, between national and global agencies, classification of data should be consistent.

- If consumers can see evidence that reporting leads to positive action, in the form of enforcement and redress, this will help to build trust in the system.

5.6 IMPROVING STAKEHOLDER COOPERATION

Establishing better collaboration and cooperation between all stakeholders at a global level is essential to providing an effective solution to the growing problem of social media scams. Improved communication between enforcement agencies would facilitate the sharing of insight and intelligence to focus resources in areas that they are needed most.

Government agencies, consumer protection authorities and social media platforms can also work together to identify threats and make sure that scam victims have access to appropriate support and remedial action. For example, we found good practice of banks working with credit companies to ensure that consumers can be reimbursed when they've lost money to a social media scam.

5.7 RAISING CONSUMER AWARENESS

Encouraging conversations around scams is hugely important, as one of the greatest barriers to understanding and preventing social media scams is the reluctance to report. Consumer education campaigns play a central role and can significantly reduce the number of victims and level of detriment. Information should focus on:

- Recognising scams – up-to-date information about how to spot scams, the latest scams to watch out for and potential risks
- Preventing scams – how to protect themselves online and what action to take if they spot a scam
- Reporting scams – consumers need clear advice on where to report scams and why this is important

Consumer organisations, consumer protection authorities, enforcement agencies, private sector organisations, such as banks, and social media platforms themselves, have a shared responsibility for educating consumers. These organisations need to think about the best way to target consumers and ensure the right information reaches the right people at the right time. This might include creative use of social media, and other channels, to share information. As illustrated by the Spanish police (see Section 4.1), engagement beyond simple warnings and news articles can be successful in normalising the issue and encouraging other victims of social media scams to have the confidence to report their experiences.

Central to protecting consumers internationally, is a solid foundation of consumer protection legislation at a national level, which establishes clear rules and responsibilities for effective monitoring and enforcement.

6. CONCLUSION

Social media scams present an increasing threat to global consumers and complex challenges to those involved in consumer protection. Tackling this growing form of sophisticated consumer detriment requires a multifaceted, collaborative and innovative approach.

Central to protecting consumers internationally, is a solid foundation of consumer protection legislation at a national level, which establishes clear rules and responsibilities for effective monitoring and enforcement.

Our study shows that the consumer experience of social media scams varies by country, so national consumer protection authorities and governments must take local differences into account when developing strategies to tackle the issues.

However, it is essential that the bigger picture is taken into account. Social media scams are omnipresent and dynamic in nature, operating across national borders. To ensure the greatest benefits for consumers, solutions must also adopt a cross-border approach. When it comes to tracking down criminals that perpetrate scams on social media and enforcing the law, international cooperation and collaboration is crucial to ensure a consistent approach and sharing of intelligence. Voluntary agreements between stakeholders also help to set clear rules in terms of detecting, preventing and responding to scams.

International standards could be a valuable tool in tackling global online fraud, detailing good practice for social media platforms and other businesses about how to identify, and respond to, harmful content. Standards already exist in the digital space, but the potential for new standards should be explored.

Social media platforms, where interactions take place, are in the most powerful position to deliver positive change for consumers. Platforms need to take greater responsibility for consumer protection and be proactive rather than reactive. This commitment can be demonstrated by having secure systems, policies and procedures in place to minimise, detect and respond to fraud.

Innovative technological solutions are vital to keep up with the fast pace of change. Artificial intelligence and digital tools have great potential to protect consumers by authenticating sources and identifying harmful content and options should be explored. As social media platforms and online marketplaces evolve, these digital safeguards should be built-in to ensure that consumer safety is inherent in system design.

Underpinning everything is a shared responsibility to raise consumer awareness and remove the misplaced stigma currently attached to scams. Social media scams are a crime and consumers must be encouraged to report them as such.

As social media continues to grow in size and influence, it is increasingly important that consumer protection is at the heart of platform design and delivery. To address global challenges, those tasked with consumer protection must work together to drive improvements, minimise detriment and build a secure digital world that consumers can trust.

Social media scams are a crime and consumers must be encouraged to report them as such.

7. APPENDIX

Country	Population	Social media users	Scam conversation volume	Scam mentions per social media user*
Nigeria	186M	19M	144.5K	0.76%
US	327.7M	190M	1.3M	0.66%
UK	65.6M	38.5M	188.9K	0.49%
Spain	45.6M	27.M	51.4K	0.19%
Argentina	43.9M	24.2M	40.7K	0.17%
Chile	17.9M	13M	9.3K	0.07%
India	1.3B	283.8M	63.7K	0.02%
Saudi Arabia	32.3M	18.1M	4.3K	0.02%
Egypt	95.7M	32.1M	1.9K	0.01%

Notes: Table sorted by scam conversation volumes by social media user (scam conversation volume divided by number of social media users) B=billion, M=million, K=thousand*

CONSUMERS INTERNATIONAL

COMING TOGETHER
FOR CHANGE

Consumers International brings together over 200 member organisations in more than 100 countries to empower and champion the rights of consumers everywhere. We are their voice in international policy-making forums and the global marketplace to ensure they are treated safely, fairly and honestly.

Consumers International is a charity (No.1122155) and a not-for-profit company limited by guarantee (No. 04337865) registered in England and Wales.

consumersinternational.org
@consumers_int
/consumersinternational