GSMA

Fraud and Scams:
Staying Safe in the Mobile World

February 2025

GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at **www.gsma.com**

Follow the GSMA on Twitter/X: **@GSMA**

Contents

GSMA

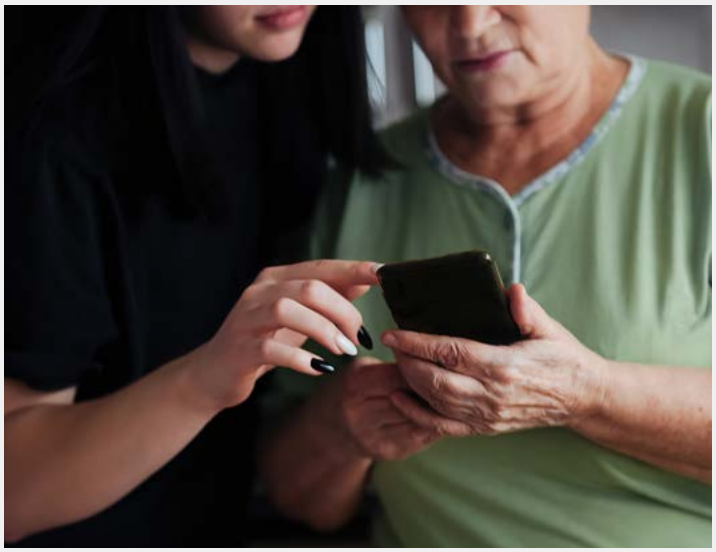
1. Executive Summary

The global financial cost of cybercrime, including fraud, is projected to be USD 15.63 trillion by 2029. The outcome of this threat for consumers can be significant financial loss, considerable emotional distress, and the erosion of trust in digital services, creating a barrier to the adoption of beneficial technologies. Despite efforts by industry to prevent fraud, criminals have found a way to bypass technical defences and target the weakest link through 'social engineering' - human behaviour. Social engineering involves the manipulation of individuals resulting in them making a financial transaction or sharing personal information. Various methods are used including 'phishing' which are emails that contain links directing victims to a fake website, or 'romance fraud' where a person is tricked into a fake relationship with a scammer, ultimately making financial payments to them.

The following is a very familiar scenario:
Very common fraud scenario: An older individual, let's call her Emma, is reasonably familiar with technology and has a social media profile that her relative, helped her set up so she could stay connected with family and friends. Her relative also assisted with setting up online shopping and banking through her bank's app, which used facial recognition for security.

One day, Emma receives a call from someone claiming to be a bank representative. This "representative" informs her that a number of bank accounts have been compromised by fraudsters, and her account is one of them. To secure her funds, the representative explains that a new account has been created and asks her to quickly transfer her money into this account to protect it from being stolen.

Concerned and wanting to secure her finances, Emma follows the instructions and authorises the transfer. Later, when Emma explains the situation to her relative, they contact the bank on her behalf to inquire about the new account.



The bank had no knowledge of the call or any such account, revealing that Emma had fallen victim to a fraudulent scam, and the money had been transferred to the fraudster's account. The bank is now working to trace the funds.

The adaptability and global reach through technology such as AI is also allowing organised criminals to perpetrate social engineering at scale and refine their deceptive tactics to target diverse populations across multiple regions. Vulnerable groups such as the elderly are often targeted in many developed markets like UK, Australia and the US, and mobile money users are a key target for criminals in the Africa, Asia Pacific and Latin American regions. A GSMA study recently found that social engineering, SIM swap fraud and identity fraud were among the top concerns within those regions.

In an effort to address the issue, mobile operators invest significant resources in identifying, filtering and blocking fraudulent traffic on their networks, however, these crimes often involve a sophisticated and organised chain of events - so technical measures alone are not sufficient. The mobile industry cannot solve the issue in isolation as the famous saying goes "it takes a village." This means that a comprehensive and multi-stakeholder effort is needed, with social media platforms, financial institutions and consumer organisations all playing a part alongside support from governments and regulators. Social engineering fraud is a global problem. Intelligence gathered for data such as INTERPOL shows that organised criminal gangs often based in multiple countries are able to scam victims in different parts of the world. Consequently, it has never been more important for all stakeholders of the value chain to share intelligence and enable law enforcement agencies to take rapid action resulting in criminals being brought to account. Mobile operators protect their customers in a number of ways, including by swiftly acting on fraud threats and behaviours, sharing intelligence with industry and other sectors (for example, through the GSMA Fraud and Security Group), providing regular employee training and educating their customers in simple helpful ways enabling them to recognise and report fraud.

Consumers can protect themselves by exercising awareness and caution, being vigilant and recognising warning signs by learning about the common impersonation types and methods used.

The highly complex and multifaceted issue of mobile fraud and scams presents a critical challenge and unique opportunity for the industry to take charge.

Fraud in all its forms is a complex and illegal issue. As technology evolves and social engineering fraud rapidly expands at a disturbing pace, a holistic approach to prevention is needed. Mobile operator actions can only influence consumers' behaviour with the objective of mitigating the risk of fraud through prevention and implementing the highest possible levels of security appropriate to their markets. While mobile operators continue in their efforts to address the issue of social engineering, they cannot work in isolation nor can they take measures that risk them breaching confidentiality of communications.

Given the enormity of the problem, it requires cross-industry and cross-sectoral collaboration, with support from governments and regulators. While legislation and regulation focus on the criminals and perpetrators, education and awareness are the primary ways to foster consumers' ability to protect themselves against social engineering fraud. In particular, in markets with a lower level of understanding, consumers today are often not leveraging the information or tools available to them. It is important that providers of the services, including operators, banks, and financial institutions, can do more to increase awareness and education. Consumers can also play their part by using the tools and information available to help navigate the online world safely and securely.

Governments and regulators can foster a collaborative approach to developing measures by:

- empowering consumers with knowledge and tools to protect themselves
- establishing frameworks to facilitate cross-sector and cross-border data sharing
- introducing regulatory sandboxes to pilot new fraud prevention technologies and services
- participating in established frameworks and conventions, e.g. ASEAN, Malabo, Budapest

Mobile operators can protect their customers by:

- swiftly acting on fraud threats and sharing intelligence with industry and other sectors
- providing regular employee training on security, fraud and scams
- encouraging employees to report suspicious behaviour
- publishing simple helpful information for consumers

Consumers can protect themselves by exercising awareness and caution, and by:

- being vigilant and recognising warning signs
- ensuring device software is kept regularly updated
- learning about the common impersonation types and methods used
- implementing two-factor authentication and employing strong, unique passwords

GSMA security information and working groups
GSMA works with industry to continually enhance the security support offered to operators as new threats targeting the mobile ecosystem emerge. Collaboration, partnership building and intelligence sharing are the cornerstone of the GSMA's work. We convene governments, intergovernmental organisations and leaders of the mobile industry – ensuring meaningful engagement, dialogue and debate on policy and regulatory issues.

The Fraud and Security Group (FASG) drives the industry's work on fraud and security matters related to mobile technology, networks and services.
https://www.gsma.com/get-involved/working-groups/fraud-security-group

The GSMA's Telecommunication Information Sharing and Analysis Center (T-ISAC) is the central hub of information sharing for the industry where threats can be reported in near-real time to allow for a coordinated and measured response.
https://www.gsma.com/solutions-and-impact/technologies/security/t-isac/

The GSMA Mobile Cybersecurity Knowledge Base is a leading example of the industry's collaborative efforts.
https://www.gsma.com/solutions-and-impact/technologies/security/5g-cybersecurity-knowledge-base/

Further resources on GSMA Security and Fraud is available here:
https://www.gsma.com/solutions-and-impact/technologies/security/

GSMA reports are a useful resource to provide information on fraud and security at a global and regional level.

Safety, privacy and security across the mobile ecosystem
https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2022/10/Safety-privacy-and-security-across-the-mobile-ecosystem.pdf

Mobile Telecommunications Security Landscape reports
https://image.email.gsma.com/lib/fe8213727c6d077572/m/1/89289301-46d1-4744-a9a3-a07b3304af4b.pdf

Mobile money fraud typologies and mitigation strategies
https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/gsma_resources/mobile-money-fraud-typologies-and-mitigation-strategies/

Consumer Attitudes Toward Fraud and Opportunities for Mobile Network Operators in South East Asia
https://www.gsma.com/about-us/regions/asia-pacific/gsma_resources/consumer-attitudes-fraud-oppty-sea/

Responsible AI Maturity Roadmap
https://www.gsma.com/solutions-and-impact/connectivity-for-good/external-affairs/responsible-ai/

GSMA™

2. Background and introduction

The rapid advancement of digital technology has opened new avenues for fraudsters, significantly impacting individuals, businesses, and society at large. Fraud is a global issue, and however perpetrated, can have a profound and lasting impact on individuals. It knows no boundaries and has emerged as a significant global threat, driven by widespread internet use, interconnected digital systems and a growing reliance on digital technology for financial and other transactions. Victims of fraud can often lose large sums of money and spend significant amounts of time and effort disputing transactions, recovering losses and restoring identities. This can lead to long term distrust in digital services and hinder the adoption of beneficial digital technologies.

Human behaviour is often the weakest link in the security chain and criminals are increasingly turning to social engineering techniques to obtain the information they need to perpetrate their online crimes. Social engineering preys on human psychology, manipulating individuals into disclosing personal information or authorising transactions they believe to be legitimate. It can lead to the loss and theft of private personal information such as passwords, bank account details and medical records- increasing vulnerability to future fraud is identity theft. Stolen data obtained by the criminals if often traded illegally and used to commit further harmful and illegal activity, including identity theft and sim swap fraud, putting consumers at continuous risk even after an initial fraud event.

Fraudsters are drawn towards social engineering because it enables them to access online services, digital devices and personal information, without the need to navigate technical security defences such as firewalls and antivirus software. Fraudsters are constantly seeking new opportunities and adapting their scams very quickly and even becoming business-like in their approach, and the use of technological advancements such as Generative Artificial Intelligence (GenAI) enables organised crime networks to better target victims through 'phishing' to impersonate friends, family, a bank or an authority figure such as an employer. Sometimes referred to as 'human hacking,' it exploits human weaknesses through psychological manipulation and plays on human emotions such as fear, curiosity and sympathy, to manipulate an individual into revealing personal sensitive information or making a financial transaction.

The global financial cost of cybercrime (criminal activity that involves a computer, network, or networked device), including fraud, is projected to escalate from **USD 9.22 trillion** in 2024 to **USD 15.63 trillion** by 2029 (Statista[1]).

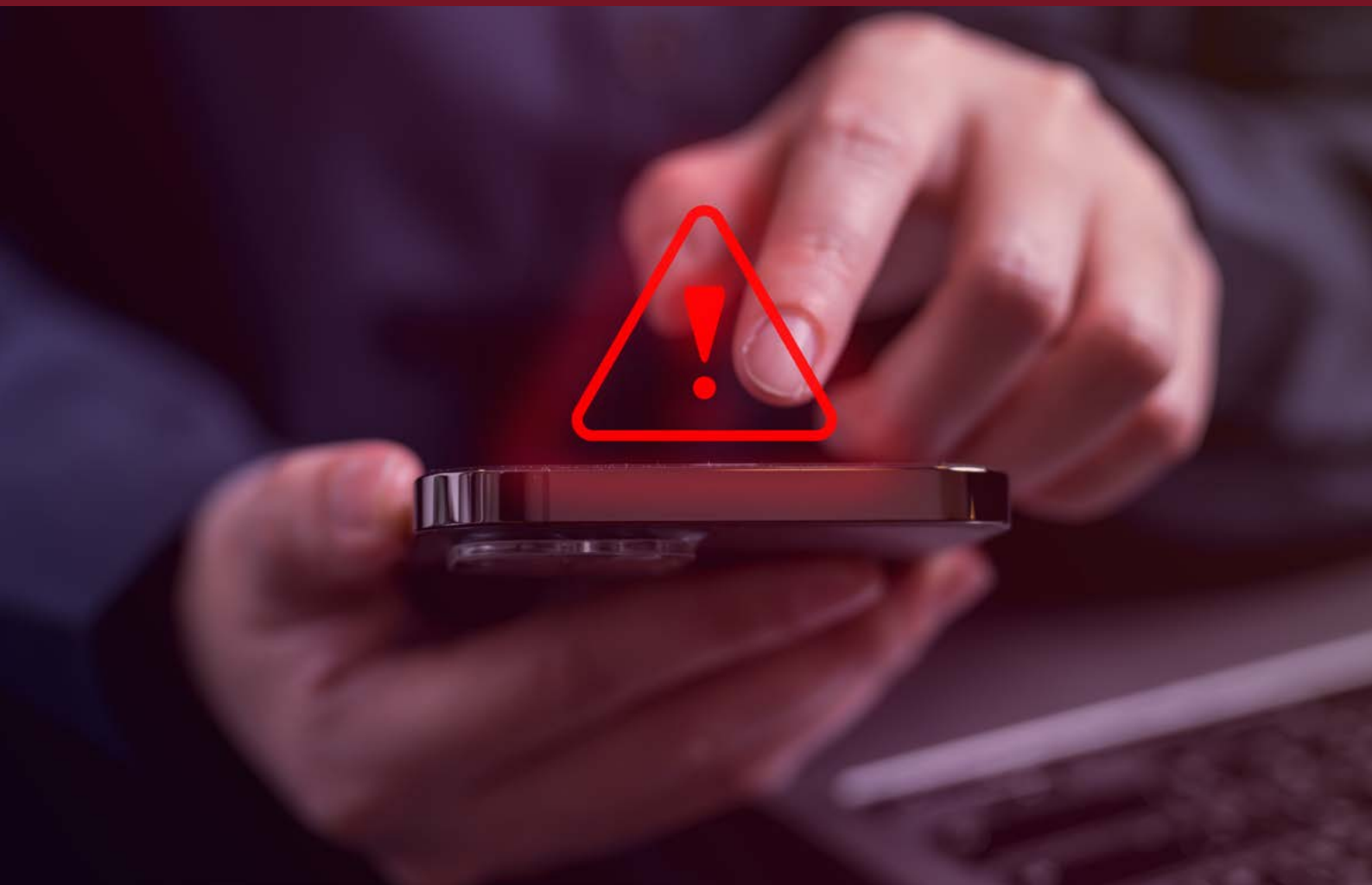
By the end of 2023, **5.6 billion people** or **69% of the global population,** subscribed to a mobile service and **58% of the world's populatio**n used mobile internet, equating to **4.7 billion users.**
(GSMA Mobile Economy Report, 2024[2]).

In 2023 criminals stole over **USD 1 trillion** from victims.
(Global Anti-Scam Alliance[3]).

71% of global organisations reported experiencing at least one successful email-based phishing attack in 2023.
(Proofpoint's 2023 State of the Phish Report[4]).

GSMA

3.
Common fraud types



Fraud and scams can be described using a variety of terms, sometimes overlapping, but each emphasising different aspects of deceptive practices employed by criminals to exploit victims. The following are some of the most common terms used.

Common Fraud Types

Authorised Push Payment fraud

When someone is deceived into sending money to a fraudster posing as a genuine payee from a trusted organisation such as a bank, to steal money.

Baiting

Where criminals offer something enticing, such as free software downloads, in exchange for personal information or system access. This can involve infected digital files or links.

Business Email Compromise

A type of fraud that involves criminals gaining access to a business's email system and deceiving employees into disclosing confidential information or transferring money.

Identity fraud

A form of impersonation that involves taking over a genuine identity of another or creating a fictitious, non-existent one.

Identity theft

Theft of an individual's personal information in order to commit fraud. Perpetrators typically obtain personal information or documents such as identity numbers or cards, biometrics or passwords and use them to assume the identity of others.

Impersonation

Where criminals pretend to be someone else, either online, by phone, or in person, to gain trust and manipulate the victim into disclosing confidential information or taking specific actions.

Phishing

Deceptive emails, messages (including SMS), social media or links to websites that appear legitimate, aiming to trick recipients into clicking and revealing sensitive information such as passwords, credit card numbers, or other personal data. This often involves impersonation, where criminals pretend to be a trustworthy entity, such as a bank, government agency, employer or well-known organisation.

Pretexting

Where criminals create a fabricated scenario or pretext in order to obtain information. This often involves impersonating someone trustworthy, such as a colleague or bank representative.

Robocall

An automated phone call that delivers a pre-recorded message, targeting a large number of recipients at a time. Robocalls can be used to carry out fraudulent behaviour by making unsolicited calls that deceive individuals into making payments or providing personal information, for example.

SIM Swap fraud

Whereby a fraudster tricks a mobile service provider into porting or transferring a victim's mobile phone number to a new SIM card under the fraudster's control.

Smishing and Vishing

Forms of phishing specific to mobile phones - vishing typically using voice calls and smishing using SMS. Criminals impersonate trusted entities and persuade victims to reveal sensitive information such as passwords, credit card numbers or other personal data. This often involves impersonation, where the criminal pretends to be a trustworthy entity, such as a bank, government agency, employer or well-known organisation.

Spear phishing

Phishing which involves targeting individuals, often impersonating someone the target knows personally. Criminals may spoof email addresses to make it appear as though the email is coming from a legitimate source (individual or company).

Spoofing

A deceptive practice where attackers manipulate online information, such as email addresses or contact names/numbers, to falsely represent their identity or that of a legitimate entity.

GSMA™

4.
Understanding Social Engineering

Criminals are increasingly turning to social engineering techniques to obtain the information they need to perpetrate their online crimes. Social engineering preys on human psychology, manipulating individuals into disclosing personal information or authorising transactions they believe to be legitimate. It can lead to the loss and theft of private personal information such as passwords, bank account details, identity numbers and medical records – increasing vulnerability to future fraud and identity theft. Stolen data obtained by the criminals if often traded illegally and used to commit further harmful and illegal activity, putting consumers at continuous risk even after an initial fraud event.

An alarming trend in social engineering fraud is the increasing sophistication of attacks.

- Romance scams otherwise known as 'pig butchering' is a form of social engineering where a criminal builds trust with their intended victim using information obtained, typically building rapport and confidence. Subsequently the victim is persuaded to make a financial transaction or investment (investment fraud or advanced payment fraud) usually into a fake scheme or account.

- SIM swap fraud specifically targets mobile phone users. The criminal contacts the victim's mobile provider and uses impersonation to manipulate the provider into porting the victim's phone number to the criminal's SIM, by claiming that they have lost their mobile phone. Once they have control of the victim's phone number and gained access to their account, they can transfer funds to other accounts (including their own) or withdraw money. In some cases, they may attempt to change the account settings, such as contact information, to hinder the victim's ability to regain control and receive notifications about the fraudulent activity.

In these scenarios, criminals have already collected information on the victims, commonly gained by 'scraping' information from popular social media websites.

GSMA™

5.
Impact and consequences for consumers and society

By the end of 2023, 5.6 billion people subscribed to a mobile service, which means that a sizeable volume of the population is exposed to fraud or scams, making social engineering a significant threat to consumers worldwide. Unlike traditional security threats which may be preventable through firewalls or antivirus software, social engineering fraud is particularly challenging because it directly targets individuals and uses human psychology. As a result, consumers can find themselves unknowingly aiding in their victimisation.

One of the immediate impacts of social engineering fraud on consumers is financial loss. Once fraudsters obtain personal information, they can access bank accounts, credit cards and initiate unauthorised loans. These financial impacts range from small, unnoticed transactions to substantial sums that drain a consumer's savings or build up debt in their name. Unfortunately, even when banks are able to provide some reimbursement, the lengthy and complex processes involved can add considerable stress to the victims. Fraud can have a devastating physical and emotional impact victims causing distress, especially for vulnerable individuals (including the elderly, the young and individuals with disabilities) who are very often targeted because of their vulnerability.

Ultimately it can affect a consumer's sense of trust and security in digital spaces. Many victims become wary of online services and reluctant to engage in digital transactions. This erosion of trust can negatively impact consumers' quality of life because many services and interaction are in the digital space such as banking and shopping. The fear of being targeted again may lead some consumers to avoid using digital services altogether, which can isolate them from the benefits of digital technology.

Fraudsters are constantly finding opportunities to harness new technologies to facilitate crime, but at the same time technology can be used to combat it. For example, AI is extensively used in the mobile and finance sectors to improve the detection and identification of fraud and scams, in filtering spam, and blocking harmful content, for example. However, there are several different ways in which criminals are leveraging generative AI tools to create advanced forms of social engineering tactics, such as removing the grammatical errors or to translate messages into native languages in phishing messages. The same tools are helping to create deep fakes (synthetic videos and fake virtual identities) that appear realistic and mimic family, friends or employers to engage victims in a conversation and socially engineer them into revealing sensitive information.

The cumulative impact of social engineering fraud extends beyond individuals to broader society, as increased consumer distrust can affect families, communities, online businesses and services. Additionally, social engineering fraud pushes companies to invest more in security measures, fraud detection, and consumer education which all result in costs which may ultimately be passed down to consumers in the form of higher fees or prices. In this way, social engineering fraud harms consumers both directly and indirectly, underscoring the need for stronger awareness and preventive measures to protect consumers from its insidious effects.

GSMA™

6.
An international threat

The effects ripple outwards, affecting global markets, increasing security costs, and hampering digital transformation efforts in vulnerable regions. On a global scale the impact of social engineering fraud is staggering. It is a worldwide issue often carried out by highly organised criminal gangs based in one country or region while targeting victims in another to avoid detection. The adaptability and global reach through the use of technology such as AI has allowed highly organised criminals to target diverse populations across different regions. Various organisations have undertaken research on the most prevalent social engineering tactics used in the different regions.

In a survey of mobile telecoms operators in the Asia Pacific region, 85% of operators ranked email phishing and SMS phishing (smishing) as top threats (GSMA Intelligence[5]). Unsolicited, or spam calls, are also on the rise; on average, mobile users in Asia Pacific receive one fraud call and two nuisance calls per month, with users in some countries receiving up to seven fraud calls per month (GSMA Intelligence[5]). In 2023, Australians lost AUD 2.74 billion to scams (Australian Competition and Consumer Commission[6]) with the elderly population most targeted resulting in losses for people over the age of 65 of AUD 120 million. Among the most common scams reported were phishing and identity theft. Asia has emerged as a focal point for romance scams, with criminal organisations in poorer countries across the region running scams as a business (INTERPOL Global Financial Fraud Assessment[7]). The region has also seen perpetrators impersonating law enforcement officers and bank officials to trick victims into disclosing credit card or bank account credentials, or part with large amounts of money.

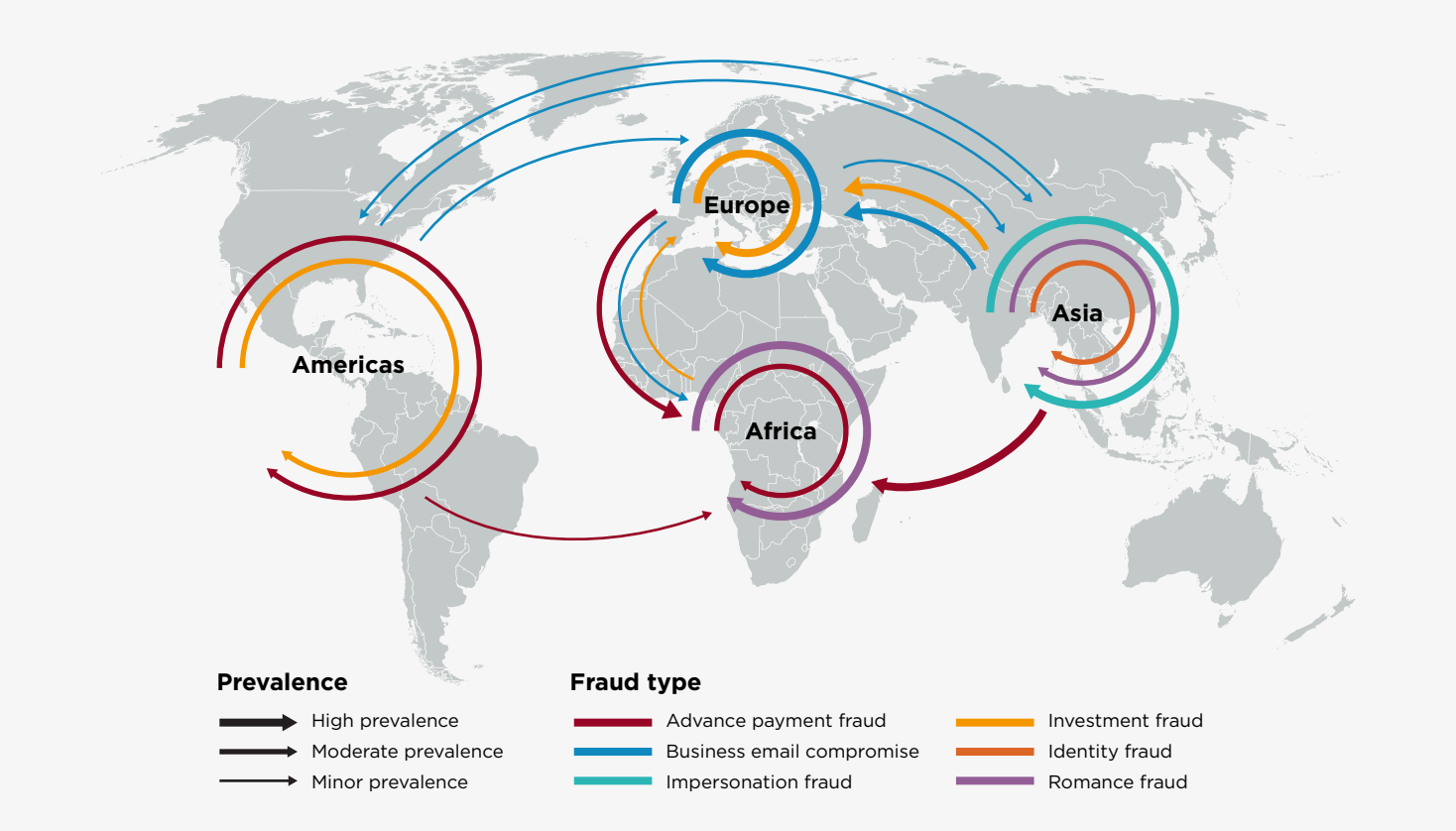
The USA reported losses of USD 10 billion to scams in 2023 with imposter (impersonation) fraud the top fraud category with reported losses of USD 2.7 billion (Federal Trade Commission[8]). Robocalls are also the cause of many complaints in the USA with consumers receiving approximately 4 billion per month (Federal Communications Commission[9]). The most frequently reported crime in 2023 across the state of California was phishing schemes (FBI Internet Crime report (San Francisco, 2024[10]).

In several Latin American countries phishing is one of the top concerns within the region (McKinsey[11]). According to 2023 data from analytics software company FICO, around 5% of Brazilians (8 million) have been victims of identity theft and fraud and another 19% claim to have “probably” or “possibly” fallen victim to this type of scam (GSMA Intelligence[12]).

INTERPOL's study on financial fraud examines trends across different regions (Fig.1) and across the most prevalent social engineering threats of investment fraud (a deceptive practice that induces investors to make purchases based on false information), advance payment fraud (a promise of a large sum of money in return for a small up-front payment), romance fraud and business email compromise.

Mobile money services in Africa, Asia and Latin America are also a common target for criminals. A study on mobile money conducted across Africa, Asia and Latin America cites social engineering, SIM swap and identity fraud among the top concerns (GSMA Mobile money fraud typologies and mitigation strategies[13]) and mitigating the risk of scams and fraud against mobile money users is a high priority for operators and providers in these regions. In Europe, investment, business email compromise and romance fraud remain the most common types of cyber-enabled fraud schemes, with phishing persisting as the most prevalent vector of attack (EUROPOL[14]).

Figure 1:
Regional trends in financial fraud



Source: Interpol

The global nature of social engineering shows that a cross-sectoral and international approach is required to bring change on a large scale. In June 2024, a global police operation involving INTERPOL (Operation First Light 2024[15]) disrupted a criminal online scam network spanning 61 countries, targeting phishing, investment fraud, fake online shopping sites, romance and impersonation scams. It led to the arrest of 3,950 suspects and identified 14,643 other possible suspects across all continents.

GSMA™

7. Countermeasures

To combat social engineering fraud, governments, regulators and the mobile industry are employing various legal, regulatory, technical and educational measures.

Education and Awareness Campaigns

As criminals continue to adapt their methods, public awareness efforts remain key to equipping individuals with the knowledge they need to safeguard their personal and financial information. Public awareness campaigns such as the UK's Take Five campaign[16] led by UK Finance provides practical advice on how the public can protect itself from financial fraud, particularly impersonation fraud whether by phone or online. By urging consumers to stop and consider whether a situation is genuine before acting, the campaign helps build a more fraud-resilient population. Mobile operators also have their own training programmes in place for their employees and publish information on their websites to help customers understand how to protect themselves and prevent themselves from becoming victims.

Mobile operator measures and initiatives

Technical measures – To protect their customers, mobile operators are investing significant resources in solutions which include firewalls, authentication mechanisms, robust information security policies and continuous system monitoring and reporting mechanisms. SMS Sender ID protection registries are also in place in some countries which allow organisations to register and protect the message headers used when sending text messages to their customers, limiting the impact of SMS phishing and spoofing.

Reporting services – Mobile operators provide spam reporting services. In the UK, the 7726 service[17] allows mobile customers to report unwanted SMS messages or phone calls to their provider who in turn will update their network protections accordingly. Operators in Canada use the same 7726 number to allow the public to report scams (Government of Canada[18]). In Finland scam calls and SMS have been a problem since 2020 when approximately EUR 7.1 million was lost to technical support scam calls. Authorities and operators have been cooperating to tackle the implementation of prevention measures based on the ability of operators to receive calls from abroad in a controlled manner. This has dramatically reduced the numbers of scam calls to EUR 600,000 in 2022 (Global Anti-Scam Alliance (GASA)[19]).

Collaboration - Cross-sectoral collaboration is also important. In the UK, the GSMA and UK Finance have joined forces to provide a collaborative framework for the UK's leading mobile network operators and banks to develop and launch Scam Signal[20], a new solution delivered to help address Authorised Push Payment fraud. Scam Signal is delivered via an Application Programmable Interface (API), enabling banks to better identify and stop fraudulent bank transfers by analysing real-time network data and identifying correlations between phone calls and fraudulent bank transfers. Since 2023, mobile operators in many regions - including Asia Pacific and Latin America - are collaborating on Open Gateway APIs in their regions to combat fraud and digital scams.

Countering mobile money fraud

In many Sub-Saharan African countries where mobile money services are highly popular, enhancing security in these platforms is a critical focus. Kenya's M-Pesa and similar services in other countries have integrated biometric authentication, improved encryption, and enhanced fraud detection systems to protect users from impersonation, SIM-swapping, and phishing attacks. In North Africa, mobile operators are taking steps to counter fraudulent SIM swapping through increasing the amount of training given to retail staff in addition to implementation of multifactor authentication. The GSMA report Mobile Money fraud typologies and mitigation strategies[21] provides a detailed classification of the various forms of fraud that can occur in mobile money systems and to identify general tendencies, the strategies typically employed by mobile money fraudsters, and an overview of useful tactics, tools, and guidelines for preventing, detecting, and responding to occurrences of mobile money fraud.

GSMA Open Gateway

Some mobile operators are looking to implement the GSMA's Mobile Connect and GSMA Open Gateway APIs to improve user authentication. Some of the Asia Pacific's region's mobile operators are collaborating through the GSMA Open Gateway[22] framework to tackle online fraud and help increase consumer trust in new digital services across Malaysia, Singapore, and Thailand. A number of APIs are aimed at improving digital security by addressing online fraud and protecting the digital identities of mobile customers (GSMA Intelligence: APAC APIs[23]). Globally, mobile operators from across all regions (Asia Pacific region, Europe, Latin America, Sub-Saharan Africa, Middle East and North Africa and North America) are committed to deploying APIs to reduce risk of fraud, including the following:

- **Number Verify** checks that the user is interacting with a service from a device with the mobile phone number that has been registered and paired with the device. It removes the need to use another authentication method such as one-time pin/ password.
- **SIM Swap** checks the last time the SIM card associated with a mobile number was changed so that onboarding procedures are reinforced by identifying suspicious SIM card activities thereby reducing the risk of identity theft.
- **Device Location verification** provides security in location-dependent transactions by allowing an application to validate that a mobile device is in proximity of a given location.
- **Know Your Customer** provides a safer onboarding process by validating user contact information quickly and easily using data from the mobile network. It aids compliance with AML/KYC regulations on money laundering and guards against identity fraud/theft.

The GSMA is a signatory to the One Consortium initiative[24] aimed at reducing spam, spoofing, and other unwanted communications by collaborating with regulators, policy makers and law enforcement agencies to share insights and develop strategies. GSMA facilitates activity through events and working groups providing the ability for its member operators to share insights and intelligence on fraud and scams as well as guidance and mitigation measures. They include the Mobile Cybersecurity Knowledge Base[25], Fraud And Security Group (FASG)[26] and Telecommunication Information Sharing and Analysis Centre (T-ISAC)[27].

Regulatory and legislative measures

Fraudulent activity is addressed by a variety of laws and regulations worldwide, with specific legal frameworks varying by country. Some dedicated laws such as the UK's Fraud Act 2006 which directly targets fraud by false representation. Others are introducing new legislation, for example, Australia is introducing legislation which implements the Scams Prevention Framework, allowing government to designate sectors (e.g. banks, telecoms, social media and direct messaging services). Financial regulators worldwide have enforced stricter 'Know Your Customer' (KYC) requirements to ensure businesses verify the identity of their clients, reducing the likelihood of impersonation fraud. In some countries, regulators have introduced guidelines that require banks and financial institutions to implement fraud detection systems, such as transaction monitoring and customer behaviour analytics. Financial institutions and regulators also share information on known fraud schemes and actors to better prevent cross-border impersonation fraud.

In 2024, the Department of Telecommunications (DoT) - in conjunction with the telecoms providers - has implemented measures to block incoming international spoofed calls before they reach mobile consumers. The UK regulator, Ofcom, is taking steps to tackle spoofing by exploring enhanced call tracing solutions[28] which aim to improve identification of the source of fraudulent calls and exploring options to block calls from abroad which are spoofing a UK mobile number.

Robocalls in the USA have been the source of many consumer complaints over recent years and seen to be a vehicle for fraud. Illegal and unwanted calls (including robocalls) were the single largest source of consumer complaints to the Federal Communications Commission (FCC) and the reason for many thousands of complaint to the Federal Trade Commission (FTC).

Codes of Practice - Governments and regulatory bodies are recognising the importance of providing clear guidelines and educational resources to help protect consumers from the ever-evolving tactics of fraudsters. Scam codes, such as those being introduced in Australia, outline the responsibilities of various industries, including telecommunications and financial institutions, ensuring that they collaborate effectively to combat fraud. These codes set out specific duties, such as blocking suspicious calls and freezing fraudulent accounts, empowering organisations to take swift action when fraud is detected.

International frameworks

As social engineering and impersonation fraud often transcend national borders, international cooperation is critical in combating these global threats. Countries and organisations around the world are increasingly collaborating to harmonise legal frameworks, share intelligence, and coordinate cross-border enforcement efforts. International frameworks exist to deal with fraud and social engineering as part of the overall cybersecurity mechanisms, such as ASEAN and African Union's Malabo Convention[29]. The USA's FTC[30] and the consumer protection authorities of Chile, Colombia, Mexico and Peru have established mechanisms to combat fraud. GASA's GIRAF[31] (Global Informal Regulatory Antifraud Forum) is an initiative to foster cooperation between European National Regulatory Authorities (supported by GSMA).

The Council of Europe's Budapest Convention on Cybercrime[32] (also known as the Budapest Convention) serves as a legal basis for international cooperation, harmonising national laws and improving investigative techniques. It encourages international cooperation when investigating and prosecuting different types of cybercrimes, including online fraud and impersonation schemes. The Malabo Convention is a pan-African agreement creating a unified legal framework for data protection and cybersecurity. It criminalises activities including identity theft and emphasises the importance of cooperation among African countries to combat cybercrime. It came into effect in June 2023 after the required 15 African countries ratified it. In August 2024, the UN Ad Hoc Council approved the 2017 treaty which, in relation to cybersecurity and fraud, mandates United Nations member states to criminalise activities such as illegal access to information systems, misuse of devices and cyber-enabled forgery and fraud. It has extra-territorial reach and requires cross-border collaboration, including sharing of evidence, and the seizure of assets.

The importance of cross-sector collaboration and data sharing

The global nature of fraud means that no single entity or industry can combat impersonation fraud alone. Collaborative data-sharing platforms are now being developed to facilitate the exchange of information between key stakeholders, enabling faster detection and response to emerging fraud schemes. Public-private partnerships have proven successful in identifying and curbing fraudulent activity. The UK government and some of the world's biggest technology companies recently agreed a series of pledges to protect the public from online fraud. The Anti-Scam Centre in Australia and cross-border agreements such as in Europe and ASEAN aim to create seamless communication channels between financial institutions, mobile operators, and law enforcement agencies. By pooling resources and sharing real-time data, these collaborations enable quicker identification of fraudulent patterns and more effective disruption of criminal networks.

GSMA™

8. Further reading

1. Statista: Estimated cost of cybercrime worldwide 2018-2029
2. GSMA Mobile Economy Report, 2024
3. Global Anti-Scam Alliance
4. Proofpoint's 2023 State of the Phish Report
5. GSMA Intelligence report: Telco security landscape and strategies: Asia Pacific (October 2024)
6. Australian Competition and Consumer Commission (ACCC)
7. INTERPOL Global Financial Fraud Assessment, May 2024
8. Federal Trade Commission
9. Combating Scam Robocalls & Robotexts (Federal Communications Commission)
10. FBI Internet Crime report (San Francisco, 2024)
11. McKinsey & Company report: Fraud management perspectives for Latin America (March 2024)
12. GSMA Intelligence report: Telco security landscape and strategies: Latin America
13. GSMA Mobile money fraud typologies and mitigation strategies (March 2024)
14. EUROPOL: Internet Organised Crime Threat Assessment (2024)
15. INTERPOL 'Operation First Light' 2024
16. UK Finance Take Five campaign
17. How to report scam texts and mobile calls to 7726 (UK)
18. Reporting spam text messages to 7726 (Canada)
19. Global Anti-Scam Alliance (GASA)
20. Mobile and Banking Industries Join Forces to Fight Fraud Scam Signal
21. Mobile Money fraud typologies and mitigation strategies
22. GSMA Open Gateway initiative
23. GSMA Intelligence: APAC APIs
24. One Consortium initiative
25. Mobile Cybersecurity Knowledge Base
26. Fraud And Security Group (FASG)
27. Telecommunication Information Sharing and Analysis Centre (T-ISAC)
28. Ofcom – Tackling scam calls / enhanced call tracing solutions
29. African Union Malabo Convention
30. Federal Trade Commission Multilateral agreement
31. GASA's GIRAF (Global Informal Regulatory Antifraud Forum)
32. Council of Europe's Budapest Convention on Cybercrime

GSMA

1 Angel Lane, London, EC4R 3AB, UK
Tel: +44 (0)207 356 0600
Email: info@gsma.com