uk digital fraud

There's a gap in the UK's digital infrastructure and it's letting the fraud in

omnisperience

the overlooked process being exploited by fraudsters

On 12 November 2022, the House of Lords (HoL) published the long-awaited report by The Members of the Fraud Act 2006 and Digital Fraud Committee[1]. The report highlighted that fraud is the most commonly-experienced crime in England and Wales, accounting for 41% of crimes against the individual[2] and costing the British economy billions each year.[3] [4] The total cost of fraud to the UK economy is very hard to quantify[5] but a report by the Centre for Counter Fraud Studies at the University of Portsmouth estimated £137 billion[6] was lost to fraud in 2021.

The HoL committee observed that despite the scale of fraud, successive governments have done little to tackle it and insufficient resources have been dedicated to combatting it. Digitalisation and changes in the economy have accelerated the scale of fraud, with an estimated 25% increase since the Covid-19 pandemic[6].

Damningly, the HoL report says that stakeholders within the 'fraud chain' have failed to put adequate systems in place to prevent fraud – effectively making them facilitators of fraud. It argues that until all stakeholders fear significant financial, legal and reputational risks they will not act and concludes that a **new criminal offence** should be created of 'failure to prevent fraud'.

The committee calls out three sectors that have failed to build future-proofed counter-fraud mechanisms into their processes – either at the point of design or retrospectively. The first of these is the UK telecoms sector, which the authors say has no real incentive to prevent fraud and has allowed blame to be placed elsewhere for too long. The second is web-hosting providers, which aren't doing enough to prevent the registration of fraudulent domains. The third is the tech sector, which isn't accurately verifying the identity of those using online platforms.

In this report we look at the consequences of the HoL report for the telecoms industry – specifically focusing on a major security gap that is baked into the core telecoms infrastructure but usually overlooked.

The UK's **number portability process** is now so antiquated and inefficient that not only does it enable fraud but it effectively prevents co-operation with the banking sector to shut down the opportunity for fraud. Most other countries have already adopted a more modern, centralised approach that is not only more efficient and futureproof, but also enables the type of co-operation against fraud that the HoL is demanding. Telecoms firms have to be clear that failing to address this issue will expose them – as well as the UK economy – to a wide and growing range of risks.

pro-customer or pro-criminal?

it's time for uk telecoms firms to decide

Compromised mobile ID enabled fraudsters to steal £40,000

Speaking to the BBC's *Rip Off Britain* show, Wendy Darby explained how she fell victim to SIM-swap fraud.

Wendy ignored a text that confirmed her service provider was processing her new SIM request. She knew she hadn't requested one. Unfortunately, this was just the start of a fast-moving scam that saw her phone disconnected when fraudsters gained control of her account. They then proceeded to launder large amounts of money through her bank account and took out £40,000 in loans against her name.[7]

Customer had £1,000 siphoned from his account

When JC received a text from his service provider saying they couldn't process his request, he tried to contact them, but could only reach a prerecorded message. Two days later, he realised his phone had been disconnected and £1,000 was missing from his bank account.[8]

£137b
estimated annual uk fraud losses

80%
percentage of fraud that's cyber-enabled

↑ 400%
increase in sim swap fraud 2015–2020

why attack phone numbers?

The UK is disproportionately affected by fraud. The National Economic Crime Centre (NECC) told the House of Lords that this is due to factors such as widespread use of English as a second language and the high uptake of digital banking and shopping in the UK.

The volume and value of fraud has increased rapidly. In 1996-97 the National Fraud Initiative, for example, prevented £19 million of public sector fraud; in 2020-21 it prevented £443 million. To date it has identified and prevented £2.4 billion of cumulative fraud, overpayments and errors.

Increasing digitisation has seen criminals adapt their methods to take advantage of the opportunities afforded to them. Action Fraud, the UK's national reporting centre for fraud and cyber-crime, says that 80% of recorded fraud is now cyber-enabled. Giving evidence, Dr Alice Hutchings explained a typical fraud chain: "We can see people creating crimeware. People use that to compromise credentials. Those credentials may then be traded, and other actors use the credentials to monetise them and cash out".

How criminals use phone numbers to commit fraud

Today, phone numbers are one of the most important digital credentials an individual possesses. They are even a component in common security processes (such as One Time Passwords).

If criminals compromise a phone number, they can compromise an individual's entire digital identity, and gain access to their communications, social media, e-commerce and bank accounts. When the victim is an employee, compromised accounts can help criminals gain access to corporate systems.

The SIM itself is a robust and secure platform, and the telecoms industry has done a great deal to secure handsets (such as passwords, biometric locks, etc), which means criminals have turned their attention to the phone number itself. Today they can easily compromise phone numbers using two common and similar methods.

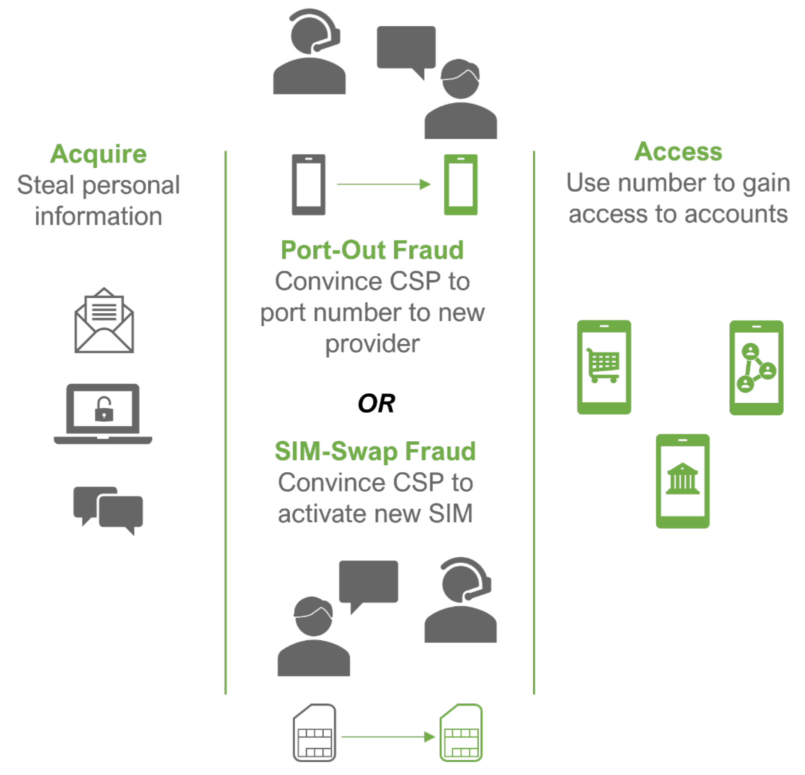
SIM swap fraud involves a fraudster taking control of a phone number by tricking CSP staff. The fraudster impersonates a legitimate customer – often using personal data captured during a phishing scam. The criminal then claims to have lost or damaged their SIM card, and asks to have a new SIM card activated. If staff are convinced by the story, they will port a legitimate number, along with the associated account and its data, to a SIM card in the fraudster's possession. All phone calls and texts will then be routed to the scammer.

Port-out fraud occurs when the fraudster poses as a legitimate customer and requests a porting authorisation code (PAC) to move to another network. As with SIM swap fraud, once the number is ported the account and digital identity of the legitimate customer is compromised.

Incidents of both SIM swap and Port-out fraud are increasing. Action Fraud reported a 400% increase in SIM swap fraud between 2015 and 2020, for example.

Closing the opportunity for this fraud is possible and other countries have acted to minimise the risk. But herein lies the problem. The UK's number portability system was implemented long before this type of cybercrime became an issue. It was designed with the purpose of making number portability as easy as possible for the customer in order to promote competition, increase choice and, ultimately, lower prices. But what's easy for the customer is also easy for the cyber-criminal.

Reasons for UK service providers to modernise number portability process


Acquire
Steal personal information
Port-Out Fraud
Convince CSP to port number to new provider
OR
SIM-Swap Fraud
Convince CSP to activate new SIM
Access
Use number to gain access to accounts

Source: Omnisperience 2023

Fraudsters used SIM swap attack to target bonds[9]

Sharon Fowler appeared on Channel 5's *Phone Scams: Don't Get Caught Out* show in 2022 to explain how a simple text alerted her to fraudsters' intentions to scam her out of thousands of pounds.

On her way home in December 2019 she received a notification from her service provider that her new SIM would be active within 24 hours. But Ms Fowler had not asked for a new SIM to be activated.

Concerned, she contacted her service provider. The agent she spoke to immediately put extra security on her account, but despite this the transfer still proceeded.

Although staff managed to reverse the process, fraudsters were still able to access Ms Fowler's NS&I accounts and attempt to transfer £10,000. NS&I's security team were able to block the transfer; but Ms Fowler's experience clearly highlights the risk customers are exposed to due to an insecure number portability process.

Worse, the process used by the UK for number portability makes it far harder to secure and impedes the type of inter-industry co-operation required to close the fraud window.

In Chile, banks can receive a consolidated list of recently-ported numbers so they can keep a closer watch on these for fraud – a service they pay for. While the US's Number Portability Administration Center (NPAC) provides a service called PortData Validate to businesses that rely on phone numbers to protect consumers, assess risk and mitigate fraud.[10]

These services are not possible in the UK, because there is no central record of ported numbers. Without a change to the process, each UK bank would need to request a list of recently ported numbers from every UK telco - making the task far harder if not impossible.

The risk is more than simple fraud

Phone numbers are an integral part of digital identity and cybersecurity. Number portability is no longer an arcane, technical facility of the telecoms sector, but a key vulnerability within the UK's critical digital infrastructure.

Short-term fraud is just part of the risk of having a sub-optimal number portability process. The criminal's intent might be a far more sophisticated or serious crime. Hijacking phone numbers and stealing customers' identities are steppingstones to obtaining new bank accounts or credit lines, claiming benefits, snooping on businesses, holding individuals and companies to ransom, and so on.

Ultimately, the current sub-optimal process represents a serious risk to the integrity of the UK's banking and payment systems, and is causing considerable extra work and costs for the financial services industry. Maintaining the integrity of phone numbers is therefore a vital part of preventing a wide range of cyber-enabled crimes and an important but completely overlooked component of improving the UK's resilience to cyberattacks.

Service providers are faced with a stark choice. Do they act to protect their customers, their own bottom lines and their reputations? Or do nothing, delay and debate the selection of a new system, and watch telecoms-enabled cybercrime continue to grow – and with it their own exposure to risk?

UK telecoms service providers need to decide whose side they're on and choose whether they're pro-customer or pro-criminal.

how we got here

What is number portability?

Number portability is a technical facility that enables customers of both fixed and mobile service providers to switch to another provider without having to change their telephone number. It is a vital component of a competitive telecoms market.

Prior to number portability being introduced, any customer changing service provider had to change their telephone number. This was a significant barrier to switching provider – particularly for business customers – and meant many remained with their current provider simply because they didn't want to incur the cost or effort associated with changing their number. A large swathe of customers were effectively locked into their existing provider and unable to benefit from lower pricing.

Current UK number portability process[11]

- Dates from 1997.
- Is non-centralised and bi-lateral.
- Is donor-led – ie the process is instigated by the customer's current network rather than the network they wish to move to.
- Uses onward routing (also known as 'indirect routing').
- Utilises a porting authorisation code or PAC (introduced in 2003).

1997 Number portability introduced

The UK was one of the first countries to introduce number portability – in 1997 for fixed line customers and in 1999 for mobile customers. This was instrumental in driving up competition and lowering pricing.

2006 Consultation

By 2006, the UK regulator, Ofcom, had come to the conclusion that the number portability process needed to be modernised to make it more robust and to accelerate the speed and volume of porting. It outlined a range of disadvantages of the UK process compared to using a central database (CDB) based process, which had subsequently become best practice internationally.

Ofcom identified an opportunity to design a more secure, efficient and robust process, with standardised data exchange, inter-operator billing, agreed routing methods and operating processes that would reduce porting timeframes for customers.

2007 Ofcom Decision

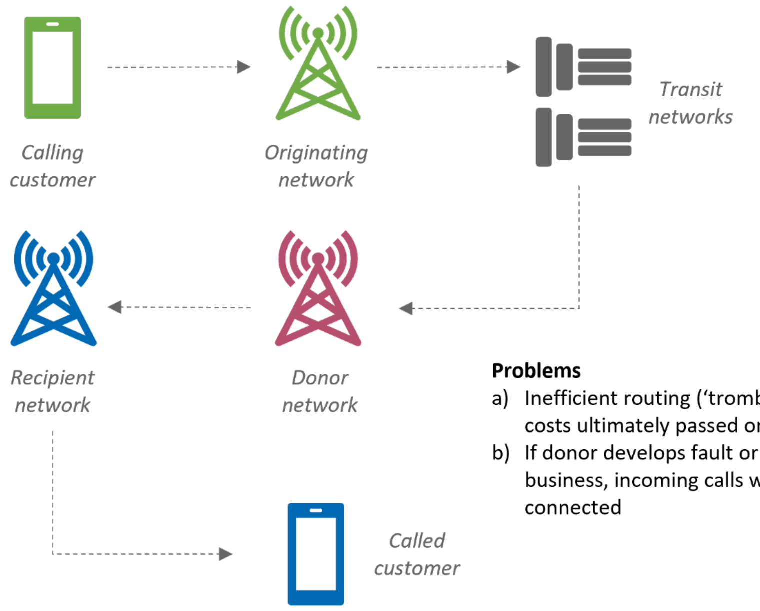
Ofcom decided to mandate a new number portability process and published this Decision on 29 November 2007.[12] The proposed process would use a central database of ported mobile numbers, with ported fixed numbers being added later. The process would become recipient-led and the timescale for porting reduced from two days to two hours.

2008 Appeal

In June 2008, Ofcom's Decision was appealed by Vodafone. They were supported by BT, Orange, T-Mobile UK, and O2. Hutchison (H3G) supported Ofcom.

The Competition Appeal Tribunal found in favour of Vodafone, which resulted in the proposed new process being set aside.[13]

UK number portability process is non-centralised and uses an inefficient onward routing process

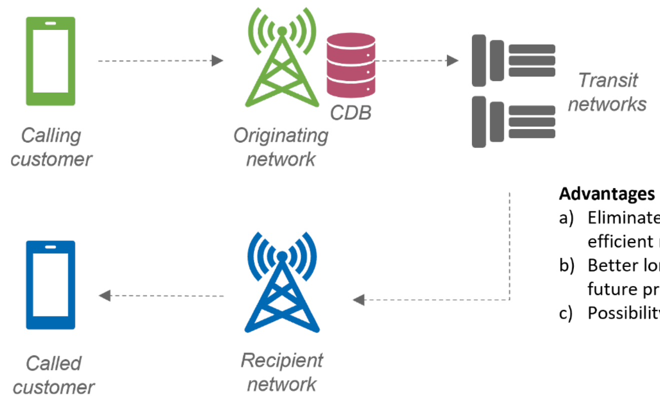


Problems

a) Inefficient routing ('tromboning'), extra costs ultimately passed on to consumer

b) If donor develops fault or goes out of business, incoming calls will not be connected

International best practice is now to use a centralised database process



Advantages

a) Eliminates donor network for more efficient routing

b) Better long-term solution, more future proofed

c) Possibility of increased security

Source: Omnisperience 2023

what's the alternative?

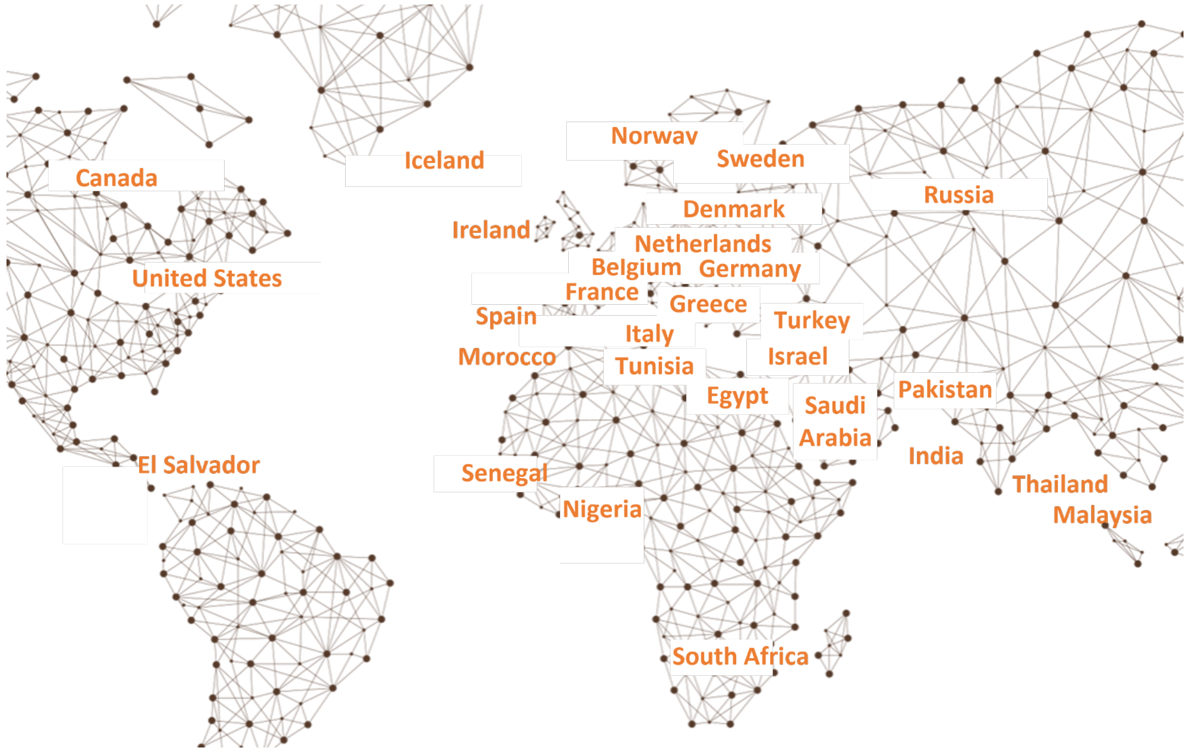
Since the UK introduced number portability in the 1990s, most other countries have opted for a process that utilises a centralised database (CDB).

A CDB approach means telecoms firms have up-to-date data on ported numbers which can be automatically queried to route calls directly to the network the number is currently assigned to (known as All Call Query or ACQ).

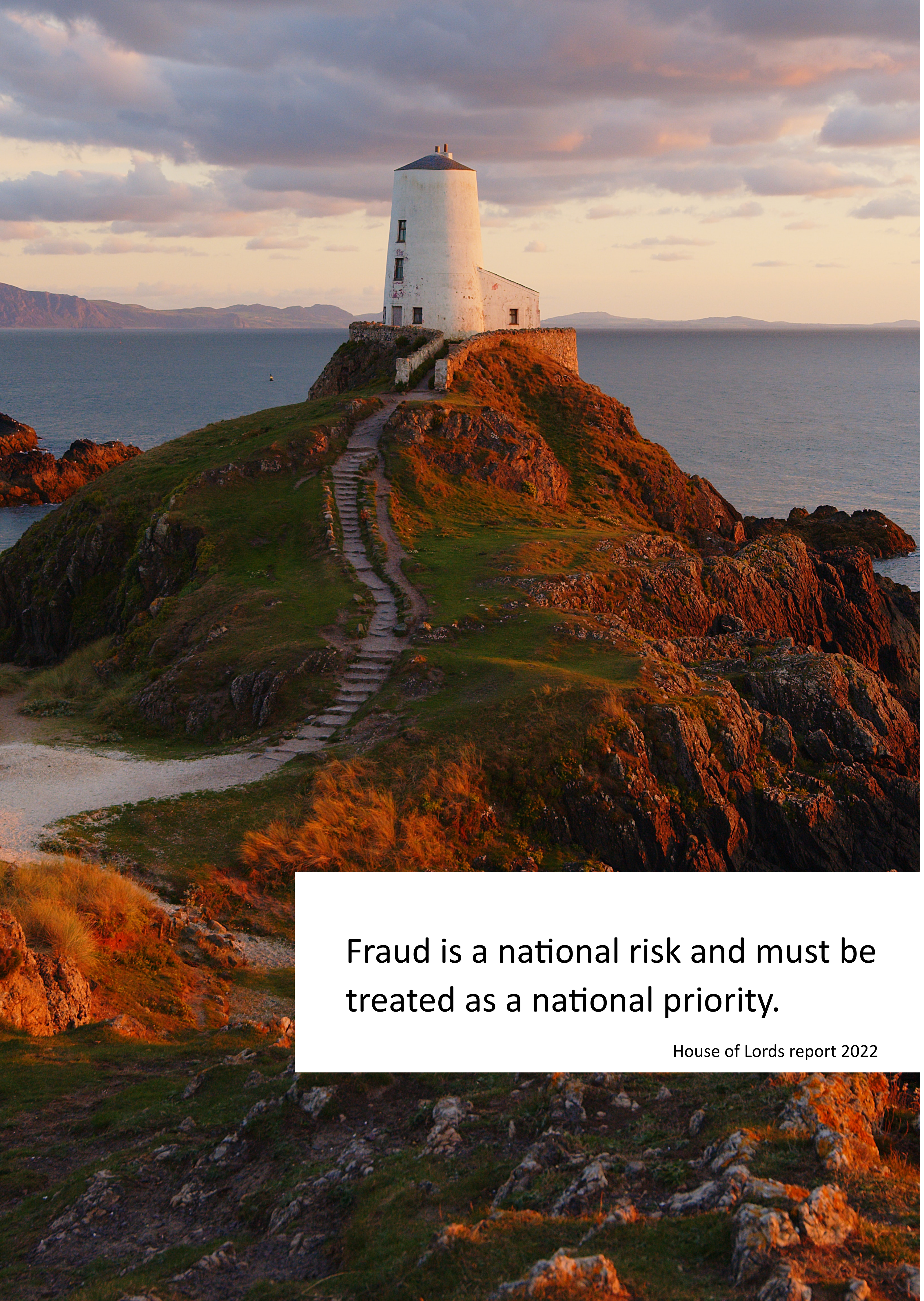
When Ofcom decided to replace the UK's process in 2007, centralised number portability systems that use the ACQ method had been successfully deployed in Denmark, Ireland, Italy, Hong Kong and the United States. And Singapore was in the process of implementing such a solution.

Since then, ACQ/CDB systems have been deployed worldwide and only a handful of countries continue to use the outdated onward-forwarding method used in the UK.

Centralised database systems are now used worldwide



Source: Omnisperience 2023



Fraud is a national risk and must be treated as a national priority.

House of Lords report 2022

why act now?

When the UK telecoms industry blocked change in 2008, it won on a technicality by arguing that the upfront cost might be too great and Ofcom's forecast costings weren't sufficiently robust.

Many countries have since discovered that the cost of implementing a new number portability process is quickly recouped through lower operating costs and there is now robust evidence around likely costs. While important, cost to the industry should not be the main motivation for replacing the UK's process.

In fact, there are a wide range of reasons why UK service providers should be urgently co-operating to address the problems associated with the country's antiquated number portability process.

Cybercrime and fraud has evolved

The UK's current number portability process was built for a very different market paradigm when cybercrime was still in its infancy. Social media, online banking and digital commerce had not yet been developed.

Cybercrime is now so widespread that it has been described as a 'cottage industry' enabled by crime-as-a-service according to one contributor to the HoL report. During all of this change, the mobile number – once simply a mechanism to call a specific phone – has evolved into a critical part of digital ID, making it a target for sophisticated criminals.

SIM swap and porting fraud alone cost the global telcoms industry over $3.2 billion in 2021, according to the Communications Fraud Control Association (CFCA)[14], but fraud is now a multi-industry phenomenon and cannot be seen in isolation as simply a telecoms issue.

When criminals gain access to a customer's mobile number and account, this impacts the customer's life, other industries such as banking and e-commerce, as well as the customer's employer (since compromised IDs can be used as a back door into corporate systems).

It's therefore essential that the UK telecoms industry stops considering themselves an operational silo and plays their part in tackling the global, multi-industry fraud chain.

Futureproofing for the 6G era

The speed of digital change meant that by 2006 it was apparent the UK's number portability process was no longer fit for purpose.

Today's UK telecoms market is very different to the market of 1997.

- There's been a huge increase in players in the UK telecoms market and a sharp rise in the number of customers – leading to a greater volume of switching.
- Voice calling has given way to data as the major traffic being carried.
- Society is increasingly connected, with ever-more services provided online and the rapid growth of the Internet of Things.
- Smart phones rather than feature phones are now the norm.
- The frequency of switching has increased – fuelled by SIMO contracts, for example.[15]

All of these factors have exacerbated the pressure on the current number portability process and further exposed its vulnerabilities and limitations. Routing inefficiencies and additional traffic associated with number porting will continue to grow, affecting both service quality and costs.

With the advent of 5G, and eventually 6G, as well as the growth of the Internet of Things (IoT), the UK is fast reaching a point at which the current process will buckle under the pressure.

Onboarding large corporate customers is already extremely difficult using the current process, which wasn't designed to 'bulk port' 1,000 or 10,000 numbers for the same customer. In future, it's as likely that IoT devices will need to be ported as consumer accounts. And it's a sobering thought that the porting of large-scale IoT implementations involving millions of SIMs will make the challenge of porting a large enterprise account seem trivial. The UK's antiquated number porting process thus threatens to undermine the growth and competitiveness of its IoT market, with customers locked into their service provider because it's so difficult for them to shift to a new one.

IoT devices are also vulnerable to hijacking and are not as well protected as people. The CFCA reported that in 2021 only 41% of service providers monitored IoT devices for fraud risks and abuse, but 35% said they had already experienced IoT-based SIM swap attacks. The organisation noted: "…IoT could face significant fraud abuse and [is] currently not adequately protected within the telecoms industry".[16]

Any replacement number portability process therefore has to be massively more scalable than the current one, so that it is able to meet the UK's future needs, and so that protection of both individuals and IoT devices can be built in.

Risk management

The HoL report specifically singles out the telecoms sector as being both lax and liable when it comes to fraud, and proposes a range of measures that UK telecoms service providers need to be aware of.

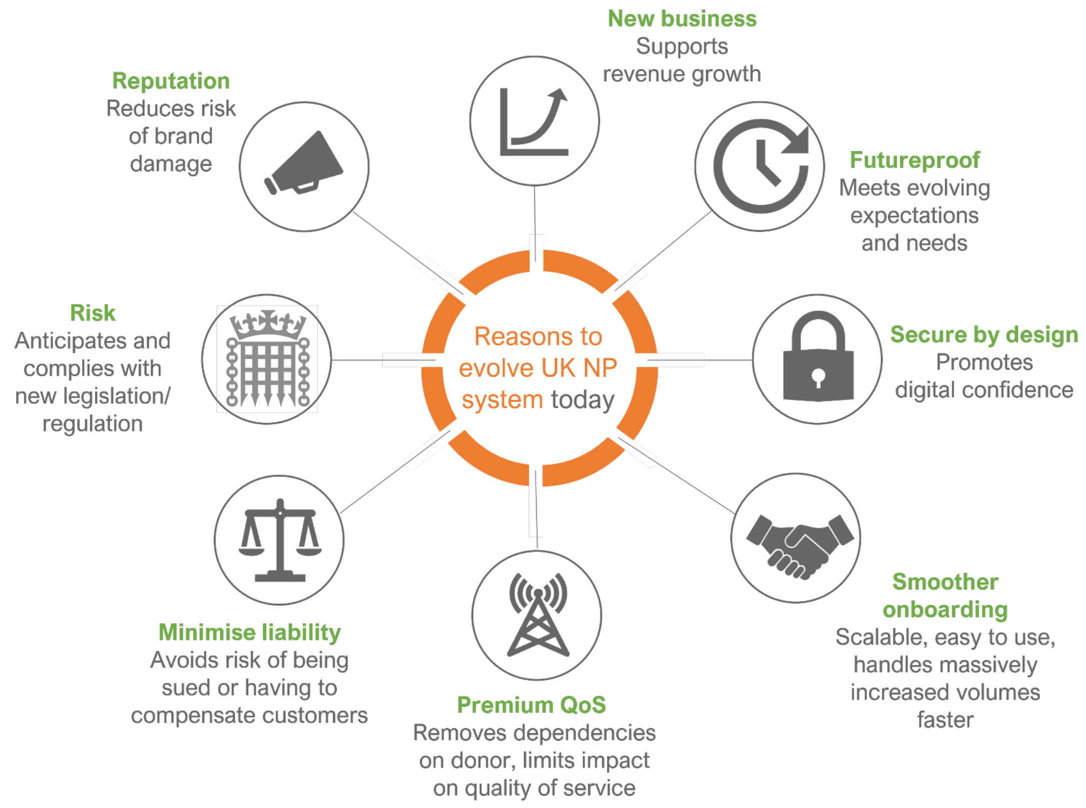
These include far more Parliamentary scrutiny of Ofcom, and by Ofcom of the telecoms sector. The committee recommends that Ofcom should present an annual fraud report to Parliament that includes a "comprehensive assessment of telephony fraud in order to tackle the worrying information deficit on the scale of the problem."

The committee welcomed the re-launch of the Joint Fraud Taskforce and other forums for discussion and cross-sector information sharing. It advocates more co-ordination between the telecoms and banking industries, and concludes the telecoms industry should supply real-time data on SIM-swaps and mobile number portability using the GSMA's Mobile Connect Account Takeover Protection standard, as well as identifying other data that further reduces the risk of fraud.[17]

While this is laudable, the recommendation is still focused on stopping fraud rather than proactively preventing it. In reality, this needs to be done in tandem with fixing the root cause of the fraud by replacing the number portability process with one based on a centralised database, as this would allow the UK to prevent fraud (as is done in countries such as the US).[18]

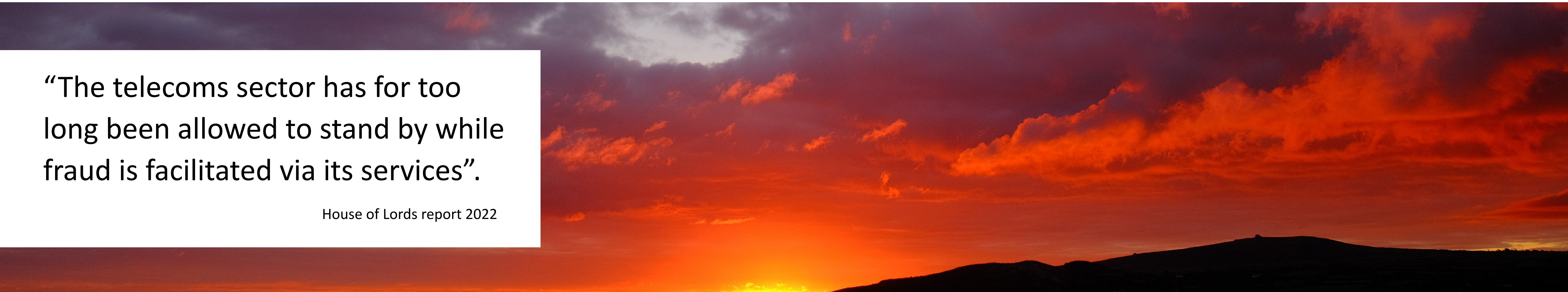
The committee also signalled its concern that industry forums are voluntary and do not maximise the potential for effective leadership in counter-fraud. "Fraud is a national risk and must be treated as a national priority," it notes, adding that forums must become more than "industry talking shops".

Reasons for UK service providers to modernise number portability process


Reasons to evolve UK NP system today
New business
Supports revenue growth
Futureproof
Meets evolving expectations and needs
Secure by design
Promotes digital confidence
Smoother onboarding
Scalable, easy to use, handles massively increased volumes faster
Premium QoS
Removes dependencies on donor, limits impact on quality of service
Minimise liability
Avoids risk of being sued or having to compensate customers
Risk
Anticipates and complies with new legislation/ regulation
Reputation
Reduces risk of brand damage

Source: Omnisperience 2023

Proposed changes to legislation include making inaction on fraud a crime, a clamp-down on the UK telecoms sector in particular, and amendments to the *Telecommunications (Security) Act 2021* to require telecoms firms to reduce the fraud taking place via its networks and services. The committee's proposal that corporate criminal liability should be extended to companies that cannot prove due diligence in preventing fraud is similar to the way GDPR makes companies liable for not adequately protecting personal data.



> "The telecoms sector has for too long been allowed to stand by while fraud is facilitated via its services".
>
> House of Lords report 2022

Fixed line number portability (1997)
Mobile number portability (1999)
Porting authorisation codes (2003)
Decision to introduce new NP process (2007)

1997-2007

Judicial review succeeds in blocking introduction of new process (2008)

2007-2010

2010-2016

2016-2019

2019-2022

2022

Right To Port introduced to enable customers to port up to 30 days after termination of contract (2023)
One Touch Switch streamlines switching process for landline and broadband customers (2023)

Reform number portability and close fraud gap?

2022-now

secure by design

To become a world leader in cybersecurity and fraud prevention, the UK must act proactively to prevent crime, rather than simply improve its detection and intervention abilities.

There is a significant opportunity for the UK telecoms industry to help the country meet these objectives by addressing the key vulnerability of the phone number as a gateway to stealing digital identity. The industry should work with key stakeholders from other industries (such as banks), utilise number portability best practice developed in other countries, and co-operate in industry forums to design a robust world-class number portability process that empowers choice and competition, is ready for the 6G era, and is **secure by design**.

But what does secure by design mean in practice within the context of number portability?

Simply put, it means developing a number portability solution that is built from the bottom up to be secure in terms of hardware, software, people and processes. Such a solution must be resilient to the type of risks that are likely to confront it both now and in future, and each component as well as the overall solution must be designed with security in mind. Importantly, it must facilitate inter-industry co-option to prevent fraud and be upgradable to meet emerging requirements.

omnisperience's view

The HoL report signifies advance notice that service providers will be held liable for their part in future cybercrime. Urgency in tackling the problems outlined in this report were underlined by a recent court case (August 2022), which found Vodafone liable for not protecting a customer from SIM swap fraud – even though the customer did not lose any money – due to what the judge termed "a serious breach" of its own procedures.[19] This case established a legal precedence of liability.

While the HoL report recommends information-sharing to minimise SIM swap and port-out fraud, effective information-sharing is almost impossible unless the UK implements a central national database of ported numbers. The root cause of this type of fraud in the UK is a number portability process that is obsolete, no longer fit-for-purpose, and overdue for replacement.

Collaboration is key to ensuring a replacement solution meets the needs of all stakeholders. A replacement cannot be designed solely by number portability experts alone; but must incorporate a far wider range of expertise including cybersecurity, user experience, commercial, business and risk management teams. Likewise, the process must work for both large and small telecoms firms, as well as their customers and partners.

Industry bodies that go beyond 'talking shops' could aid rapid consensus while providing access to international expertise, best practices, industry standards and proven technology – bringing together telecoms firms with banks, software vendors, academics and independent experts to develop a world-class solution that becomes the new standard for digital markets everywhere. The TM Forum Catalyst programme is a great example of this type of industry-led mechanism.

Importantly, the UK is simply out of time. Either the industry acts today, or UK political leaders need to mandate a deadline for action. Delay will continue to cost the economy untold millions in fraud for absolutely no good reason and undermine confidence in the UK's digital economy.

references and notes

1. ‘Fighting Fraud: Breaking the Chain’ can be downloaded from https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf

2. See: ONS, ‘Crime in England and Wales: Appendix tables’ (27 October 2022), table 1: www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

3. See: ‘Cross-sector action needed as criminal gangs steal more than £1.3 billion’, UK Finance (August 2022): www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2022

4. See: ‘The threat from fraud’, NCA: www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime

5. Action Fraud data revealed that in the 13 months to October 2022 there were 357,129 reports of fraud, with losses totalling £4 billion. 316,520 reports (89%) were from individuals and 68% were cyber-enabled. See also: ONS, ‘Crime in England and Wales: year ending June 2022’ (27 October 2022): www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwale/yearendingjune2022#fraud and City of London Police, ‘NFIB Fraud and Cyber Crime Dashboard: 13 months of data’: colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46

6. Total fraud is much higher than reported fraud. See: ‘The Financial Cost of Fraud 2021’. www.crowe.com/uk/insights/financial-cost-fraud-data-2021

7. See: www.express.co.uk/finance/personalfinance/1608245/scam-warning-SIM-card-fraud-rip-off-britain

8. See: www.theguardian.com/money/2020/sep/09/oops-one-message-on-my-mobile-cost-me-1000-in-a-sim-swap

9. See: www.express.co.uk/finance/personalfinance/1623349/scam-warning-premium-bonds-sim-swap-fraud-alert-tactic

10. NPAC provides three services in addition to the central function of number porting. PortData Source is for law enforcement and public safety agencies that need to verify the service provider and porting history for specific numbers. PortData Comply supports compliance with the US’s Telephone Consumer Protect Act (TCPA). PortData Validate is for businesses that rely on phone number data to protect consumers, assess risk and mitigate fraud.

11. The UK porting system is supplied by Syniverse.

12. This required it to alter Part 1 and General Condition 18 of Part 2 of the General Conditions regarding number portability, as set out in Annex 2 to the concluding statement entitled “Telephone number portability for consumers switching suppliers”.

13. See: www.catribunal.org.uk/sites/default/files/Judgment_1094_180908.pdf

14. See: ‘Fraud Loss Survey Report 2021’ by Communications Fraud Control Association (CFCA) cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf

15. SIM Only (SIMO) is a mobile subscription without a handset. They are usually cheaper than traditional postpaid deals because the cost of the handset does not need to be recouped, and they allow more frequent switching (as often as monthly).

16. Ibid. CFCA pages 46-47.

17. This is Action 4 in the HoL report.

18. See page 7 of this report.

19. See: inews.co.uk/inews-lifestyle/money/bills/vodafone-pay-damages-landmark-sim-swap-case-1812653

things you should know now

Mobiles are an integral part of a person’s digital identity

If fraudsters can hijack your mobile account they can intercept your communications, steal your ID, empty your bank account, and worse…

SIMs are highly secure. Handsets are now secure. **So criminals are targeting your phone number.**

MIND THE GAP

Unfortunately, there’s a hidden gap in the UK’s digital infrastructure criminals can easily exploit

Number portability lets people keep their number when they shift provider. It’s essential for a competitive market.

But the UK’s process is old, inefficient and insecure.

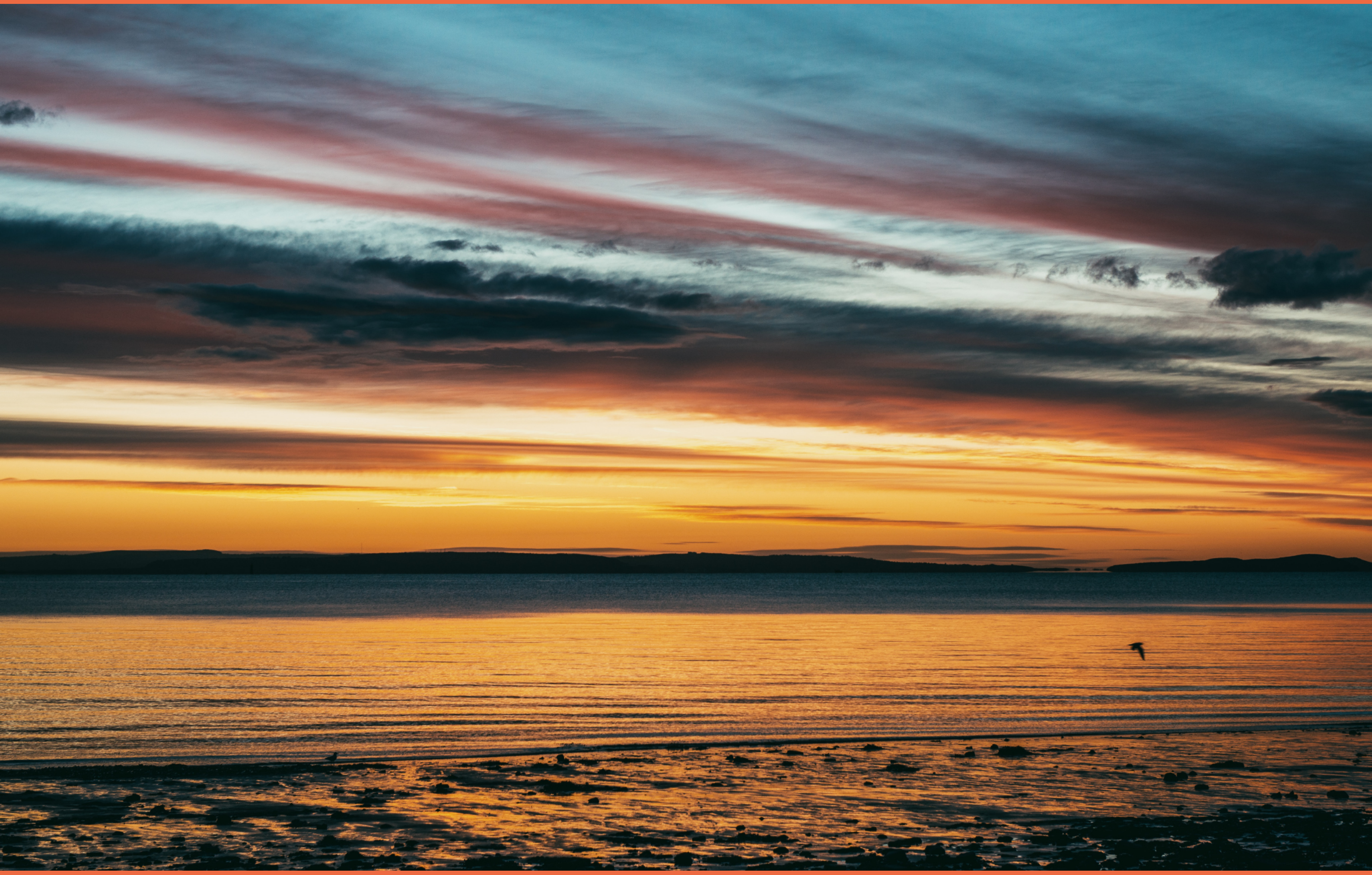
This leaves customers, banks and the national digital infrastructure **vulnerable to fraudsters.**

The UK is now a long way behind, because most other countries have a far more modern, efficient and secure number porting process

The UK telecoms industry **urgently** needs to act to protect its customers and its reputation, and to get itself ready for the future digital economy.

Source: Omnisperience 2023

omnisperience



About the author

Teresa Cottam is the Chief Analyst and founder of telecoms industry analysts Omnisperience, where she leads research & analysis. She is a renowned expert on customer experience, employee experience, customer communications & engagement, pricing, packaging & bundling, billing & charging. A judge of the GSMA's Global Mobile Awards (GloMos) and the World Communications Awards (WCA), she is also a Contributing Analyst to the TM Forum.

About Omnisperience

Located in the heart of the UK, Omnisperience's experienced analysts focus on improving the commercial success of digital service providers. We take a fresh approach to research and advisory projects, helping our clients better understand their market and customers and, as a result, become more profitable. Find out more at www.omnisperience.com

Omnisperience – Value Through Experience